

kaspersky

Kaspersky Endpoint Security for Windows 11.6.0

© 2023 AO Kaspersky Lab

Contenu

[Foire aux questions](#)

[Nouveautés](#)

[Kaspersky Endpoint Security for Windows](#)

[Distribution](#)

[Configurations logicielles et matérielles](#)

[Comparaison des fonctions de l'application selon le type de système d'exploitation](#)

[Comparaison des fonctions de l'application en fonction des outils d'administration](#)

[Compatibilité avec d'autres applications](#)

[Installation et suppression de l'application](#)

[Déploiement via Kaspersky Security Center 12](#)

[Installation standard de l'application](#)

[Création du paquet d'installation](#)

[Mise à jour des bases dans le paquet d'installation](#)

[Création de la tâche d'installation à distance](#)

[Installation locale de l'application à l'aide de l'Assistant](#)

[Installation de l'application via la ligne de commande](#)

[Installation à distance de l'application à l'aide de System Center Configuration Manager](#)

[Description des paramètres d'installation dans le fichier setup.ini](#)

[Modification de la sélection des modules de l'application](#)

[Mise à jour de la version précédente de l'application](#)

[Suppression de l'application](#)

[Suppression via Kaspersky Security Center](#)

[Suppression de l'application à l'aide de l'assistant](#)

[Suppression de l'application via la ligne de commande](#)

[Licence de l'application](#)

[À propos du Contrat de licence](#)

[À propos de la licence](#)

[À propos du certificat de licence](#)

[À propos de l'abonnement](#)

[À propos de la clé de licence](#)

[À propos du code d'activation](#)

[À propos du fichier clé](#)

[Activation de l'application](#)

[Activation de l'application via Kaspersky Security Center](#)

[Activation de l'application à l'aide de l'assistant d'activation de l'application](#)

[Activation de l'application à l'aide de la ligne de commande](#)

[Consultation des informations relatives à la licence](#)

[Achat d'une licence](#)

[Renouvellement de l'abonnement](#)

[À propos des données](#)

[À propos des données dans le cadre du Contrat de licence utilisateur final](#)

[Collecte des données dans le cadre de l'utilisation de Kaspersky Security Network](#)

[Respect de la législation de l'Union européenne \(RGPD\)](#)

[Guide de démarrage](#)

[À propos du plug-in d'administration de Kaspersky Endpoint Security for Windows](#)

[Particularités de l'utilisation de plug-ins d'administration de différentes versions](#)

[Considérations particulières lors de l'utilisation de protocoles chiffrés pour l'interaction avec des services externes](#)

[Interface de l'application](#)

[Icône de l'application dans la zone de notification](#)

[Interface de l'application simplifiée](#)

[Configuration de l'affichage de l'interface de l'application](#)

[Guide de démarrage](#)

[Administration des stratégies](#)

[Gestion de la tâche](#)

[Configuration des paramètres locaux de l'application](#)

[Lancement et arrêt de Kaspersky Endpoint Security](#)

[Suspension et rétablissement de la protection et du contrôle de l'ordinateur](#)

[Analyse de l'ordinateur](#)

[Lancement et arrêt de la tâche d'analyse](#)

[Modification du niveau de sécurité](#)

[Modification de l'action sur les fichiers infectés](#)

[Composition de la liste des objets à analyser](#)

[Sélection du type de fichiers à analyser](#)

[Optimisation de l'analyse des fichiers](#)

[Analyse des fichiers composés](#)

[Utilisation des méthodes d'analyse](#)

[Utilisation des technologies d'analyse](#)

[Sélection du mode de lancement de la tâche d'analyse](#)

[Configuration du lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur](#)

[Analyse des disques amovibles lors de leur connexion à l'ordinateur](#)

[Analyse en arrière-plan](#)

[Vérification de l'intégrité de l'application](#)

[Mise à jour des bases de données et des modules de l'application](#)

[Schémas de mise à jour des bases de données et des modules de l'application](#)

[Mise à jour depuis un stockage du serveur](#)

[Mise à jour depuis un dossier partagé](#)

[Mise à jour à l'aide de Kaspersky Update Utility](#)

[Mise à jour en mode mobile](#)

[Lancement et arrêt des tâches](#)

[Lancement de la tâche de mise à jour avec les privilèges d'un autre utilisateur](#)

[Sélection du mode de lancement de la tâche de mise à jour](#)

[Ajout d'une source des mises à jour](#)

[Configuration de la mise à jour depuis un dossier partagé](#)

[Mise à jour des modules d'application](#)

[Utilisation du serveur proxy lors de la mise à jour](#)

[Annulation de la dernière mise à jour](#)

[Manipulation des menaces actives](#)

[Protection de l'ordinateur](#)

[Protection contre les fichiers malicieux](#)

[Activation et désactivation de la Protection contre les fichiers malicieux](#)

[Suspension automatique de la Protection contre les fichiers malicieux](#)

[Modification de l'action du module Protection contre les fichiers malicieux sur les objets infectés](#)

[Composition de la zone de protection du module Protection contre les fichiers malicieux](#)

[Utilisation des méthodes d'analyse](#)

[Utilisation des technologies d'analyse dans le cadre du fonctionnement du module Protection contre les fichiers malicieux](#)

[Optimisation de l'analyse des fichiers](#)

[Analyse des fichiers composés](#)

[Modification du mode d'analyse des fichiers](#)

[Protection contre les menaces Internet](#)

[Activation et désactivation de la Protection contre les menaces Internet](#)

[Modification de l'action à effectuer sur les objets malveillants du trafic Internet](#)

[Analyse des URL par rapport aux bases de données de phishing et d'adresses Internet malveillantes](#)

[Utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les menaces Internet](#)

[Constitution d'une liste des URL de confiance](#)

[Exportation et importation de la liste des adresses Internet de confiance](#)

[Protection contre les menaces par emails](#)

[Activation et désactivation de la Protection contre les menaces par emails](#)

[Modification de l'action exécutée sur les messages électroniques infectés](#)

[Composition de la zone de protection du module Protection contre les menaces par emails](#)

[Analyse des fichiers composés joints aux messages électroniques](#)

[Filtrage des pièces jointes dans les messages électroniques](#)

[Exportation et importation d'extensions pour le filtrage des pièces jointes](#)

[Analyse du courrier dans Microsoft Office Outlook](#)

[Protection contre les menaces réseau](#)

[Activation et désactivation de la Protection contre les menaces réseau](#)

[Blocage d'un ordinateur attaquant](#)

[Configuration des adresses des exclusions du blocage](#)

[Exportation et importation de la liste des exclusions de blocage](#)

[Configuration de la protection contre les attaques réseau par type](#)

[Firewall](#)

[Activation et désactivation du Pare-feu](#)

[Modification de l'état de la connexion réseau](#)

[Application des règles pour les paquets réseau](#)

[Création d'une règle pour les paquets réseau](#)

[Activation et désactivation de la règle pour les paquets réseau](#)

[Modification de l'action du Pare-feu pour la règle pour les paquets réseau](#)

[Modification de la priorité de la règle pour les paquets réseau](#)

[Règles d'exportation et d'importation des paquets réseau](#)

[Application des règles réseau pour les applications](#)

[Création d'une règle réseau d'applications](#)

[Activation et désactivation de la règle réseau des applications](#)

[Modification de l'action du Pare-feu pour la règle réseau des applications](#)

[Modification de la priorité de la règle réseau des applications](#)

[Surveillance du réseau](#)

[Protection BadUSB](#)

[Activation et désactivation de la Protection BadUSB](#)

[Utilisation d'un clavier virtuel pour l'autorisation des appareils USB](#)

[Protection AMSI](#)

[Activation et désactivation de la protection AMSI](#)

[Utilisation de la protection AMSI pour analyser les fichiers composés](#)

[Protection contre les Exploits](#)

[Activation et désactivation de la Protection contre les Exploits](#)

[Sélection de l'action à exécuter en cas de détection d'un exploit](#)

[Protection de la mémoire des processus système](#)

[Détection comportementale](#)

[Activation et désactivation de la Détection comportementale](#)

[Sélection de l'action à exécuter en cas de détection d'une activité malveillante d'une application](#)

[Protection des dossiers partagés contre le chiffrement externe](#)

[Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe](#)

[Sélection de l'action à exécuter en cas de détection du chiffrement externe de dossiers partagés](#)

[Création d'une exclusion pour la protection des dossiers partagés contre le chiffrement externe](#)

[Configuration des adresses des exclusions de la protection des dossiers partagés contre le chiffrement externe](#)

[Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe](#)

[Prévention des intrusions](#)

[Activation et désactivation de la Prévention des intrusions](#)

[Utilisation des groupes de confiance d'applications](#)

[Modifier le groupe de confiance d'une application](#)

[Configuration des privilèges des groupes de confiance](#)

[Sélection du groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security](#)

[Sélection d'un groupe de confiance pour les applications inconnues](#)

[Sélection d'un groupe de confiance pour les applications dotées d'une signature numérique](#)

[Utilisation des privilèges des applications](#)

[Protection des ressources du système d'exploitation et des données personnelles](#)

[Suppression des informations sur les applications inutilisées](#)

[Surveillance du module Prévention des intrusions](#)

[Protection de l'accès au flux audio et vidéo](#)

[Réparation des actions malicieuses](#)

[Kaspersky Security Network](#)

[Activation et désactivation de l'utilisation de Kaspersky Security Network](#)

[Restrictions de KSN privé](#)

[Activation et désactivation du mode Cloud pour les modules de la protection](#)

[Vérification de la connexion à Kaspersky Security Network](#)

[Vérification de la réputation d'un fichier dans Kaspersky Security Network](#)

[Analyse des connexions chiffrées](#)

[Configuration des paramètres d'analyse des connexions chiffrées](#)

[Analyse de connexions chiffrées dans Firefox et Thunderbird](#)

[Exclusion des connexions chiffrées de l'analyse](#)

[Contrôle de l'ordinateur](#)

[Contrôle Internet](#)

[Activation et désactivation du Contrôle Internet](#)

[Actions avec les règles d'accès aux sites Internet](#)

[Ajout d'une règle d'accès aux ressources Internet](#)

[Définition de la priorité des règles d'accès aux sites Internet](#)

[Activation et désactivation de la règle d'accès aux sites Internet](#)

[Exportation et importation de la liste des adresses Internet de confiance](#)

[Vérification du fonctionnement des règles d'accès aux sites Internet](#)

[Exportation et importation de la liste des adresses de sites Internet](#)

[Surveillance de l'activité des utilisateurs sur Internet](#)

[Modification des modèles de messages du Contrôle Internet](#)

[Règles de création de masques d'adresses de sites Internet](#)

[Migration des règles d'accès aux ressources Internet depuis des versions antérieures de l'application](#)

[Contrôle des appareils](#)

[Activation et désactivation du Contrôle des appareils](#)

[À propos des règles d'accès](#)

[Modification d'une règle d'accès aux appareils](#)

[Modification de la règle d'accès au bus de connexion](#)

[Ajout d'un réseau Wi-Fi à la liste des réseaux de confiance](#)

[Surveillance de l'utilisation des disques amovibles](#)

[Modification de la durée de mise en cache](#)

[Actions avec les appareils de confiance](#)

[Ajout d'appareils à la liste des appareils de confiance via l'interface de l'application](#)

[Ajout d'un appareil à la liste des appareils de confiance de Kaspersky Security Center](#)

[Exportation et importation de la liste des appareils de confiance](#)

[Obtention de l'accès à l'appareil bloqué](#)

[Octroi de l'accès en mode en ligne](#)

[Octroi de l'accès en mode hors ligne](#)

[Modification des modèles de messages du Contrôle des appareils](#)

[Anti-Bridging](#)

[Activation de la fonctionnalité Anti-Bridging](#)

[Modification de l'état d'une règle d'établissement de connexion](#)

[Modification de la priorité d'une règle d'établissement de connexion](#)

[Contrôle évolutif des anomalies](#)

[Activation et désactivation du Contrôle évolutif des anomalies](#)

[Activation et désactivation d'une règle du Contrôle évolutif des anomalies](#)

[Modification de l'action en cas de déclenchement d'une règle du Contrôle évolutif des anomalies](#)

[Création d'une exclusion pour une règle du Contrôle évolutif des anomalies](#)

[Exportation et importation d'exclusions pour les règles du Contrôle évolutif des anomalies](#)

[Application des mises à jour pour les règles du Contrôle évolutif des anomalies](#)

[Modification des modèles de messages du Contrôle évolutif des anomalies](#)

[Consultation des rapports du Contrôle évolutif des anomalies](#)

[Contrôle des applications](#)

[Restrictions sur le fonctionnement du Contrôle des applications](#)

[Activation et désactivation du Contrôle des applications](#)

[Sélection du mode du Contrôle des applications](#)

[Utilisation des règles du Contrôle des applications dans l'interface de l'application](#)

[Ajout d'une règle du Contrôle des applications](#)

[Ajout d'une condition de déclenchement de la règle de Contrôle des applications](#)

[Modification de l'état de la règle de Contrôle des applications](#)

[Gestion des règles du Contrôle des applications dans Kaspersky Security Center](#)

[Récupération des informations relatives aux applications installées sur les ordinateurs des utilisateurs](#)

[Création des catégories d'applications](#)

[Ajout à une catégorie d'applications de fichiers exécutables issus du dossier Fichiers exécutables](#)

[Ajout à une catégorie d'applications de fichiers exécutables liés à des événements](#)

[Ajout et modification des règles de Contrôle des applications à l'aide de Kaspersky Security Center](#)

[Modification de l'état de la règle de Contrôle des applications via Kaspersky Security Center](#)

[Exportation et importation de règles du Contrôle des applications](#)

[Test des règles de Contrôle des applications via Kaspersky Security Center](#)

[Consultation des événements à l'issue du fonctionnement d'essai du module Contrôle des applications](#)

[Consultation du rapport sur les applications interdites en mode d'essai](#)

[Consultation des événements à l'issue du fonctionnement du module Contrôle des applications](#)

[Consultation du rapport sur les applications interdites](#)

[Test des règles du Contrôle des applications](#)

[Surveillance des applications](#)

[Règles de création de masques de noms de fichiers ou de dossiers](#)

[Modification des modèles de messages du Contrôle des applications](#)

[Pratiques exemplaires en matière de mise en œuvre d'une liste d'applications autorisées](#)

[Configuration du mode de liste d'autorisation pour les applications](#)

[Test du mode de liste d'autorisation](#)

[Prise en charge du mode de liste d'autorisation](#)

[Contrôle des ports réseau](#)

[Activation du contrôle de tous les ports réseau](#)

[Constitution de la liste des ports réseau contrôlés](#)

[Constitution de la liste des applications dont tous les ports réseau sont contrôlés](#)

[Exportation et importation de listes de ports contrôlés](#)

[Protection élargie contre les menaces](#)

[Managed Detection and Response](#)

[Kaspersky Endpoint Agent](#)

[Suppression des données](#)

[Protection par mot de passe](#)

[Activation de la Protection par mot de passe](#)

[Octroi d'autorisations à des utilisateurs ou des groupes distincts](#)

[Utilisation du mot de passe temporaire pour octroyer un accès](#)

[Particularités des autorisations de la Protection par mot de passe](#)

[Zone de confiance](#)

[Définition de l'exclusion de l'analyse](#)

[Lancement et arrêt du fonctionnement de l'exclusion de l'analyse](#)

[Composition de la liste des applications de confiance](#)

[Activation et désactivation de l'effet des règles de la zone de confiance sur l'application de la liste des applications de confiance](#)

[Utilisation du stockage système sécurisé des certificats](#)

[Utilisation de la sauvegarde](#)

[Configuration de la durée de conservation maximale des fichiers dans la sauvegarde](#)

[Configuration de la taille maximale de la Sauvegarde](#)

[Restauration des fichiers depuis la sauvegarde](#)

[Suppression des copies de sauvegarde des fichiers depuis le dossier de sauvegarde](#)

[Service des notifications](#)

[Configuration des paramètres des journaux des événements](#)

[Configuration de l'affichage et la remise des notifications](#)

[Configuration de l'affichage des avertissements sur l'état de l'application dans la zone de notification](#)

[Utilisation des rapports](#)

[Consulter les rapports](#)

[Configuration de la durée maximale de conservation des rapports](#)

[Configuration de la taille maximale du fichier de rapport](#)

[Enregistrement du rapport dans un fichier](#)

[Suppression des informations des rapports](#)

[Autodéfense de Kaspersky Endpoint Security](#)

[Activation et désactivation du mécanisme de l'autodéfense](#)

[Activation et désactivation de la prise en charge de la technologie AM-PPL](#)

[Activation et désactivation du mécanisme de l'autodéfense contre l'administration externe](#)

[Assurance de fonctionnement des applications de l'administration à distance](#)

[Performances de Kaspersky Endpoint Security et compatibilité avec d'autres applications](#)

[Sélection des types d'objets à détecter](#)

[Activation et désactivation de la technologie de désinfection avancée](#)

[Activation et désactivation du mode d'économie d'énergie](#)

[Activation et désactivation du mode de transfert des ressources vers d'autres applications](#)

[Création et utilisation d'un fichier de configuration](#)

[Restauration des paramètres par défaut de l'application](#)

[Échange de messages entre utilisateur et administrateur](#)

[Chiffrement des données](#)

[Restrictions de la fonction de chiffrement](#)

[Modification de la longueur de la clé de chiffrement \(AES56/AES256\)](#)

[Kaspersky Disk Encryption](#)

[Particularités du chiffrement des disques SSD](#)

[Chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption](#)

[Composition de la liste des disques durs exclus du chiffrement](#)

[Exportation et importation de la liste des disques durs à exclure du chiffrement](#)

[Activation de l'utilisation de la technologie d'authentification unique \(SSO\)](#)

[Administration des comptes utilisateur de l'Agent d'authentification](#)

[Utilisation du token et de la carte à puce lors de l'utilisation de l'Agent d'authentification](#)

[Déchiffrement des disques durs](#)

[Restauration de l'accès à un disque protégé par la technologie Kaspersky Disk Encryption](#)

[Mise à jour du système d'exploitation](#)

[Élimination des erreurs lors de la mise à jour de la fonctionnalité de chiffrement](#)

[Sélection du niveau de traçage de l'Agent d'authentification](#)

[Modification des textes d'aide de l'Agent d'authentification](#)

[Suppression des objets et données restants au terme du fonctionnement test de l'Agent d'authentification](#)

[Administration BitLocker](#)

[Lancement du chiffrement de disque BitLocker](#)

[Déchiffrement d'un disque dur protégé par BitLocker](#)

[Restauration de l'accès au disque protégé par BitLocker](#)

[Chiffrement des fichiers sur les disques locaux de l'ordinateur](#)

[Lancement du chiffrement des fichiers sur les disques locaux de l'ordinateur](#)

[Composition des règles d'accès des applications aux fichiers chiffrés](#)

[Chiffrement des fichiers créés et modifiés par des applications distinctes](#)

[Composition de la règle de déchiffrement](#)

[Déchiffrement des fichiers sur les disques locaux de l'ordinateur](#)

[Création d'archives chiffrées](#)

[Restauration de l'accès aux fichiers chiffrés](#)

[Restauration de l'accès aux données chiffrées en cas de panne du système d'exploitation](#)

[Modification des modèles de messages pour l'octroi de l'accès aux fichiers chiffrés](#)

[Chiffrement des disques amovibles](#)

[Lancement du chiffrement des disques amovibles](#)

[Ajout d'une règle de chiffrement pour les disques amovibles](#)

[Exportation et importation d'une liste de règles de chiffrement pour les disques amovibles](#)

[Mode portable pour utiliser les fichiers chiffrés sur les disques amovibles](#)

[Déchiffrement des disques amovibles](#)

[Consultation des informations relatives au chiffrement des données](#)

[Consultation des états du chiffrement](#)

[Consultation des statistiques de chiffrement sur les volets d'informations de Kaspersky Security Center](#)

[Consultation des erreurs de chiffrement des fichiers sur les disques locaux de l'ordinateur](#)

[Consultation du rapport sur le chiffrement des données](#)

[Utilisation des appareils chiffrés en l'absence d'accès à ceux-ci.](#)

[Récupération de données à l'aide de l'utilitaire de restauration FDERT](#)

[Création d'un disque de dépannage du système d'exploitation](#)

[Administration de l'application via la ligne de commande](#)

[Commandes](#)

[SCAN. Recherche de virus](#)

[UPDATE. Mise à jour des bases de données et des modules de l'application](#)

[ROLLBACK. Restauration de la dernière mise à jour](#)

[TRACES. Traces](#)

[START. Activation du profil](#)

[STOP. Désactivation du profil](#)

[STATUS. État du profil](#)

[STATISTICS. Statistiques de l'exécution du profil](#)

[RESTORE. Restauration des fichiers](#)

[EXPORT. Exportation des paramètres de l'application](#)

[IMPORT. Importation des paramètres de l'application](#)

[ADDKEY. Application du fichier clé](#)

[LICENSE. Licence](#)

[RENEW. Achat d'une licence](#)

[PBATESTRESET. Réinitialiser les résultats de l'analyse avant le chiffrement du disque](#)

[EXIT. Quitter l'application](#)

[EXITPOLICY. Désactiver la stratégie](#)

[STARTPOLICY. Activation de la stratégie](#)

[DISABLE. Désactivation de la protection](#)

[SPYWARE. Détection de logiciels espion](#)

[MDRLICENSE. Activation MDR](#)

[KSN. Transition Global/Private KSN](#)

[Commandes KESCLI](#)

[Analyse. Recherche de virus](#)

[GetScanState. État d'achèvement de l'analyse](#)

[GetLastScanTime. Calcul du temps requis pour l'analyse](#)

[GetThreats. Collecte de données à propos des menaces détectées](#)

[UpdateDefinitions. Mise à jour des bases de données et des modules de l'application](#)

[GetDefinitionState. Calcul du temps requis pour la mise à jour](#)

[EnableRTP. Activation de la protection](#)

[GetRealTimeProtectionState. États de la Protection contre les fichiers malicieux](#)

[Version. Identification de la version de l'application](#)

[Codes d'erreur](#)

[Application. Profils d'application](#)

[Administration de l'application via l'API REST](#)

[Installation d'une application avec API REST](#)

[Utilisation de l'API](#)

[Sources d'informations sur l'application](#)

[Contacter le Support Technique](#)

[À propos de la composition et de la conservation des fichiers de traçage](#)

[Trace de l'application](#)

[Trace des performances de l'application](#)

[Enregistrement des fichiers dump](#)

[Protection des fichiers dump et de traçage](#)

[Restrictions et avertissements](#)

[Glossaire](#)

[Agent d'administration](#)

[Agent d'authentification](#)

[Archive](#)

[Base des URL de phishing](#)

[Base des URL malveillantes](#)

[Bases antivirus](#)

[Certificat de licence](#)

[Clé active](#)

[Clé complémentaires](#)

[Émetteur de certificat](#)

[Faux positif](#)

[Fichier infectable](#)

[Fichier infecté](#)

[Forme normalisée de l'adresse du site Internet](#)

[Gestionnaire de fichiers portable](#)

[Groupe d'administration](#)

[Masque](#)

[Objet OLE](#)

[Réparation d'objets](#)

[Tâche](#)

[Trusted Platform Module](#)

[Zone d'analyse](#)

[Zone de protection](#)

[Annexes](#)

[Annexe 1. Paramètres de l'application](#)

[Protection contre les fichiers malicieux](#)

[Protection contre les menaces Internet](#)

[Protection contre les menaces par emails](#)

[Protection contre les menaces réseau](#)

[Firewall](#)

[Protection BadUSB](#)

[Protection AMSI](#)

[Protection contre les Exploits](#)

[Détection comportementale](#)

[Prévention des intrusions](#)

[Réparation des actions malicieuses](#)

[Kaspersky Security Network](#)

[Contrôle Internet](#)

[Contrôle des appareils](#)
[Contrôle des applications](#)
[Contrôle évolutif des anomalies](#)
[Endpoint Sensor](#)
[Chiffrement du disque](#)
[Chiffrement des fichiers](#)
[Chiffrement des disques amovibles](#)
[Modèles \(chiffrement des données\)](#)
[Exclusions](#)
[Paramètres de l'application](#)
[Rapports et stockage](#)
[Paramètres du réseau](#)
[Interface](#)
[Gestion des paramètres](#)
[Gestion de la tâche](#)
[Analyse de l'ordinateur](#)
[Analyse en arrière-plan](#)
[Analyse depuis le menu contextuel](#)
[Analyse des disques amovibles](#)
[Vérification de l'intégrité](#)
[Mise à jour des bases de données et des modules de l'application](#)
[Annexe 2. Groupes de confiance d'applications](#)
[Annexe 3. Extensions de fichiers pour l'analyse rapide des disques amovibles](#)
[Annexe 4. Types de fichiers pour le filtre de pièces jointes de Protection contre les menaces par emails](#)
[Annexe 5. Paramètres de réseau pour l'interaction avec les services externes](#)
[Annexe 6. Événements relatifs à l'application dans le journal des événements Windows](#)
[Informations sur le code tiers](#)
[Notice sur les marques de commerce](#)

Foire aux questions



GÉNÉRAL

[Quels ordinateurs prennent en charge Kaspersky Endpoint Security ?](#)

[Qu'est-ce qui a changé par rapport à la dernière version ?](#)

[Avec laquelle de nos autres applications Kaspersky Endpoint Security est-il compatible ?](#)

[Comment économiser les ressources de l'ordinateur lors de l'exécution de Kaspersky Endpoint Security ?](#)



DEPLOIEMENT

[Comment installer Kaspersky Endpoint Security sur tous les ordinateurs d'une entreprise ?](#)

[Quels paramètres d'installation peuvent être configurés via la ligne de commande ?](#)

[Comment supprimer Kaspersky Endpoint Security à distance ?](#)



MISE À JOUR

[Quels sont les différents moyens de mise à jour des bases de données ?](#)

[Que faire si des problèmes surviennent après la mise à jour ?](#)

[Comment mettre à jour les bases de données en dehors du réseau de l'entreprise ?](#)

[Est-il possible d'utiliser un serveur proxy pour réaliser la mise à jour ?](#)



SECURITE

[Comment Kaspersky Endpoint Security analyse-t-il le courrier ?](#)

[Comment exclure un fichier de confiance de l'analyse ?](#)

[Comment protéger votre ordinateur contre les virus sur les clés USB ?](#)

[Comment effectuer une recherche de virus que l'utilisateur ne remarquera pas ?](#)

[Comment suspendre la protection de Kaspersky Endpoint Security pendant un certain temps ?](#)

[Comment récupérer un fichier que Kaspersky Endpoint Security a supprimé par erreur ?](#)



INTERNET

[Kaspersky Endpoint Security analyse-t-il les connexions sécurisées \(HTTPS\) ?](#)

[Comment autoriser les utilisateurs à se connecter uniquement à des réseaux Wi-Fi sécurisés ?](#)

[Comment bloquer les réseaux sociaux ?](#)



APPLICATIONS

[Comment savoir quels programmes sont installés sur l'ordinateur de l'utilisateur \(inventaire\) ?](#)

[Comment empêcher le lancement de jeux sur l'ordinateur ?](#)

[Comment l'exactitude de la configuration du Contrôle des applications ?](#)

[Comment ajouter une application à la liste des applications de confiance ?](#)



APPAREILS

[Comment interdire l'utilisation de clés USB ?](#)

[Comment ajouter un appareil à la liste de confiance ?](#)

[Puis-je accéder à un appareil verrouillé ?](#)



CHIFFREMENT

[Dans quelles conditions le chiffrement est-il impossible ?](#)

[Comment restreindre l'accès à une archive à l'aide d'un mot de passe ?](#)

[Est-il possible d'utiliser des cartes à puce et des tokens pour le chiffrement ?](#)

[Est-il possible d'accéder à des données chiffrées en l'absence de connexion avec Kaspersky Security Center ?](#)

[Que faire en cas de plantage du système d'exploitation alors que les données n'ont pas été déchiffrées ?](#)



SUPPORT TECHNIQUE

[Où se trouver le fichier de rapport ?](#)

[Comment créer un fichier de traçage ?](#)

[Comment activer l'enregistrement des fichiers dump ?](#)

Comment protéger Kaspersky Endpoint Security contre une suppression par l'utilisateur ?

Nouveautés

Mise à jour 11.6.0

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security for Windows 11.6.0 :

1. [Prise en charge de Windows 10 21H1](#). Les particularités de la prise en charge du système d'exploitation Microsoft Windows 10 sont reprises dans la [base des connaissances du Support Technique](#).
2. [Le module Managed Detection and Response a été ajouté](#). Ce module facilite l'interaction avec la solution connue sous le nom de Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* offre une protection 24 heures sur 24 contre un nombre croissant de menaces capables de contourner les mécanismes de protection automatisés pour les organisations qui ont du mal à trouver des experts ou qui disposent de ressources internes limitées. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter le [guide d'aide de Kaspersky Managed Detection and Response](#).
3. L'application [Kaspersky Endpoint Agent](#), incluse dans le paquet de distribution, a été mise à jour jusqu'à la version 3.10. Kaspersky Endpoint Agent 3.10 offre de nouvelles fonctionnalités, résout certains problèmes antérieurs et a amélioré la stabilité. Pour en savoir plus à propos de l'application, veuillez consulter la documentation des solutions Kaspersky qui prennent en charge Kaspersky Endpoint Agent.
4. Elle permet désormais d'administrer la protection contre les attaques comme l'inondation des réseaux et l'analyse des ports dans les [paramètres de la Protection contre les menaces réseau](#).
5. Ajout d'une nouvelle méthode de création de règles réseau pour le pare-feu. Vous pouvez ajouter des [règles de paquets](#) et des [règles d'application](#) pour les connexions qui sont affichées dans la fenêtre de la [Surveillance du réseau](#). Toutefois, les paramètres de connexion aux règles réseau seront configurés automatiquement.
6. L'interface de la [Surveillance du réseau](#) est désormais améliorée. Ajout des informations concernant l'activité du réseau : identifiant du processus qui initie l'activité réseau ; type de réseau (réseau local ou Internet) ; ports locaux. Par défaut, les informations sur le type de réseau sont masquées.
7. Il est désormais possible de créer automatiquement des comptes de l'Agent d'authentification pour les nouveaux utilisateurs Windows. L'Agent permet à un utilisateur de compléter l'authentification pour l'accès aux disques qui ont été [chiffrés à l'aide de la technologie Kaspersky Disk Encryption](#), et de charger le système d'exploitation. L'application vérifie les informations relatives aux comptes utilisateur Windows sur l'ordinateur. Si Kaspersky Endpoint Security détecte un compte utilisateur Windows qui ne dispose pas de compte d'Agent d'authentification, l'application créera un nouveau compte pour accéder aux disques chiffrés. Par conséquent, vous n'avez pas besoin d'[ajouter manuellement des comptes d'Agent d'authentification](#) pour les ordinateurs avec des disques déjà chiffrés.
8. Il est désormais possible de surveiller le processus de chiffrement du disque dans l'interface de l'application sur les ordinateurs des utilisateurs (Kaspersky Disk Encryption et BitLocker). Vous pouvez exécuter l'outil Surveillance du chiffrement à partir de la [fenêtre principale de l'application](#).

Mise à jour 11.5.0

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security for Windows 11.6.0 :

1. [Prise en charge de Windows 10 20H2](#). Les particularités de la prise en charge du système d'exploitation Microsoft Windows 10 sont reprises dans la [base des connaissances du Support Technique](#).
2. [Interface de l'application](#) mise à jour. L'[icône de l'application dans la zone de notification](#), les notifications d'application et les boîtes de dialogue ont également été mises à jour.






3. Amélioration de l'interface du plug-in Web de Kaspersky Endpoint Security pour les modules Contrôle des applications, Contrôle des appareils et Contrôle évolutif des anomalies.
4. Ajout d'une fonctionnalité permettant d'importer et d'exporter des listes de règles et d'exclusions au format XML. Le format XML vous autorise à modifier les listes après leur exportation. Vous ne pouvez administrer les listes que dans Kaspersky Security Center Console. Les listes suivantes sont disponibles pour l'exportation/importation :
 - [Détection comportementale \(liste des exclusions\)](#).
 - [Protection contre les menaces Internet \(liste des adresses Internet de confiance\)](#).
 - [Protection contre les menaces par emails \(liste des extensions de filtres de pièces jointes\)](#).
 - [Protection contre les menaces réseau \(liste des exclusions\)](#).
 - [Pare-feu \(liste des règles pour les paquets réseau\)](#).
 - [Contrôle des applications \(liste des règles\)](#).
 - [Contrôle Internet \(liste des règles\)](#).
 - [Surveillance des ports réseau \(des listes de ports et d'applications surveillés par Kaspersky Endpoint Security\)](#).
 - [Kaspersky Disk Encryption \(liste des exclusions\)](#).
 - [Chiffrement des disques amovibles \(liste des règles\)](#).
5. Des informations sur l'objet MD5 ont été ajoutées au [rapport de détection des menaces](#). Dans les versions précédentes de l'application, Kaspersky Endpoint Security ne montrait que le hachage SHA256 d'un objet.
6. Ajout de la possibilité d'[attribuer la priorité aux règles d'accès aux appareils](#) dans les paramètres du Contrôle des appareils. L'attribution de priorités permet une configuration plus souple de l'accès des utilisateurs aux appareils. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Endpoint Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 0 au groupe des administrateurs et une priorité de 1 au groupe Tous. Vous pouvez configurer la priorité uniquement pour les appareils qui disposent d'un système de fichiers. Cela comprend les disques durs, les disques amovibles, les disquettes, les lecteurs de CD/DVD et les appareils portables (MTP).
7. De nouvelles fonctionnalités ont été ajoutées :
 - [Gestion des notifications audio](#).
 - Cost-Aware Networking Kaspersky Endpoint Security limite son propre trafic réseau si la connexion Internet est limitée (par exemple, via une connexion mobile).
 - [Gestion des paramètres de Kaspersky Endpoint Security via des applications d'administration à distance fiables](#) (comme TeamViewer, LogMeIn Pro et Remotely Anywhere). Vous pouvez utiliser des applications d'administration à distance pour lancer Kaspersky Endpoint Security et gérer les paramètres dans l'interface de l'application.
 - [Gestion des paramètres pour l'analyse du trafic sécurisé dans Firefox et Thunderbird](#). Vous pouvez sélectionner le stockage de certificats qui sera utilisé par Mozilla : le stockage de certificats de Windows ou le stockage de certificats de Mozilla. Cette fonctionnalité n'est offerte que pour les ordinateurs qui ne

disposent pas d'une stratégie appliquée. Si une stratégie est appliquée à un ordinateur, Kaspersky Endpoint Security permet automatiquement d'utiliser le stockage des certificats Windows dans Firefox et Thunderbird.

8. Ajout de la possibilité de [configurer le mode d'analyse du trafic sécurisé](#) : toujours analyser le trafic même si les modules de la protection sont désactivés, ou analyser le trafic lorsque les modules de la protection le demandent.
9. Révision de la procédure de [suppression d'informations dans les rapports](#). Un utilisateur ne peut supprimer que tous les rapports. Dans les versions précédentes de l'application, un utilisateur pouvait sélectionner des éléments particuliers de l'application dont les informations seraient supprimées des rapports.
10. Révision de la procédure d'[importation d'un fichier de configuration contenant les paramètres de Kaspersky Endpoint Security](#) et révision de la procédure de [restauration des paramètres de l'application](#). Avant l'importation ou la restauration, Kaspersky Endpoint Security n'affiche qu'un avertissement. Dans les versions précédentes de l'application, vous pouviez consulter les valeurs des nouveaux paramètres avant qu'ils ne soient appliqués.
11. Simplification de la [procédure de restauration de l'accès à un disque qui a été chiffré par BitLocker](#). Une fois que la procédure de récupération d'accès est terminée, Kaspersky Endpoint Security invite l'utilisateur à définir un nouveau mot de passe ou code PIN. Après que l'utilisateur a défini un nouveau mot de passe, BitLocker chiffrera le disque. Dans la version précédente de l'application, l'utilisateur devait réinitialiser manuellement le mot de passe dans les paramètres de BitLocker.
12. Les utilisateurs ont maintenant la possibilité de créer leur propre [zone de confiance](#) locale pour un ordinateur particulier. De cette façon, les utilisateurs peuvent créer leurs propres listes locales d'[exclusions](#) et d'[applications de confiance](#) en plus de la zone de confiance générale proposée par une stratégie. Un administrateur peut autoriser ou interdire l'utilisation d'exclusions locales ou d'applications locales de confiance. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.
13. Ajout de la possibilité d'[ajouter des commentaires dans les propriétés des applications de confiance](#). Les commentaires permettent de simplifier les recherches et le tri des applications de confiance.
14. [Administration de l'application via l'API REST](#) :
 - Il est maintenant possible de configurer les paramètres de l'extension Protection contre les menaces par emails pour Outlook.
 - Il est interdit de désactiver la détection des virus, des vers et des chevaux de Troie.

Mise à jour 11.4.0

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security for Windows 11.4.0 :

1. Mise à jour du design de [l'icône de l'application dans la zone de notification](#). L'icône  remplace l'icône . Si l'utilisateur doit effectuer une action (par exemple, redémarrer l'ordinateur après la mise à jour de l'application), l'icône se transforme en . Si les modules de la protection de l'application sont désactivés ou interrompus, l'icône devient  ou . Quand vous positionnez le curseur sur l'icône, Kaspersky Endpoint Security affiche une description du problème de protection de votre ordinateur.
2. L'application Kaspersky Endpoint Agent, incluse dans le paquet de distribution, a été mise à jour jusqu'à la version 3.9. Kaspersky Endpoint Agent 3.9 est compatible avec l'intégration aux nouvelles solutions de Kaspersky. Pour en savoir plus à propos de l'application, veuillez consulter la documentation des solutions Kaspersky qui prennent en charge Kaspersky Endpoint Agent.

3. Ajout de l'état *La licence n'est pas prise en charge* pour les composants de Kaspersky Endpoint Security. Vous pouvez consulter l'état des modules en cliquant sur le bouton **Modules de la protection** dans la [fenêtre principale de l'application](#).
4. De nouveaux événements concernant le fonctionnement [du module Protection contre les Exploits](#) ont été ajoutés aux [rapports](#).
5. Les pilotes de la [technologie Kaspersky Drive Encryption](#) sont automatiquement ajoutés à l'environnement de récupération Windows (WinRE - Windows Recovery Environment) lors du démarrage du chiffrement de disque. Dans la version précédente, l'application ajoutait les pilotes lors de l'installation de Kaspersky Endpoint Security. L'ajout de pilotes à WinRE améliore la stabilité de l'application lors de la restauration du système d'exploitation sur des ordinateurs protégés par la technologie Kaspersky Disk Encryption.

Le module Endpoint Sensor a été exclu de l'application Kaspersky Endpoint Security. Vous pouvez continuer à configurer les paramètres du module Endpoint Sensor à l'aide d'une stratégie si Kaspersky Endpoint Security versions 11.0.0 - 11.3.0 est installé sur l'ordinateur.

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (ci-après Kaspersky Endpoint Security) garantit la protection complexe de l'ordinateur contre divers types de menaces, d'attaques de réseau et d'escroqueries.

Pour protéger votre ordinateur, Kaspersky Endpoint Security utilise les technologies de détection des menaces suivantes :

- **Machine learning.** Kaspersky Endpoint Security utilise un modèle basé sur l'apprentissage machine. Ce modèle a été développé par les experts de Kaspersky. Tout au long de son utilisation, le modèle reçoit continuellement des données mises à jour sur les menaces de la part de KSN, ce qui permet d'entraîner le modèle.
- **Analyse sur le Cloud.** Kaspersky Endpoint Security reçoit des données sur les menaces de la part de Kaspersky Security Network. *Kaspersky Security Network (KSN)* est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications.
- **Analyse des experts.** Kaspersky Endpoint Security utilise des données sur les menaces ajoutées par les analystes de virus de Kaspersky. Les analystes de virus vérifient manuellement les objets si la réputation d'un objet ne peut pas être déterminée automatiquement.
- **Analyse comportementale.** Kaspersky Endpoint Security analyse l'activité d'un objet en temps réel.
- **Analyse automatique.** Kaspersky Endpoint Security reçoit des données d'un système d'analyse automatique des objets. Le système traite tous les objets reçus par Kaspersky, puis détermine la réputation des objets et ajoute les données correspondantes aux bases antivirus. Si le système ne parvient pas à déterminer la réputation d'un objet, il envoie une demande aux analystes de virus de Kaspersky.
- **Kaspersky Sandbox.** Kaspersky Endpoint Security analyse les objets sur une machine virtuelle. Kaspersky Sandbox analyse le comportement d'un objet et prend une décision concernant sa réputation. Cette technologie est disponible uniquement si vous utilisez Kaspersky Sandbox.

Chacune de ces menaces est traitée par un module particulier. Il est possible d'activer ou de désactiver les modules de votre choix, ainsi que de configurer leurs paramètres de fonctionnement.

Les modules suivants de l'application sont les modules de contrôle :

- **Contrôle des applications.** Le module surveille les tentatives de lancement d'applications par les utilisateurs et gère le lancement d'applications.
- **Contrôle des appareils.** Le module permet de configurer en toute souplesse des restrictions d'accès aux types d'appareils suivants : sources d'information (notamment, disques durs, disques amovibles, lecteurs de bande, CD/DVD), dispositifs de transfert de données (notamment, modems), dispositifs de conversion (notamment, imprimantes) ou interfaces qui permettent de connecter les appareils à l'ordinateur (notamment, USB, Bluetooth).
- **Contrôle Internet.** Le module permet de configurer en toute souplesse des restrictions d'accès aux sites Internet pour différents groupes d'utilisateurs.
- **Contrôle évolutif des anomalies.** Le module traque et régit les actions potentiellement dangereuses, atypiques pour l'ordinateur protégé.

Les modules de la protection sont les modules suivants :

- **Détection comportementale.** Ce module reçoit des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent offrir une protection plus efficace.

- **Protection contre les Exploits.** Le module traque les fichiers exécutables lancés par les applications vulnérables. S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier.
- **Prévention des intrusions.** Le module enregistre les actions réalisées par les applications dans le système d'exploitation et gère les actions des applications en fonction du groupe dans lequel le module place cette application. Il existe un ensemble de règles défini pour chaque groupe. Ces règles gèrent l'accès aux données personnelles de l'utilisateur et aux ressources du système d'exploitation. Les données personnelles de l'utilisateur sont les fichiers d'utilisateur dans le dossier "Mes documents", les fichiers cookie, les fichiers contenant les informations sur l'activité utilisateur, ainsi que les fichiers, les dossiers et les clés de registre avec les paramètres de fonctionnement et les informations importantes sur les applications le plus souvent utilisées.
- **Réparation des actions malicieuses.** Le module permet à Kaspersky Endpoint Security d'annuler les actions exécutées par les programmes malveillants dans le système d'exploitation.
- **Protection contre les fichiers malicieux.** Ce module permet d'éviter l'infection du système de fichiers de l'ordinateur. Le module est opérationnel directement après le lancement de Kaspersky Endpoint Security. Il se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les appareils de stockage de masse branchés. Le module intercepte toute tentative de requête au fichier et recherche dans celui-ci la présence éventuelle de virus et autres applications présentant une menace.
- **Protection contre les menaces Internet.** Le module analyse le trafic qui arrive sur l'ordinateur de l'utilisateur via le protocole HTTP et FTP et définit également si une adresse Internet appartient à la base des adresses Internet malveillantes ou de phishing.
- **Protection contre les menaces par emails.** Le module analyse l'ensemble des messages électroniques entrants et sortants à la recherche d'éventuels virus et d'autres applications présentant une menace.
- **Protection contre les menaces réseau.** Le module recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque l'activité réseau de l'ordinateur attaquant.
- **Pare-feu.** Le module assure la protection des données personnelles stockées sur l'ordinateur de l'utilisateur en bloquant la majorité des menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local.
- **Protection BadUSB.** Le module permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier.
- **Protection AMSI.** Le module analyse les objets selon la requête de l'application tierce et transmet les résultats de l'analyse à l'application qui a envoyé la requête.

En plus de la protection en temps réel assurée par les modules de l'application, il est conseillé de *réaliser* une recherche systématique d'éventuels virus et autres programmes dangereux sur votre ordinateur. Cette opération s'impose pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules en raison, par exemple, d'un niveau de sécurité faible.

La *mise à jour des bases et des modules de l'application* utilisés dans le fonctionnement de l'application est requise pour maintenir la protection de l'ordinateur à jour. Par défaut, l'application est mise à jour automatiquement. En cas de besoin, vous pouvez toujours mettre à jour manuellement les bases et les modules de l'application.

L'application Kaspersky Endpoint Security prévoit les tâches suivantes :

- **Vérification de l'intégrité.** Kaspersky Endpoint Security vérifie si les modules de l'application, situés dans le dossier d'installation de l'application, ont été endommagés ou modifiés. Si le module de l'application possède une signature numérique incorrecte, le module est considéré comme endommagé.

- **Analyse complète.** Kaspersky Endpoint Security lance l'analyse du système d'exploitation y compris la mémoire du noyau, les objets chargés au lancement du système d'exploitation, les secteurs d'amorçage, la sauvegarde du système d'exploitation et tous les disques durs et amovibles.
- **Analyse personnalisée.** Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur.
- **Analyse des zones critiques.** Kaspersky Endpoint Security analyse la mémoire du noyau et les objets et secteurs d'amorçage chargés au lancement du système d'exploitation.
- **Mise à jour.** Kaspersky Endpoint Security charge les mises à jour de la base et des modules de l'application. Ceci garantit l'actualité de la protection de l'ordinateur contre les virus et autres applications dangereuses.
- **Restauration de la dernière mise à jour.** Kaspersky Endpoint Security annule la dernière mise à jour des bases de données et des modules. Cela permet de revenir à l'utilisation des bases et les modules de l'application antérieurs le cas échéant, par exemple si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sûre.

Fonctions de service de l'application

Kaspersky Endpoint Security propose plusieurs fonctions de service. Les fonctions de service servent à maintenir le logiciel à jour, à élargir les possibilités d'utilisation de l'application et à fournir de l'aide pendant l'utilisation de l'application.

- **Rapports.** Pendant le fonctionnement de l'application, celle-ci génère un rapport pour chaque module de l'application. Les rapports permettent également de surveiller les résultats de l'exécution des tâches. Les rapports contiennent les listes des événements survenus pendant le fonctionnement de Kaspersky Endpoint Security et dans toutes les opérations exécutées par l'application. En cas de problème, vous pouvez envoyer ces rapports aux experts de Kaspersky ce qui leur permettra d'analyser la situation plus en détail.
- **Stockage des données.** Si l'application détecte des fichiers infectés lors de la recherche d'éventuels virus ou autres programmes dangereux sur l'ordinateur, elle bloque les fichiers en question. Kaspersky Endpoint Security sauvegarde les copies des fichiers réparés ou supprimés dans la *sauvegarde*. Kaspersky Endpoint Security met les fichiers qui n'ont pas été traités pour une raison quelconque sur la *liste des menaces actives*. Vous pouvez analyser les fichiers, restaurer les fichiers vers leur dossier d'origine et purger les stockages.
- **Service des notifications.** Le Service des notifications tient l'utilisateur au courant des événements qui ont un impact sur l'état de la protection de l'ordinateur et sur le fonctionnement de Kaspersky Endpoint Security. Les notifications peuvent être affichées sur l'écran ou envoyées par courrier électronique.
- **Kaspersky Security Network.** La participation de l'utilisateur au fonctionnement de Kaspersky Security Network permet d'augmenter l'efficacité de la protection grâce à une utilisation plus rapide des informations relatives à la réputation des fichiers, des sites Internet et du logiciel fourni par les utilisateurs du monde entier.
- **Licence.** L'achat d'une licence permet d'utiliser toutes les fonctions de l'application, d'accéder à la mise à jour des bases et des modules de l'application et de bénéficier du support technique par téléphone ou courrier électronique pour toute question liée à l'installation, à la configuration et à l'utilisation de l'application.
- **Assistance.** Tous les utilisateurs inscrits de Kaspersky Endpoint Security peuvent bénéficier de l'aide des experts du Support Technique de Kaspersky. Vous pouvez envoyer la demande au Support Technique de Kaspersky depuis le portail Kaspersky CompanyAccount ou par téléphone.

Si des erreurs ou des blocages apparaissent au cours de l'utilisation de l'application, cette dernière peut être automatiquement relancée.

Si des erreurs redondantes apparaissent au cours de l'utilisation de l'application et que ces erreurs en interrompent le fonctionnement, l'application exécute les actions suivantes :

1. Elle désactive les fonctions de contrôle et de protection (la fonction de chiffrement reste active).
2. Elle avertit l'utilisateur de la désactivation de ces fonctions.
3. Après la mise à jour des bases ou la mise en œuvre des bases des modules de l'application, la fonction tente d'en rétablir le fonctionnement.

Distribution

La distribution contient les paquets de distribution suivants :

- **Strong encryption (AES256)**

Le paquet de distribution contient les outils de chiffrement qui exploitent l'algorithme de chiffrement AES (Advanced Encryption Standard) avec une clé de 256 bits.

- **Lite encryption (AES56)**

Le paquet de distribution contient les outils de chiffrement qui exploitent l'algorithme de chiffrement AES avec une clé de 56 bits.

Chaque paquet de distribution contient les fichiers suivants :

| | |
|-------------------------------------|--|
| kes_win.msi | Paquet d'installation de Kaspersky Endpoint Security. |
| setup_kes.exe | Les fichiers nécessaires à l' installation de l'application selon tous les moyens disponibles ; |
| kes_win.kud | Fichier pour la création du paquet d'installation de Kaspersky Endpoint Security . |
| klcfginst.msi | Paquet d'installation du plug-in d'administration Kaspersky Endpoint Security pour Kaspersky Security Center. |
| bases.cab | Les fichiers des paquets de mise à jour utilisés lors de l'installation de l'application. |
| cleaner.cab | Fichiers pour la suppression des applications incompatibles. |
| incompatible.txt | Le fichier contenant la liste des applications incompatibles. |
| ksn_<ID de la langue>.txt | Le fichier à l'aide duquel vous pouvez prendre connaissance des conditions de participation à Kaspersky Security Network. |
| license.txt | Le fichier qui vous permet de prendre connaissance du Contrat de licence et de la Politique de confidentialité. |
| installer.ini | Le fichier contenant les paramètres interne de la distribution. |
| endpointagent.msi | Le paquet d'installation de la version 3.10 de Kaspersky Endpoint Agent , qui est l'application requise pour l'intégration à d'autres solutions de Kaspersky (par exemple, Kaspersky Sandbox). |
| NDP<version>-<propriétés du paquet> | Paquet d'installation de Microsoft .NET Framework. |
| keswin_web_plugin.zip | Archive contenant les fichiers nécessaires à l'installation du plug-in Web de Kaspersky Endpoint Security . |

Il est déconseillé de modifier la valeur de ces paramètres. Si vous voulez modifier les paramètres d'installation, utilisez le [fichier setup.ini](#).

Configurations logicielles et matérielles

Afin de garantir le fonctionnement de Kaspersky Endpoint Security, votre ordinateur doit avoir au minimum la configuration suivante.

Configuration minimale requise :

- Espace disponible sur le disque dur : 2 Go
- Processeur :
 - Poste de travail : 1 GHz
 - Server : 1,4 GHz
 - Prise en charge des instructions de SSE2
- mémoire vive :
 - Poste de travail (x86) : 1 Go
 - Poste de travail (x64) : 2 Go
 - Serveur : 2 Go
- Microsoft .NET Framework 4.0 ou version ultérieure

Systèmes d'exploitation compatibles pour les postes de travail :

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 ou version ultérieure ;
- Windows 8 Professional/Enterprise ;
- Windows 8.1 Professional/Enterprise ;
- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise.

L'algorithme de signature du module SHA-1 a été rendu obsolète par Microsoft. La mise à jour KB4474419 est requise pour installer correctement Kaspersky Endpoint Security sur un ordinateur fonctionnant sous le système d'exploitation Microsoft Windows 7. Pour en savoir plus à propos de cette mise à jour, consultez le [site de l'assistance technique de Microsoft](#).

Les particularités de la prise en charge du système d'exploitation Microsoft Windows 10 sont reprises dans la [base des connaissances du Support Technique](#).

Systèmes d'exploitation compatibles pour les serveurs :

- Windows Small Business Server 2011 Essentials/Standard (64 bits) ;

Microsoft Small Business Server 2011 Standard (64 bits) n'est pris en charge que si le Service Pack 1 pour Microsoft Windows Server 2008 R2 est installé.

- Windows MultiPoint Server 2011 (64 bits) ;
- Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter Service Pack 1 et suivants ;
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter ;
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter ;
- Windows Server 2016 Essentials/Standard/Datacenter ;
- Windows Server 2019 Essentials/Standard/Datacenter.

L'algorithme de signature du module SHA-1 a été rendu obsolète par Microsoft. La mise à jour KB4474419 est requise pour installer correctement Kaspersky Endpoint Security sur un ordinateur fonctionnant sous le système d'exploitation Windows Server 2008 R2. Pour en savoir plus à propos de cette mise à jour, consultez le [site de l'assistance technique de Microsoft](#) ².

Les particularités de la prise en charge des systèmes d'exploitation Microsoft Windows Server 2016 et Microsoft Windows Server 2019 sont reprises dans la [base des connaissances du Support Technique](#) ² :

Types de serveurs de terminaux pris en charge :

- Microsoft Remote Desktop Services basé sur Windows Server 2008 R2 SP1 ;
- Microsoft Remote Desktop Services basé sur Windows Server 2012 ;
- Microsoft Remote Desktop Services basé sur Windows Server 2012 R2 ;
- Microsoft Remote Desktop Services basé sur Windows Server 2016 ;
- Microsoft Remote Desktop Services basé sur Windows Server 2019.

Plateformes virtuelles compatibles :

- VMWare Workstation 16 Pro
- VMware ESXi 7.0 Mise à jour 1a
- Microsoft Hyper-V Server 2019 ;
- Citrix Virtual Apps and Desktops 7
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security fonctionne avec les versions suivantes de Kaspersky Security Center :

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Correctif A
- Kaspersky Security Center 12 Correctif B
- Kaspersky Security Center 13
- Kaspersky Security Center 13,1
- Kaspersky Security Center 13,2

Comparaison des fonctions de l'application selon le type de système d'exploitation

L'ensemble des fonctions disponibles dans Kaspersky Endpoint Security dépend du type du système d'exploitation : poste de travail ou serveur (voir tableau ci-dessous).

Comparaison des fonctions de Kaspersky Endpoint Security

| Fonction | Poste de travail | Serveur |
|--|------------------|---------|
| Protection avancée | | |
| Kaspersky Security Network | ✓ | ✓ |
| Détection comportementale | ✓ | ✓ |
| Protection contre les Exploits | ✓ | ✓ |
| Prévention des intrusions | ✓ | – |
| Réparation des actions malicieuses | ✓ | ✓ |
| Protection principale | | |
| Protection contre les fichiers malicieux | ✓ | ✓ |
| Protection contre les menaces Internet | ✓ | – |
| Protection contre les menaces par emails | ✓ | – |
| Firewall | ✓ | ✓ |
| Protection contre les menaces réseau | ✓ | ✓ |
| Protection BadUSB | ✓ | ✓ |
| Protection AMSI | ✓ | ✓ |
| Contrôles de sécurité | | |
| Contrôle des applications | ✓ | ✓ |
| Contrôle des appareils | ✓ | – |
| Contrôle Internet | ✓ | – |
| Contrôle évolutif des anomalies | ✓ | – |

| Chiffrement des données | | |
|---------------------------------------|---|---|
| Kaspersky Disk Encryption | ✓ | – |
| Chiffrement de disque BitLocker | ✓ | ✓ |
| Chiffrement des fichiers | ✓ | – |
| Chiffrement des disques amovibles | ✓ | – |
| Endpoint Agent | ✓ | ✓ |
| Managed Detection and Response | ✓ | ✓ |

Comparaison des fonctions de l'application en fonction des outils d'administration

L'ensemble des fonctions disponibles de Kaspersky Endpoint Security dépend des outils d'administration (cf. tableau ci-dessous).

Vous pouvez administrer l'application à l'aide des consoles Kaspersky Security Center 12 suivantes :

- Console d'administration. Composant logiciel enfichable pour la Microsoft Management Console (MMC) installée sur le poste de travail de l'administrateur.
- Web Console. Composant de Kaspersky Security Center installé sur le Serveur d'administration. Vous pouvez utiliser Web Console via un navigateur sur n'importe quel ordinateur qui a accès au Serveur d'administration.

Vous pouvez également administrer l'application à l'aide de Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* est une version de Kaspersky Security Center dans le Cloud. Cela signifie que le Serveur d'administration et d'autres modules de Kaspersky Security Center sont installés dans l'infrastructure Cloud de Kaspersky. Pour obtenir de plus amples informations sur l'administration des applications à l'aide de Kaspersky Security Center Cloud Console, consultez [l'aide de Kaspersky Security Center Cloud Console](#).

Comparaison des fonctions de Kaspersky Endpoint Security

| Fonction | Kaspersky Security Center 12 | | Kaspersky Security Center |
|--|------------------------------|-------------|---------------------------|
| | Console d'administration | Web Console | Cloud Console |
| Protection avancée | | | |
| Kaspersky Security Network | ✓ | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ | – |
| Détection comportementale | ✓ | ✓ | ✓ |
| Protection contre les Exploits | ✓ | ✓ | ✓ |
| Prévention des intrusions | ✓ | ✓ | ✓ |
| Réparation des actions malicieuses | ✓ | ✓ | ✓ |
| Protection principale | | | |
| Protection contre les fichiers malicieux | ✓ | ✓ | ✓ |
| Protection contre les menaces Internet | ✓ | ✓ | ✓ |

| | | | |
|--|---|---|---|
| Protection contre les menaces par emails | ✓ | ✓ | ✓ |
| Firewall | ✓ | ✓ | ✓ |
| Protection contre les menaces réseau | ✓ | ✓ | ✓ |
| Protection BadUSB | ✓ | ✓ | ✓ |
| Managed Detection and Response | ✓ | ✓ | ✓ |
| Protection AMSI | ✓ | ✓ | ✓ |
| Contrôles de sécurité | | | |
| Contrôle des applications | ✓ | ✓ | ✓ |
| Contrôle des appareils | ✓ | ✓ | ✓ |
| Contrôle Internet | ✓ | ✓ | ✓ |
| Contrôle évolutif des anomalies | ✓ | ✓ | ✓ |
| Chiffrement des données | | | |
| Kaspersky Disk Encryption | ✓ | ✓ | – |
| Chiffrement de disque BitLocker | ✓ | ✓ | ✓ |
| Chiffrement des fichiers | ✓ | ✓ | – |
| Chiffrement des disques amovibles | ✓ | ✓ | – |
| Endpoint Agent | ✓ | ✓ | ✓ |
| Tâches | | | |
| Ajout d'une clé | ✓ | ✓ | ✓ |
| Modification de la sélection des modules de l'application | ✓ | ✓ | ✓ |
| Inventaire | ✓ | ✓ | ✓ |
| Mise à jour | ✓ | ✓ | ✓ |
| Restauration de la mise à jour | ✓ | ✓ | ✓ |
| Recherche de virus | ✓ | ✓ | ✓ |
| Vérification de l'intégrité | ✓ | ✓ | – |
| Suppression des données | ✓ | ✓ | ✓ |
| Administration des comptes utilisateur de l'Agent d'authentification | ✓ | ✓ | – |

Compatibilité avec d'autres applications

Kaspersky Endpoint Security recherche la présence éventuelle d'autres applications de Kaspersky avant l'installation. L'application vérifie également que l'ordinateur ne contient aucun logiciel incompatible. La liste des applications incompatibles figure dans le fichier incompatible.txt du [kit de la distribution](#).

 [TÉLÉCHARGER LE FICHIER INCOMPATIBLE.TXT](#)

L'application Kaspersky Endpoint Security est incompatible avec les applications suivantes de Kaspersky :

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (y compris le module Endpoint Sensor).
- Kaspersky Sandbox (y compris Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (y compris le module Endpoint Sensor).

Si le module Endpoint Sensor est installé sur l'ordinateur à l'aide des outils de déploiement d'autres applications de Kaspersky, il sera automatiquement supprimé lors de l'installation de Kaspersky Endpoint Security. Dans ce cas, Kaspersky Endpoint Security peut inclure le module Endpoint Sensor/Kaspersky Endpoint Agent si vous avez sélectionné Endpoint Agent dans la liste des modules de l'application.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server.
- Kaspersky Embedded Systems Security.

Si des applications de cette liste sont installées sur l'ordinateur, Kaspersky Endpoint Security les supprime. Attendez la fin de ce processus pour poursuivre l'installation de Kaspersky Endpoint Security.

Installation et suppression de l'application

Il existe plusieurs méthodes pour installer l'application Kaspersky Endpoint Security sur un ordinateur :

- localement à l'aide de l'[Assistant d'installation de l'application](#).
- localement via la [ligne de commande](#).
- à distance via [Kaspersky Security Center 12](#).
- à distance via l'éditeur de gestion de stratégies de groupe Microsoft Windows (pour en savoir plus, consultez le [site de l'assistance technique de Microsoft](#)).
- à distance à l'aide de [System Center Configuration Manager](#).

Vous pouvez configurer les paramètres d'installation de l'application de plusieurs manières. Si vous utilisez simultanément plusieurs méthodes de configuration des paramètres, Kaspersky Endpoint Security applique les paramètres qui possèdent la priorité la plus élevée. Kaspersky Endpoint Security respecte l'ordre de priorité suivant :

1. Paramètres tirés du fichier [setup.ini](#).
2. Paramètres tirés du fichier installer.ini.
3. Paramètres tirés de la [ligne de commande](#).

Avant de lancer l'installation de Kaspersky Endpoint Security (y compris l'installation à distance), il est conseillé de quitter toutes les applications en cours d'exécution.

Déploiement via Kaspersky Security Center 12

Kaspersky Endpoint Security peut être déployé sur des ordinateurs dans le réseau de l'organisation de plusieurs façons. Vous pouvez sélectionner la méthode de déploiement qui convient le mieux à votre organisation ou utiliser plusieurs méthodes de déploiement simultanément. Kaspersky Security Center 12 prend en charge les principaux modes de déploiement suivants :

- Installation de l'application à l'aide de l'assistant de déploiement de la protection.
[Mode standard d'installation](#) qui convient si vous êtes satisfaits des paramètres par défaut de Kaspersky Endpoint Security et si votre organisation possède une infrastructure simple qui ne requiert pas de configuration spéciale.

- Installation de l'application à l'aide d'une tâche d'installation à distance.

Le mode universel d'installation qui permet de configurer les paramètres de Kaspersky Endpoint Security et d'administrer en souplesse les tâches d'installation à distance. L'installation de Kaspersky Endpoint Security comprend les étapes suivantes :

1. [création du paquet d'installation](#) ;
2. [création de la tâche d'installation à distance](#).

Kaspersky Security Center 12 prend également en charge d'autres modes d'installation de Kaspersky Endpoint Security, par exemple, le déploiement au sein d'une image du système d'exploitation. Pour en savoir plus sur les autres modes de déploiement, [consultez l'aide de Kaspersky Security Center 12](#).

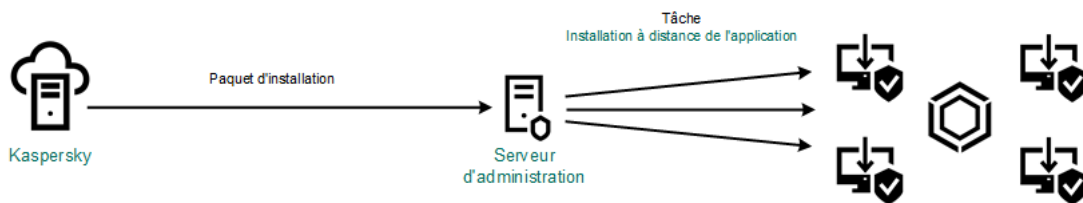
Installation standard de l'application

Pour installer l'application sur les ordinateurs de l'organisation, Kaspersky Security Center prévoit un assistant de déploiement de la protection. L'assistant de déploiement de la protection comprend les principales actions suivantes :

1. Sélection du paquet d'installation de Kaspersky Endpoint Security.

Le *paquet d'installation* désigne l'ensemble de fichiers formé pour l'installation à distance de l'application de Kaspersky à l'aide de Kaspersky Security Center. Le paquet d'installation contient l'ensemble de paramètres indispensables à l'installation de l'application et à la garantie de son fonctionnement immédiatement après l'installation. Le paquet d'installation est créé sur la base des fichiers portant l'extension kpd et kud qui figurent dans la distribution de l'application. Le paquet d'installation de Kaspersky Endpoint Security est commun à toutes les versions prises en charge du système d'exploitation Windows et des types d'architecture du processeur.

2. La création de la tâche du Serveur d'administration de Kaspersky Security Center *Installation à distance de l'application*.



Déploiement de Kaspersky Endpoint Security

[Procédure de lancement de l'assistant de déploiement de sécurité dans la Console d'administration \(MMC\)](#)

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Avancé** → **Installation à distance**.

2. Cliquez sur le lien **Déployer le paquet d'installation sur les appareils administrés (postes de travail)**.

L'Assistant de déploiement de la protection démarre. Suivez les instructions de l'assistant.

Il faut ouvrir les ports TCP 139 et 445 ainsi que les ports UDP 137 et 138 sur l'ordinateur client.

Étape 1. Sélection du paquet d'installation

Sélectionnez le paquet de Kaspersky Endpoint Security dans la liste des paquets d'installation. Si le paquet d'installation de Kaspersky Endpoint Security ne figure pas dans la liste, vous pouvez le créer dans l'assistant.

Vous pouvez configurer les [paramètres des paquets d'installation](#) dans Kaspersky Security Center. Par exemple, vous pouvez sélectionner les modules de l'application qui seront installés sur un ordinateur.

L'Agent d'administration est installé en même temps que Kaspersky Endpoint Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

Étape 2. Sélection d'appareils pour l'installation

Sélectionnez les ordinateurs sur lesquels l'application Kaspersky Endpoint Security va être installée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'Agent d'administration n'est pas installé sur les appareils non distribués. Dans ce cas, la tâche est affectée à l'ensemble d'appareils. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 3. Définition des paramètres de la tâche d'installation à distance

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le chargement du paquet d'installation.** Sélectionnez le mode d'installation de l'application :
 - **À l'aide de l'Agent d'administration.** Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.

- **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution.** Le paquet d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, [consultez l'aide de Kaspersky Security Center](#).
- **À l'aide des outils du système d'exploitation à l'aide d'un Serveur d'administration.** Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.
- **Comportement des appareils administrés par d'autres serveurs.** Sélectionnez le mode d'installation de Kaspersky Endpoint Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.
- **Ne pas installer l'application si elle est déjà installée.** Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.
- **Désigner l'installation de l'Agent d'administration dans les stratégies de groupe Active Directory.** Installation de l'Agent d'administration à l'aide des outils d'Active Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.

Étape 4. Sélection de la clé de licence

Ajoutez la clé au paquet d'installation pour l'activation de l'application. Cette étape est facultative. Si une clé de licence avec fonction de distribution automatique se trouve sur le Serveur d'administration, la clé sera ajoutée automatiquement plus tard. Vous pouvez également [activer l'application](#) plus tard à l'aide de la tâche *Ajouter la clé*.

Étape 5. Sélection du paramètre de redémarrage du système d'exploitation

Sélectionnez l'action à exécuter quand le redémarrage de l'ordinateur est requis. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.

Étape 6. Suppression des applications incompatibles avant d'installer le programme

Prenez connaissance de la liste des applications incompatibles et autorisez la suppression. Si des applications incompatibles sont présentes sur l'ordinateur, l'installation de Kaspersky Endpoint Security se solde sur une erreur.

Étape 7. Sélection du compte utilisateur pour accéder à l'ordinateur

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 8. Lancement de l'installation

Quittez l'assistant. Si nécessaire, cochez la case **Ne pas lancer la tâche après la fin de l'assistant d'installation à distance**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

[Procédure de lancement de l'assistant de déploiement de sécurité dans Web Console et Cloud Console](#) 

Dans la fenêtre principale de Web Console choisissez **Sondage du réseau et déploiement** → **Déploiement et destination** → **Assistant de déploiement de la protection**.

L'Assistant de déploiement de la protection démarre. Suivez les instructions de l'assistant.

Il faut ouvrir les ports TCP 139 et 445 ainsi que les ports UDP 137 et 138 sur l'ordinateur client.

Étape 1. Sélection du paquet d'installation

Sélectionnez le paquet de Kaspersky Endpoint Security dans la liste des paquets d'installation. Si le paquet d'installation de Kaspersky Endpoint Security ne figure pas dans la liste, vous pouvez le créer dans l'assistant. Pour créer le paquet d'installation, il n'est pas nécessaire de chercher le paquet de distribution et de l'enregistrer dans la mémoire de l'ordinateur. Kaspersky Security Center contient la liste des paquets de distribution situés sur les serveurs de Kaspersky et la création du paquet d'installation est automatique. Kaspersky met à jour la liste après l'émission des nouvelles versions des applications.

Vous pouvez configurer les [paramètres des paquets d'installation](#) dans Kaspersky Security Center. Par exemple, vous pouvez sélectionner les modules de l'application qui seront installés sur un ordinateur.

Étape 2. Sélection de la clé de licence

Ajoutez la clé au paquet d'installation pour l'activation de l'application. Cette étape est facultative. Si une clé de licence avec fonction de distribution automatique se trouve sur le Serveur d'administration, la clé sera ajoutée automatiquement plus tard. Vous pouvez également [activer l'application](#) plus tard à l'aide de la tâche *Ajouter la clé*.

Étape 3. Sélection de l'Agent d'administration

Sélectionnez la version de l'Agent d'administration qui va être installé en même temps que Kaspersky Endpoint Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

Étape 4. Sélection d'appareils pour l'installation

Sélectionnez les ordinateurs sur lesquels l'application Kaspersky Endpoint Security va être installée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'Agent d'administration n'est pas installé sur les appareils non distribués. Dans ce cas, la tâche est affectée à l'ensemble d'appareils. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 5. Configuration des paramètres complémentaires

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le chargement du paquet d'installation.** Sélection du mode d'installation de l'application :
 - **À l'aide de l'Agent d'administration.** Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.
 - **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution.** Le paquet d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez [l'aide de Kaspersky Security Center](#).
 - **À l'aide des outils du système d'exploitation à l'aide d'un Serveur d'administration.** Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.
- **Ne pas installer l'application si elle est déjà installée.** Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.
- **Désigner l'installation du paquet d'installation dans les stratégies de groupe Active Directory.** L'installation de Kaspersky Endpoint Security s'opère à l'aide des outils de l'Agent d'administration ou des outils d'Active Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.

Étape 6. Sélection du paramètre de redémarrage du système d'exploitation

Sélectionnez l'action à exécuter quand le redémarrage de l'ordinateur est requis. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.

Étape 7. Suppression des applications incompatibles avant d'installer le programme

Prenez connaissance de la liste des applications incompatibles et autorisez la suppression. Si des applications incompatibles sont présentes sur l'ordinateur, l'installation de Kaspersky Endpoint Security se solde sur une erreur.

Étape 8. Déplacement dans un groupe d'administration

Sélectionnez le groupe d'administration dans lequel il faut déplacer les ordinateurs après l'installation de l'Agent d'administration. Le déplacement dans un groupe d'administration est indispensable pour l'application des [stratégies](#) et [des tâches de groupe](#). Si l'ordinateur se trouve déjà dans un groupe d'administration quelconque, il ne sera pas déplacé. Si vous ne choisissez pas un groupe d'administration, les ordinateurs seront ajoutés au groupe **Appareils non distribués**.

Étape 9. Sélection du compte utilisateur pour accéder à l'ordinateur

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 10. Lancement de l'installation

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Création du paquet d'installation

Le *paquet d'installation* désigne l'ensemble de fichiers formé pour l'installation à distance de l'application de Kaspersky à l'aide de Kaspersky Security Center. Le paquet d'installation contient l'ensemble de paramètres indispensables à l'installation de l'application et à la garantie de son fonctionnement immédiatement après l'installation. Le paquet d'installation est créé sur la base des fichiers portant l'extension kpd et kud qui figurent dans la distribution de l'application. Le paquet d'installation de Kaspersky Endpoint Security est commun à toutes les versions prises en charge du système d'exploitation Windows et des types d'architecture du processeur.

[Procédure de création d'un paquet d'installation dans la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Avancé** → **Installation à distance** → **Paquets d'installation**.

La liste des paquets d'installation téléchargés depuis Kaspersky Security Center s'affiche.

2. Cliquez sur le bouton **Créer un paquet d'installation**.

L'Assistant de création du paquet d'installation démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de paquet d'installation

Sélectionnez l'option **Créer un paquet d'installation pour l'application de Kaspersky**.

Étape 2. Sélection du nom du paquet d'installation

Saisissez le nom du paquet d'installation, par exemple, Kaspersky Endpoint Security for Windows 11.6.0.

Étape 3 Sélection du paquet de distribution de l'application à installer

Cliquez sur le bouton **Parcourir** et sélectionnez le fichier `kes_win.kud` repris dans le [paquet de distribution](#).

Si nécessaire, mettez à jour les bases antivirus du paquet d'installation en cochant la case **Copier les mises à jour du stockage vers le paquet d'installation**.

Étape 4. Contrat de licence et Politique de confidentialité

Lisez et acceptez les dispositions du Contrat de licence et de la Politique de confidentialité.

Le paquet d'installation est créé et ajouté dans Kaspersky Security Center. Le paquet d'installation permet d'installer Kaspersky Endpoint Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application. De même, vous pouvez sélectionner dans les paramètres du paquet d'installation les modules de l'application et configurer les paramètres d'installation de l'application (cf. tableau ci-dessous). Le paquet d'installation contient les bases antivirus du stockage du Serveur d'administration. Vous pouvez [mettre à jour les bases dans le paquet d'installation](#) pour réduire la consommation de trafic lors de la mise à jour des bases après l'installation de Kaspersky Endpoint Security.

[Procédure de création d'un paquet d'installation dans la Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Détection d'appareils et déploiement** → **Déploiement et cible** → **Paquets d'installation**.

La liste des paquets d'installation téléchargés depuis Kaspersky Security Center s'affiche.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création du paquet d'installation démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de paquet d'installation

Sélectionnez l'option **Créer un paquet d'installation pour l'application de Kaspersky**.

L'Assistant créera un paquet d'installation à partir du kit de distribution situé sur les serveurs de Kaspersky. La liste se renouvelle automatiquement au fur et à mesure de l'édition de nouvelles versions de l'application. Pour installer Kaspersky Endpoint Security, il est recommandé de sélectionner cette option.

Vous pouvez également créer un paquet d'installation à partir d'un fichier.

Étape 2. Paquets d'installation

Choisissez le paquet d'installation de Kaspersky Endpoint Security for Windows. Le processus de création du paquet d'installation démarre. Lors de la création du paquet d'installation, vous devez accepter les termes du Contrat de licence utilisateur final et de la Politique de confidentialité.

Le paquet d'installation est créé et ajouté dans Kaspersky Security Center. Le paquet d'installation permet d'installer Kaspersky Endpoint Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application. De même, vous pouvez sélectionner dans les paramètres du paquet d'installation les modules de l'application et configurer les paramètres d'installation de l'application (cf. tableau ci-dessous). Le paquet d'installation contient les bases antivirus du stockage du Serveur d'administration. Vous pouvez [mettre à jour les bases dans le paquet d'installation](#) pour réduire la consommation de trafic lors de la mise à jour des bases après l'installation de Kaspersky Endpoint Security.

Paramètres du paquet d'installation

| Section | Description |
|----------------------------------|--|
| Modules de la protection | Cette section permet de choisir les modules de l'application qui seront disponibles. Vous pouvez modifier la sélection des modules de l'application plus tard à l'aide de la tâche Modification de la sélection des modules de l'application . Les modules Protection BadUSB, Endpoint Agent et les modules de chiffrement des données ne sont pas installés par défaut. Ces modules peuvent être ajoutés dans les paramètres du paquet d'installation. |
| Paramètres d'installation | <p>Ajouter le chemin de l'application dans la variable d'environnement %PATH%. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% du % pour le confort de l'utilisation de l'interface de la ligne de commande.</p> <p>Ne pas protéger le processus d'installation. La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Endpoint Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop).</p> |

Garantir la compatibilité avec Citrix PVS. Vous pouvez activer la prise en charge de Citrix Provisioning Services pour l'installation de Kaspersky Endpoint Security sur une machine virtuelle.

Chemin d'accès au dossier d'installation de l'application. Vous pouvez modifier le chemin de l'installation de Kaspersky Endpoint Security sur l'ordinateur client. Par défaut l'application s'installe dans le dossier %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.

Fichier de configuration. Vous pouvez charger le fichier qui définit les paramètres de fonctionnement de Kaspersky Endpoint Security. Vous pouvez [créer un fichier de configuration dans l'interface locale de l'application](#).

Mise à jour des bases dans le paquet d'installation

Le paquet d'installation contient les bases antivirus extraites du stockage du Serveur d'administration et qui étaient à jour au moment de la création du paquet d'installation. Une fois le paquet d'installation créé, vous pouvez mettre à jour les bases antivirus dans le paquet. Cela permet de réduire la consommation de données liée à la mise à jour des bases antivirus après l'installation de Kaspersky Endpoint Security.

Pour mettre à jour les bases antivirus dans le stockage du Serveur d'administration, utilisez la tâche *Chargement des mises à jour dans le stockage du Serveur d'administration* du Serveur d'administration. Pour en savoir plus sur la mise à jour des bases antivirus dans le stockage du Serveur d'administration, consultez l'[aide de Kaspersky Security Center](#).

Vous pouvez mettre à jour les bases dans le paquet d'installation uniquement dans la Console d'administration de Kaspersky Security Center et dans Kaspersky Security Center 12 Web Console. Il n'est pas possible de mettre à jour les bases dans le paquet d'installation dans l'application Kaspersky Security Center Cloud Console.

[Procédure de mise à jour des bases antivirus dans le paquet d'installation via la Console d'administration \(MMC\)](#)

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Avancé** → **Installation à distance** → **Paquets d'installation**.

La liste des paquets d'installation téléchargés depuis Kaspersky Security Center s'affiche.

2. Ouvrez les propriétés du paquet d'installation.

3. Dans la section **Général**, cliquez sur le bouton **Mettre à jour les bases**.

Les bases antivirus du paquet d'installation sont alors mises à jour à partir du stockage du Serveur d'administration. Le fichier `bases.cab` qui figure dans [la paquet d'installation](#) est remplacé par le dossier `bases`. Ce dossier contient les fichiers des paquets de mises à jour.

[Procédure de mise à jour des bases antivirus dans le paquet d'installation via Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Détection d'appareils et déploiement** → **Déploiement et cible** → **Paquets d'installation**.

La liste des paquets d'installation téléchargés depuis Web Console s'affiche.

2. Cliquez sur le nom du paquet d'installation de Kaspersky Endpoint Security dans lequel vous souhaitez mettre à jour les bases antivirus.

La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Sous l'onglet **Informations générales**, cliquez sur le lien **Mettre à jour les bases**.

Les bases antivirus du paquet d'installation sont alors mises à jour à partir du stockage du Serveur d'administration. Le fichier `bases . cab` qui figure dans [la paquet d'installation](#) est remplacé par le dossier `bases`. Ce dossier contient les fichiers des paquets de mises à jour.

Création de la tâche d'installation à distance

Pour installer Kaspersky Endpoint Security à distance, utilisez la tâche *Installation d'application à distance* prévue. La tâche *Installation à distance de l'application* permet de déployer le [paquet d'installation de l'application](#) sur tous les ordinateurs de l'organisation. Avant de déployer le paquet d'installation, vous pouvez [mettre à jour les bases antivirus](#) à l'intérieur du paquet, ainsi que sélectionner les modules de l'application disponibles dans les propriétés du paquet d'installation.

[Procédure de création d'une tâche d'installation à distance dans la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Sélectionnez **Serveur d'administration de Kaspersky Security Center** → **Installation à distance de l'application**.

Étape 2. Sélection du paquet d'installation

Sélectionnez le paquet de Kaspersky Endpoint Security dans la liste des paquets d'installation. Si le paquet d'installation de Kaspersky Endpoint Security ne figure pas dans la liste, vous pouvez le créer dans l'assistant.

Vous pouvez configurer les [paramètres des paquets d'installation](#) dans Kaspersky Security Center. Par exemple, vous pouvez sélectionner les modules de l'application qui seront installés sur un ordinateur.

L'Agent d'administration est installé en même temps que Kaspersky Endpoint Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

Étape 3. Avancé

Choisissez le paquet d'installation de l'Agent d'administration. La version sélectionnée de l'Agent d'administration est installée avec Kaspersky Endpoint Security.

Étape 4. Paramètres

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le chargement du paquet d'installation.** Sélectionnez le mode d'installation de l'application :
 - **À l'aide de l'Agent d'administration.** Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.
 - **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution.** Le paquet d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez [l'aide de Kaspersky Security Center](#).
 - **À l'aide des outils du système d'exploitation à l'aide d'un Serveur d'administration.** Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.

- **Comportement des appareils administrés par d'autres serveurs.** Sélectionnez le mode d'installation de Kaspersky Endpoint Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.
- **Ne pas installer l'application si elle est déjà installée.** Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.

Étape 5. Sélection du paramètre de redémarrage du système d'exploitation

Sélectionnez l'action à exécuter quand le redémarrage de l'ordinateur est requis. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.

Étape 6. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels l'application Kaspersky Endpoint Security va être installée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'Agent d'administration n'est pas installé sur les appareils non distribués. Dans ce cas, la tâche est affectée à l'ensemble d'appareils. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 7. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.



Étape 8. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 9. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple Installer Kaspersky Endpoint Security for Windows 11.6.0.

Étape 10. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. L'application est installée en mode silencieux. Après l'installation, l'icône  est ajoutée à la zone de notification de l'ordinateur de l'utilisateur. Si l'icône ressemble à , confirmez que vous avez [activé l'application](#).

[Procédure de création d'une tâche d'installation à distance dans la Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste **Application**, choisissez **Kaspersky Security Center**.

2. Dans la liste **Type de tâche**, choisissez **Installation à distance de l'application**.

3. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple **Installation de Kaspersky Endpoint Security for Windows pour les cadres**.

4. Dans le groupe **Appareils auxquels la tâche va être affectée**, choisissez la zone d'action de la tâche.

Étape 2. Sélection d'ordinateurs pour l'installation

À cette étape, sélectionnez les ordinateurs sur lesquels Kaspersky Endpoint Security va être installé conformément à l'option de zone d'action de la tâche sélectionnée.

Étape 3. Configuration des paramètres du paquet d'installation

Cette étape permet de configurer les paramètres du paquet d'installation :

1. Choisissez le paquet d'installation de Kaspersky Endpoint Security for Windows (11.6.0).

2. Choisissez le paquet d'installation de l'Agent d'administration.

La version sélectionnée de l'Agent d'administration est installée avec Kaspersky Endpoint Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

3. Dans le groupe **Forcer le téléchargement du paquet d'installation**, choisissez les outils d'installation de l'application :



- **À l'aide de l'Agent d'administration.** Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.
- **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution.** Le paquet d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez [l'aide de Kaspersky Security Center](#).

- **À l'aide des outils du système d'exploitation à l'aide d'un Serveur d'administration.** Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.
4. Dans le champ **Nombre maximum de téléchargements simultanés**, définissez la limite du nombre de requêtes adressées au Serveur d'administration pour le téléchargement du paquet d'installation. La restriction des demandes permet d'éviter la surcharge du réseau.
 5. Définissez dans le champ **Nombre de tentatives d'installation** la limite de tentatives d'installation de l'application. Si l'installation Kaspersky Endpoint Security se solde sur une erreur, la tâche lance à nouveau l'installation automatiquement.
 6. Le cas échéant, décochez la case **Ne pas installer l'application si elle est déjà installée**. Cela permet, par exemple, d'installer une application d'une version antérieure.
 7. Le cas échéant, décochez la case **Vérifier préalablement la version du système d'exploitation**. Cela permet d'éviter le téléchargement du paquet de distribution de l'application si le système d'exploitation de l'ordinateur ne répond pas à la configuration logicielle requise. Si vous êtes certain que le système d'exploitation est conforme à la configuration logicielle requise, vous pouvez ignorer cette vérification.
 8. Le cas échéant, cochez la case **Cible de l'installation du paquet d'installation dans les stratégies de groupe Active Directory**. L'installation de Kaspersky Endpoint Security s'opère à l'aide des outils de l'Agent d'administration ou des outils d'Active Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.
 9. Le cas échéant, cochez la case **Proposer à l'utilisateur de quitter les applications en cours d'exécution**. L'installation de Kaspersky Endpoint Security requiert des ressources de l'ordinateur. Pour le confort de l'utilisateur, l'assistant d'installation de l'application propose de quitter les applications en cours d'exécution avant de lancer l'installation. Cela permettra d'éviter le ralentissement des autres applications et les échecs possibles de l'ordinateur.
 10. Dans le groupe **Comportement des appareils administrés par ce Serveur**, sélectionnez le mode d'installation de Kaspersky Endpoint Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.

Étape 4. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. L'application est installée en mode silencieux. Après l'installation, l'icône  est ajoutée à la zone de notification de l'ordinateur de l'utilisateur. Si l'icône ressemble à , confirmez que vous avez [activé l'application](#).

Installation locale de l'application à l'aide de l'Assistant

L'interface de l'Assistant d'installation de l'application est composée d'une série de fenêtres qui correspondent aux différentes étapes de l'installation de l'application.

Pour installer l'application ou mettre à jour la version précédente de l'application à l'aide de l'Assistant d'installation de l'application,

1. Copiez le dossier du [kit de distribution](#) sur l'ordinateur de l'utilisateur.
2. Exécutez le fichier setup_ks.exe.

L'Assistant d'installation de l'application sera lancé.

Préparation de l'installation

Avant l'installation de Kaspersky Endpoint Security sur l'ordinateur ou avant la mise à jour de la version précédente de l'application, les conditions suivantes sont vérifiées :

- Absence d'une application non compatible (la liste des applications incompatibles figure dans le fichier incompatible.txt du [kit de la distribution](#)) ;
- Respect des [configurations logicielle et matérielle](#) ;
- Présences des privilèges pour l'installation du logiciel.

Si une des conditions énumérées n'est pas remplie, un message apparaît.

Si l'ordinateur correspond aux pré-requis, l'Assistant d'installation de l'application exécute la recherche des applications de Kaspersky dont l'utilisation simultanée peut entraîner des conflits. Si ce type d'applications est détecté, vous devrez les supprimer manuellement.

Si la liste des applications détectées contient des versions précédentes de Kaspersky Endpoint Security, toutes les données qui peuvent être migrées (par exemple, les informations sur l'activation, les paramètres de l'application), sont conservées et sont utilisées lors de l'installation de Kaspersky Endpoint Security 11.6.0 for Windows, et la version précédente de l'application est supprimée automatiquement. Cela se concerne les versions suivantes de l'application :

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (version 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (version 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (version 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (version 11.0.0.6499).
- Kaspersky Endpoint Security for Windows 11.0.1 (version 11.0.1.90).

- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (version 11.0.190).
- Kaspersky Endpoint Security 11.1.0 for Windows (version 11.1.0.15919).
- Kaspersky Endpoint Security for Windows 11.1.1 (version 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (version 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (version 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (version 11.3.0.773).
- Kaspersky Endpoint Security for Windows 11.4.0 (version 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (version 11.5.0.590).

Modules de Kaspersky Endpoint Security

Au cours de l'installation, vous pouvez sélectionner les modules de Kaspersky Endpoint Security que vous voulez installer. Le module Protection contre les fichiers malicieux doit obligatoirement être installé. Vous ne pouvez pas annuler son installation.

Par défaut, tous les modules à l'exception des modules suivants sont sélectionnés pour l'installation :

- [Protection BadUSB](#).
- [Chiffrement des fichiers](#).
- [Chiffrement du disque](#).
- [Administration BitLocker](#).
- [Endpoint Agent](#). *Endpoint Agent* installe l'application Kaspersky Endpoint Agent 3.10 pour garantir l'interaction entre l'application et les [solutions de Kaspersky](#) conçues pour détecter les menaces complexes (par exemple, Kaspersky Sandbox).

Vous pouvez [modifier la liste des modules après avoir installé l'application](#). Pour ce faire, vous devez lancer à nouveau l'assistant d'installation et sélectionner l'opération de modification de la sélection des modules.

Paramètres avancés

Protéger le processus d'installation de l'application. La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Endpoint Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop).

Garantir la compatibilité avec Citrix PVS. Vous pouvez activer la prise en charge de Citrix Provisioning Services pour l'installation de Kaspersky Endpoint Security sur une machine virtuelle.

Ajouter le chemin de l'application dans la variable d'environnement %PATH%. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% du % pour le confort de [l'utilisation de l'interface de la ligne de commande](#).

Installation de l'application via la ligne de commande

L'installation locale de Kaspersky Endpoint Security for Windows peut être réalisée d'une des manières suivantes :

- en mode interactif à l'aide de l'Assistant d'installation de l'application.
- En mode silencieux. Une fois que vous aurez lancé l'installation en mode silencieux, vous n'aurez plus à intervenir dans l'installation. Pour installer l'application en mode silencieux, utilisez les arguments /s et /qn.

Avant d'installer l'application en mode silencieux, ouvrez et lisez le Contrat de licence utilisateur final et le texte de la Politique de confidentialité. Le Contrat de licence utilisateur final et le texte de la Politique de confidentialité font partie du [kit de distribution de Kaspersky Endpoint Security](#). Installez l'application uniquement si vous avez entièrement lu, compris et accepté les termes et conditions du Contrat de licence, si vous comprenez et acceptez que vos données seront traitées et transmises (y compris à des pays tiers), conformément à la Politique de confidentialité, si vous avez lu et compris l'ensemble des dispositions de la Politique de confidentialité. Si vous n'acceptez pas les termes et conditions du Contrat de licence et de la Politique de confidentialité, n'installez pas Kaspersky Endpoint Security et ne l'utilisez pas.

Pour installer l'application ou mettre à jour une version antérieure, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le paquet de distribution Kaspersky Endpoint Security.
3. Exécutez la commande :

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nom d'utilisateur>
/pKLPASSWD=<mot de passe> /pKLPASSWDAREA=<zone d'action du mot de passe>]
[/pENABLETRACES=1|0 /pTRACESLEVEL=<niveau de traçage>] [/s]
```

ou

```
msiexec /i <nom du kit de distribution> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nom d'utilisateur> KLPASSWD=<mot de
passe> KLPASSWDAREA=<zone d'action du mot de passe>] [ENABLETRACES=1|0 TRACESLEVEL=
<niveau de traçage>] [/qn]
```

| | |
|-----------------|--|
| EULA=1 | Acceptation des dispositions du Contrat de licence Utilisateur final. Le texte Contrat de licence utilisateur final fait partie de la distribution de Kaspersky Endpoint Security . L'acceptation des dispositions du contrat de licence Utilisateur final est une condition indispensable pour installer l'application ou pour la mettre à jour. |
| PRIVACYPOLICY=1 | Acceptation de la Politique de confidentialité. Le texte de la Politique de confidentialité fait partie du kit de distribution de Kaspersky Endpoint Security . |

| | |
|------------------------|--|
| | <p>L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.</p> |
| KSN | <p>Participation ou non au Kaspersky Security Network (KSN). Si le paramètre n'est pas précisé, Kaspersky Endpoint Security sollicitera la confirmation de la participation à KSN au premier lancement de l'application. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : acceptation de la participation à KSN. • 0 : refus de la participation à KSN (valeur par défaut). <p>Le paquet de distribution de Kaspersky Endpoint Security est optimisé pour l'utilisation de Kaspersky Security Network. Si vous avez refusé de participer au Kaspersky Security Network, mettez à jour Kaspersky Endpoint Security directement à l'issue de l'installation.</p> |
| ALLOWREBOOT=1 | <p>Redémarrage automatique de l'ordinateur après l'installation ou la mise à jour de l'application, le cas échéant. Si le paramètre n'est pas défini, le redémarrage automatique de l'ordinateur est interdit.</p> <p>Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.</p> |
| SKIPPRODUCTCHECK=1 | <p>Désactivation de la recherche de logiciels incompatibles. La liste des applications incompatibles figure dans le fichier incompatible.txt du kit de la distribution. Si le paramètre n'est pas spécifié, l'installation de Kaspersky Endpoint Security est interrompue en cas de détection d'une application incompatible.</p> |
| SKIPPRODUCTUNINSTALL=1 | <p>Interdiction de la suppression automatique de l'application incompatible détectée. Si le paramètre n'est pas spécifié, Kaspersky Endpoint Security tente de supprimer l'application incompatible.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>La suppression automatique des logiciels incompatibles ne peut pas être activée lors de l'installation de Kaspersky Endpoint Security en utilisant le programme d'installation msiexec. Utilisez l'outil setup_kes.exe pour activer le retrait automatique des logiciels incompatibles.</p> </div> |
| KLLOGIN | <p>Définition du nom d'utilisateur pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (module Protection par mot de passe). Le nom d'utilisateur est défini avec les paramètres KLPASSWD et KLPASSWDAREA. Le nom d'utilisateur par défaut est KLAdmin.</p> |
| KLPASSWD | <p>Définition du mot de passe pour l'accès à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (le mot de passe est défini en même temps que les paramètres KLLOGIN et KLPASSWDAREA).</p> <p>Si vous avez indiqué un mot de passe, mais que vous n'avez pas défini le nom d'utilisateur à l'aide du paramètre KLLOGIN, le nom d'utilisateur KLAdmin sera utilisé par défaut.</p> |

| | |
|--------------|--|
| KLPASSWDAREA | <p>Définition de la zone d'action du mot de passe pour l'accès à Kaspersky Endpoint Security. Quand l'utilisateur tente d'exécuter une action depuis cette zone, Kaspersky Endpoint Security demande les identifiants de l'utilisateur (paramètres KLLOGIN et KLPASSWD). Pour indiquer plusieurs valeurs, utilisez le caractère ";" . Valeurs possibles :</p> <ul style="list-style-type: none"> • SET – modification des paramètres de l'application. • EXIT – arrêt de l'application. • DISPROTECT – désactivation des modules de la protection et arrêt des tâches d'analyse. • DISPOLICY – désactivation de la stratégie de Kaspersky Security Center. • UNINST – suppression de l'application de l'ordinateur. • DISCTRL – désactivation des modules de contrôle. • REMOVELIC – suppression de la clé. • REPORTS – consultation des rapports. |
| ENABLETRACES | <p>Activation ou désactivation du traçage de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces après le lancement. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : le traçage est activé. • 0 : le traçage est désactivé (valeur par défaut). |
| TRACESLEVEL | <p>Niveau de détail du traçage Valeurs possibles :</p> <ul style="list-style-type: none"> • 100 (critique). Uniquement les messages relatifs aux erreurs irrémédiables. • 200 (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables. • 300 (diagnostique). Messages relatifs à toutes les erreurs et messages d'avertissement. • 400 (important). Messages relatifs à l'ensemble des erreurs, des avertissements, ainsi que des informations supplémentaires. • 500 (ordinaire). Messages relatifs à l'ensemble des erreurs, avertissements, ainsi que des informations détaillées sur le fonctionnement de l'application en mode normal (valeur par défaut). • 600 (bas). Tous les messages. |
| AMPPL | <p>Activation ou désactivation de la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL (Antimalware</p> |

| | |
|-------------------|---|
| | <p>Protected Process Light). Pour en savoir plus sur la technologie AM-PPL, consultez le site de Microsoft.</p> <p>La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est activée (valeur par défaut). • 0 : la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est désactivée. |
| RESTAPI | <p>Administration de l'application via l'API REST. Pour administrer l'application via l'API REST, vous devez préciser un nom d'utilisateur (paramètre RESTAPI_User).</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : l'administration via l'API REST est autorisée. • 0 : l'administration via l'API REST est interdite (valeur par défaut). <p>Pour administrer l'application via l'API REST, l'administration via les systèmes d'administration doit être autorisée. Pour ce faire, définissez le paramètre AdminKitConnector=1. Si vous administrez l'application via l'API REST, il est impossible de l'administrer via les systèmes d'administration de Kaspersky.</p> |
| RESTAPI_User | <p>Nom d'utilisateur du compte de domaine Windows pour l'administration de l'application via l'API REST. Seul cet utilisateur peut administrer l'application via l'API REST. Saisissez un nom d'utilisateur au format <DOMAIN>\<UserName> (par exemple, RESTAPI_User=COMPANY\Administrator). Vous ne pouvez sélectionner qu'un seul utilisateur pour utiliser l'API REST.</p> <p>L'ajout d'un nom d'utilisateur est une condition indispensable à l'administration de l'application via l'API REST.</p> |
| RESTAPI_Port | <p>Port destiné à l'administration de l'application via l'API REST. Le port 6782 est utilisé par défaut.</p> |
| ADMINKITCONNECTOR | <p>Administration de l'application à l'aide du système d'administration. Les systèmes d'administration désignent, par exemple, Kaspersky Security Center. Outre les systèmes d'administration de Kaspersky, vous pouvez utiliser des solutions d'éditeurs tiers. Pour cela, Kaspersky Endpoint Security propose une API.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : l'administration de l'application via le système d'administration est autorisée (valeur par défaut). • 0 : l'administration de l'application est possible uniquement via l'interface locale. |

Exemple :

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Après l'installation de l'application, Kaspersky Endpoint Security, l'activation selon une licence d'essai est réalisée, si vous n'aviez pas renseigné un code d'activation dans le [fichier setup.ini](#). En général, la durée de validité d'une licence d'essai est brève. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, vous devez l'activer sous une licence commerciale à l'aide de l'[assistant d'activation de l'application](#) ou d'une [commande spéciale](#).

Pendant l'installation de l'application ou la mise à jour de celle-ci en mode silencieux, l'utilisation des fichiers suivants est prise en charge :

- [setup.ini](#) : paramètres généraux d'installation de l'application ;
- [install.cfg](#) : paramètres locaux de l'application Kaspersky Endpoint Security.
- setup.reg : clés du registre.

L'enregistrement des clés de registre du fichier setup.reg dans le registre se réalise uniquement si le fichier [setup.ini](#) affiche la valeur setup.reg pour le paramètre SetupReg. Le fichier setup.reg est créé par les experts de Kaspersky. Il est déconseillé de modifier le contenu de ce fichier.

Pour appliquer les paramètres des fichiers setup.ini, install.cfg et setup.reg, installez ces fichiers dans le dossier contenant le kit de distribution de Kaspersky Endpoint Security. Vous pouvez également placer le fichier setup.reg dans un autre dossier. Dans ce cas, vous devez indiquer le chemin d'accès au fichier dans la commande suivante d'installation de l'application : SETUPREG=<chemin d'accès au fichier setup.reg>.

Installation à distance de l'application à l'aide de System Center Configuration Manager

Ces instructions sont valables pour la version System Center Configuration Manager 2012 R2.

Pour installer l'application à distance à l'aide de System Center Configuration Manager, procédez comme suit :

1. Ouvrez la console Configuration Manager.
2. Dans la partie droite de la console, dans le groupe **Administration des applications** choisissez la section **Paquets**.
3. Dans la partie supérieure de la console, dans le panneau d'administration, cliquez sur le bouton **Créer un paquet**.
L'*Assistant de création de paquets et d'applications* est lancé.
4. Dans l'Assistant de création de paquets et d'applications, procédez comme suit :
 - a. Dans la colonne **Paquet**, procédez comme suit :

- Dans le champ **Nom**, saisissez le nom du paquet d'installation.
- Dans le champ **Dossier d'origine**, indiquez le chemin d'accès au dossier dans lequel se trouve le paquet de distribution de Kaspersky Endpoint Security.

b. Dans la section **Type d'application**, choisissez l'option **Application standard**.

c. Dans la section **Application standard**, procédez comme suit :

- Saisissez dans le champ **Nom** le nom unique du paquet d'installation (par exemple, le nom de l'application avec indication de la version).
- Saisissez dans le champ **Ligne de commande** les paramètres d'installation de Kaspersky Endpoint Security via la ligne de commande.
- Via le bouton **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application.
- Confirmez que vous avez bien choisi l'option **Lancer sous les autorisations d'administrateur** dans la liste **Mode d'exécution**.

d. Dans la section **Exigences**, procédez comme suit :

- Cochez la case **Lancer d'abord une autre application** si vous voulez qu'une autre application soit lancée avant l'installation de Kaspersky Endpoint Security.
Choisissez l'application dans la liste déroulante **Application** ou indiquez le chemin d'accès au fichier exécutable de cette application à l'aide du bouton **Parcourir**.
- Choisissez l'option **Cette application peut être lancée uniquement sur les plateformes indiquées** dans le groupe **Configuration de la plateforme** si vous voulez que l'application soit installée uniquement dans les systèmes d'exploitation indiqués.
Cochez dans la liste les applications en regard des systèmes d'exploitation sur lesquels Kaspersky Endpoint Security doit être installé.

Cette étape est facultative.

e. Dans la section **Synthèse**, vérifiez toutes les valeurs définies des paramètres, puis cliquez sur le bouton **Suivant**.

Le paquet d'installation créé apparaîtra dans la section **Paquets** dans la liste des paquets d'installation disponibles.

5. Dans le menu contextuel du paquet d'installation, choisissez l'option choisissez l'option **Déployer**.

L'Assistant déploiement du logiciel est lancé.

6. Dans l'Assistant de déploiement du logiciel, procédez comme suit :

a. Dans la colonne **Général**, procédez comme suit :

- Dans le champ **Logiciel**, saisissez le nom unique du paquet d'installation ou choisissez le paquet d'installation de la liste à l'aide du bouton **Parcourir**.
- Dans le champ **Collection**, saisissez le nom de la collection d'ordinateurs sur lesquels l'application doit être installée ou sélectionnez cette collection à l'aide du bouton **Parcourir**.

b. dans la section **Contenu**, ajoutez les points de diffusion (pour en savoir plus, consultez la documentation qui accompagne System Center Configuration Manager).

c. Le cas échéant, vous pouvez définir les valeurs des autres paramètres dans l'Assistant de déploiement du logiciel. Ces paramètres sont facultatifs pour l'installation à distance de Kaspersky Endpoint Security.

d. Dans la section **Synthèse**, vérifiez toutes les valeurs définies des paramètres, puis cliquez sur le bouton **Suivant**.

À la fin de l'Assistant de déploiement du logiciel, une tâche d'installation à distance de Kaspersky Endpoint Security sera lancée.

Description des paramètres d'installation dans le fichier setup.ini

Le fichier setup.ini est utilisé dans le cadre de l'installation de l'application via la ligne de commande ou à l'aide de l'éditeur de gestion des stratégies de groupe de Microsoft Windows. Pour appliquer les paramètres du fichier setup.ini, placez le fichier dans le dossier contenant le kit de distribution de Kaspersky Endpoint Security.

 [TÉLÉCHARGER LE FICHIER SETUP.INI](#) 

Le fichier setup.ini comprend les sections suivantes :

- `[Setup]` – paramètres généraux d'installation de l'application.
- `[Components]` – sélection des modules de l'application à installer. Si aucun module n'a été désigné, tous les modules disponibles pour le système d'exploitation sont installés. La Protection contre les fichiers malicieux est un module obligatoire qui est installé sur l'ordinateur, quels que soient les paramètres définis dans ce groupe. Le module Managed Detection and Response ne figure pas non plus dans cette section. Pour installer ce module, vous devez [activer le module Managed Detection and Response dans Kaspersky Security Center Console](#).
- `[Tasks]` – sélection des tâches à ajouter à la liste des tâches de Kaspersky Endpoint Security. Si aucune tâche n'est désignée, toutes les tâches sont reprises dans la liste des tâches de Kaspersky Endpoint Security.

À la place de la valeur 1, les valeurs `yes`, `on`, `enable`, `enabled` peuvent être utilisées.

Les valeurs `no`, `off`, `disable`, `disabled` peuvent être utilisées à la place de la valeur 0.

Paramètres du fichier setup.ini

| Section | Paramètre | Description |
|----------------------|-----------------------------|---|
| <code>[Setup]</code> | <code>InstallDir</code> | Chemin d'accès au dossier d'installation de l'application. |
| | <code>ActivationCode</code> | Code d'activation de Kaspersky Endpoint Security. |
| | <code>EULA=1</code> | Acceptation des dispositions du Contrat de licence Utilisateur final. Le texte Contrat de licence utilisateur final fait partie de la distribution de Kaspersky Endpoint Security . <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">L'acceptation des dispositions du contrat de licence Utilisateur final est une condition indispensable pour installer l'application ou pour la mettre à jour.</div> |

| | | |
|--|-----------------|--|
| | PrivacyPolicy=1 | <p>Acceptation de la Politique de confidentialité. Le texte de la Politique de confidentialité fait partie du kit de distribution de Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.</p> </div> |
| | KSN | <p>Participation ou non au Kaspersky Security Network (KSN). Si le paramètre n'est pas précisé, Kaspersky Endpoint Security sollicitera la confirmation de la participation à KSN au premier lancement de l'application. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : acceptation de la participation à KSN. • 0 : refus de la participation à KSN (valeur par défaut). <p>Le paquet de distribution de Kaspersky Endpoint Security est optimisé pour l'utilisation de Kaspersky Security Network. Si vous avez refusé de participer au Kaspersky Security Network, mettez à jour Kaspersky Endpoint Security directement à l'issue de l'installation.</p> |
| | Login | <p>Définition du nom d'utilisateur pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (module Protection par mot de passe). Le nom d'utilisateur est défini avec les paramètres Password et PasswordArea. Le nom d'utilisateur par défaut est KLAdmin.</p> |
| | Mot de passe | <p>Définition du mot de passe pour l'accès à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (le mot de passe est défini en même temps que les paramètres Login et PasswordArea).</p> <p>Si vous avez indiqué un mot de passe, mais que vous n'avez pas défini le nom d'utilisateur à l'aide du paramètre Login, le nom d'utilisateur KLAdmin sera utilisé par défaut.</p> |
| | PasswordArea | <p>Définition de la zone d'action du mot de passe pour l'accès à Kaspersky Endpoint Security. Quand l'utilisateur tente d'exécuter une action à partir de cette zone, Kaspersky Endpoint Security demande les identifiants de l'utilisateur (paramètres Identifiant et Mot de passe). Pour indiquer plusieurs valeurs, utilisez le caractère ";" ". Valeurs possibles :</p> <ul style="list-style-type: none"> • SET – modification des paramètres de l'application. • EXIT – arrêt de l'application. • DISPROTECT – désactivation des modules de la protection et arrêt des tâches d'analyse. |

| | | |
|--|----------------|---|
| | | <ul style="list-style-type: none"> • DISPOLICY – désactivation de la stratégie de Kaspersky Security Center. • UNINST – suppression de l'application de l'ordinateur. • DISCTRL – désactivation des modules de contrôle. • REMOVELIC – suppression de la clé. • REPORTS – consultation des rapports. |
| | SelfProtection | <p>Activation ou désactivation du mécanisme de protection de l'installation de l'application. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : le mécanisme de protection de l'installation de l'application est activé (valeur par défaut). • 0 – désactivation du mécanisme de protection de l'installation de l'application. <p>La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Endpoint Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop).</p> |
| | Reboot=1 | <p>Redémarrage automatique de l'ordinateur après l'installation ou la mise à jour de l'application, le cas échéant. Si le paramètre n'est pas défini, le redémarrage automatique de l'ordinateur est interdit.</p> <p>Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.</p> |
| | AddEnvironment | <p>Ajout dans la variable système %PATH% du chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 – ajouter à la variable système %PATH% le chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security. • 0 – le chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security n'est pas ajouté à la variable système %PATH%. |

| | | |
|--------------|--|--|
| AMPPL | | <p>Activation ou désactivation de la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL (Antimalware Protected Process Light). Pour en savoir plus sur la technologie AM-PPL, consultez le site de Microsoft.</p> <p>La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019.</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est activée (valeur par défaut). • 0 : la protection des processus de Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est désactivée. |
| SetupReg | | <p>Activation de l'enregistrement des clés du registre du fichier setup.reg dans le registre. Le paramètre SetupReg prend la valeur : setup.reg.</p> |
| EnableTraces | | <p>Activation ou désactivation du traçage de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces après le lancement. Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : le traçage est activé. • 0 : le traçage est désactivé (valeur par défaut). |
| TracesLevel | | <p>Niveau de détail du traçage Valeurs possibles :</p> <ul style="list-style-type: none"> • 100 (critique). Uniquement les messages relatifs aux erreurs irrémédiables. • 200 (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables. • 300 (diagnostique). Messages relatifs à toutes les erreurs et messages d'avertissement. • 400 (important). Messages relatifs à l'ensemble des erreurs, des avertissements, ainsi que des informations supplémentaires. • 500 (ordinaire). Messages relatifs à l'ensemble des erreurs, avertissements, ainsi que des informations détaillées sur le fonctionnement de l'application en mode normal (valeur par défaut). • 600 (bas). Tous les messages. |
| RESTAPI | | <p>Administration de l'application via l'API REST. Pour administrer l'application via l'API REST, vous devez</p> |

| | | |
|--------------|--------------------------|---|
| | | <p>préciser un nom d'utilisateur (paramètre RESTAPI_User).</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> • 1 : l'administration via l'API REST est autorisée. • 0 : l'administration via l'API REST est interdite (valeur par défaut). <p>Pour administrer l'application via l'API REST, l'administration via les systèmes d'administration doit être autorisée. Pour ce faire, définissez le paramètre AdminKitConnector=1. Si vous administrez l'application via l'API REST, il est impossible de l'administrer via les systèmes d'administration de Kaspersky.</p> |
| | RESTAPI_User | <p>Nom d'utilisateur du compte de domaine Windows pour l'administration de l'application via l'API REST. Seul cet utilisateur peut administrer l'application via l'API REST. Saisissez un nom d'utilisateur au format <DOMAIN>\<UserName> (par exemple, RESTAPI_User=COMPANY\Administrator). Vous ne pouvez sélectionner qu'un seul utilisateur pour utiliser l'API REST.</p> <p>L'ajout d'un nom d'utilisateur est une condition indispensable à l'administration de l'application via l'API REST.</p> |
| | RESTAPI_Port | <p>Port destiné à l'administration de l'application via l'API REST. Le port 6782 est utilisé par défaut.</p> |
| [Components] | ALL | <p>Installation de tous les modules. Si vous attribuez la valeur 1 au paramètre, tous les modules seront installés, quels que soient les paramètres d'installation des modules séparés.</p> |
| | MailThreatProtection | <p>Protection contre les menaces par emails.</p> |
| | WebThreatProtection | <p>Protection contre les menaces Internet.</p> |
| | AMSI | <p>Protection AMSI.</p> |
| | HostIntrusionPrevention | <p>Prévention des intrusions.</p> |
| | BehaviorDetection | <p>Détection comportementale.</p> |
| | ExploitPrevention | <p>Protection contre les Exploits.</p> |
| | RemediationEngine | <p>Réparation des actions malicieuses.</p> |
| | Firewall | <p>Pare-feu.</p> |
| | NetworkThreatProtection | <p>Protection contre les menaces réseau.</p> |
| | WebControl | <p>Contrôle Internet.</p> |
| | DeviceControl | <p>Contrôle des appareils.</p> |
| | ApplicationControl | <p>Contrôle des applications.</p> |
| | AdaptiveAnomaliesControl | <p>Contrôle évolutif des anomalies.</p> |
| | FileEncryption | <p>Bibliothèques pour le chiffrement des fichiers.</p> |

| | | |
|---------|------------------------|--|
| | DiskEncryption | Bibliothèques pour le chiffrement du disque. |
| | BadUSBAttackPrevention | Protection BadUSB. |
| | AntiAPT | Endpoint Agent. <i>Endpoint Agent</i> installe l'application Kaspersky Endpoint Agent 3.10 pour garantir l'interaction entre l'application et les solutions de Kaspersky conçues pour détecter les menaces complexes (par exemple, Kaspersky Sandbox). |
| | AdminKitConnector | Administration de l'application à l'aide du système d'administration. Les systèmes d'administration désignent, par exemple, Kaspersky Security Center. Outre les systèmes d'administration de Kaspersky, vous pouvez utiliser des solutions d'éditeurs tiers. Pour cela, Kaspersky Endpoint Security propose une API. Valeurs possibles : <ul style="list-style-type: none"> • 1 : l'administration de l'application via le système d'administration est autorisée (valeur par défaut). • 0 : l'administration de l'application est possible uniquement via l'interface locale. |
| [Tasks] | ScanMyComputer | Tâche d'analyse complète. Valeurs possibles : <ul style="list-style-type: none"> • 1 – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • 0 – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security. |
| | ScanCritical | Tâche d'analyse rapide. Valeurs possibles : <ul style="list-style-type: none"> • 1 – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • 0 – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security. |
| | Updater | Tâche de mise à jour. Valeurs possibles : <ul style="list-style-type: none"> • 1 – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • 0 – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security. |

Modification de la sélection des modules de l'application

Lors de l'installation de l'application, vous pouvez sélectionner les modules qui seront disponibles. Vous pouvez modifier la composition de l'application des manières suivantes :

- Localement à l'aide de l'Assistant d'installation de l'application.

La modification de la composition de l'application s'opère de manière traditionnelle pour le système d'exploitation Windows, à savoir via le Panneau de configuration. Exécutez l'assistant d'installation de l'application et sélectionnez l'opération de modification de la composition des modules de l'application. Suivez les instructions à l'écran.

- À distance via Kaspersky Security Center.

Pour modifier la sélection des modules de Kaspersky Endpoint Security après l'installation de l'application, utilisez la tâche *Modification de la sélection des modules de l'application*.

La modification de la composition de l'application présente les caractéristiques suivantes :

- [Certains modules de Kaspersky Endpoint Security](#) (par exemple, le Contrôle évolutif des anomalies) ne peuvent être installés sur les ordinateurs tournant sous Windows Server.
- Si les disques durs de votre ordinateur sont protégés par [le chiffrement complet du disque \(FDE\)](#), vous ne pouvez pas supprimer le module Chiffrement du disque. Pour supprimer le module Chiffrement du disque, déchiffrez tous les disques durs de l'ordinateur.
- Si l'ordinateur contient [des fichiers chiffrés \(FLE\)](#) ou si l'utilisateur utilise [des lecteurs amovibles chiffrés \(FDE ou FLE\)](#), il ne sera plus possible d'accéder aux fichiers et aux disques amovibles après la suppression des modules de chiffrement des données. Pour accéder aux fichiers et aux lecteurs amovibles, il faudra réinstaller les modules de chiffrement des données.

[Procédure d'ajout ou de suppression de modules de l'application dans la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Sélectionnez **Kaspersky Endpoint Security for Windows (11.6.0)** → **Modification de la sélection des modules de l'application**.

Étape 2. Paramètres de la tâche de modification des modules de l'application

Choisissez les modules de l'application qui seront accessibles sur l'ordinateur.

Cochez la case **Supprimer les applications incompatibles d'éditeurs tiers**. La liste des applications incompatibles figure dans le fichier `incompatible.txt`, repris dans [le kit de distribution](#). Si des applications incompatibles sont présentes sur l'ordinateur, l'installation de Kaspersky Endpoint Security se solde sur une erreur.

Le cas échéant, activez la [protection par mot de passe](#) pour l'exécution de la tâche :

1. Cliquez sur le bouton **Avancé**.

2. Cochez la case **Utiliser le mot de passe pour modifier la sélection de modules**.

3. Saisissez les informations d'identification d'utilisateur KLAdmin.

Étape 3. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 4. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 5. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple, Ajout du module Contrôle des applications.

Étape 6. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Cette action entraîne la modification de la sélection de modules de Kaspersky Endpoint Security sur les ordinateurs des utilisateurs en mode silencieux. Les paramètres des modules accessibles apparaissent dans l'interface locale de l'application. Les modules qui n'ont pas été sélectionnés pour l'application sont désactivés et leurs paramètres ne sont pas accessibles.

[Procédure d'ajout et de suppression de modules de l'application dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

2. Dans la liste **Type de tâche**, choisissez **Modification de la sélection des modules de l'application**.

3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, Ajout du module Contrôle des applications.

4. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

Étape 2. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Par exemple, sélectionnez un groupe d'administration distinct ou effectuez une sélection.

Étape 3. Fin de la création de la tâche

Cochez la case **Ouvrir la fenêtre des propriétés de la tâche après sa création** et quittez l'assistant. Dans les propriétés de la tâche, sélectionnez l'onglet **Paramètres de l'application** et sélectionnez les modules de l'application qui seront disponibles.

Le cas échéant, activez la [protection par mot de passe](#) pour l'exécution de la tâche :

1. Dans la section **Paramètres avancés**, cochez la case **Utiliser le mot de passe pour modifier la sélection de modules**.

2. Saisissez les informations d'identification d'utilisateur KLAdmin.

Enregistrez les modifications et exécutez la tâche.

Cette action entraîne la modification de la sélection de modules de Kaspersky Endpoint Security sur les ordinateurs des utilisateurs en mode silencieux. Les paramètres des modules accessibles apparaissent dans l'interface locale de l'application. Les modules qui n'ont pas été sélectionnés pour l'application sont désactivés et leurs paramètres ne sont pas accessibles.

Mise à jour de la version précédente de l'application

La mise à jour de la version précédente de l'application présente les caractéristiques suivantes :

- Kaspersky Endpoint Security 11.6.0 est compatible avec Kaspersky Security Center 12.
- Avant de commencer la mise à jour de l'application, il est conseillé de fermer toutes les applications en cours d'exécution.
- Si les disques durs de l'ordinateur ont été soumis au [chiffrement du disque](#), il faudra les déchiffrer tous avant de réaliser la mise à niveau depuis Kaspersky Endpoint Security de la version 10 vers la version 11.0.0 et versions ultérieures.

Avant la mise à niveau, Kaspersky Endpoint Security bloque la fonctionnalité de chiffrement du disque. En cas d'échec du blocage de la fonction de chiffrement du disque, l'installation de la mise à jour n'est pas lancée. Après la mise à jour de l'application, la fonction de chiffrement du disque est restaurée.

Kaspersky Endpoint Security prend en charge la mise à jour des versions suivantes de l'application :

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (version 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (version 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (version 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (version 11.0.0.6499).
- Kaspersky Endpoint Security for Windows 11.0.1 (version 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (version 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (version 11.1.0.15919).
- Kaspersky Endpoint Security for Windows 11.1.1 (version 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (version 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (version 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (version 11.3.0.773).
- Kaspersky Endpoint Security for Windows 11.4.0 (version 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (version 11.5.0.590).

Lors de la mise à niveau de Kaspersky Endpoint Security 10 Service Pack 2 for Windows jusqu'à Kaspersky Endpoint Security for Windows 11.6.0, les fichiers placés dans la Sauvegarde et dans la Quarantaine de la version antérieure de l'application sont transférés dans la nouvelle version. Pour les versions de Kaspersky Endpoint Security antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows, le transfert des fichiers placés dans la sauvegarde ou dans la quarantaine dans la version antérieure de l'application n'a pas lieu.

Il existe plusieurs méthodes pour mettre à jour l'application Kaspersky Endpoint Security sur un ordinateur :

- localement à l'aide de l'[Assistant d'installation de l'application](#).
- localement via la [ligne de commande](#).
- à distance via [Kaspersky Security Center 12](#).
- à distance via l'éditeur de gestion de stratégies de groupe Microsoft Windows (pour en savoir plus, consultez le [site de l'assistance technique de Microsoft](#)).
- à distance à l'aide de [System Center Configuration Manager](#).

Si une application avec un ensemble de modules autre que l'ensemble par défaut est déployé sur le réseau de l'organisation, la mise à jour de l'application via la console d'administration (MMC) diffère de la mise à jour de l'application via Web Console et Cloud Console. La mise à jour de Kaspersky Endpoint Security possède les particularités suivantes :

- Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console.

Si vous avez créé un paquet d'installation pour une nouvelle version de l'application avec l'ensemble de modules par défaut, l'ensemble de modules sur l'ordinateur de l'utilisateur ne sera pas modifié après la mise à jour. Pour utiliser Kaspersky Endpoint Security avec l'ensemble de modules par défaut, vous devez [ouvrir les propriétés du paquet d'installation](#), modifier l'ensemble de modules, rétablir l'ensemble de modules à son état d'origine et enregistrer les modifications.

- Console d'administration de Kaspersky Security Center.

L'ensemble de modules de l'application après la mise à jour correspondra à l'ensemble de modules du paquet d'installation. Autrement dit, si la nouvelle version de l'application utilise l'ensemble de modules par défaut, alors, par exemple, le module Protection BadUSB sera supprimé de l'ordinateur, car ce module est exclu de l'ensemble par défaut. Pour continuer à utiliser l'application avec le même ensemble de modules, vous devez sélectionner les modules nécessaires dans les [paramètres du paquet d'installation](#).

Suppression de l'application

Suite à la suppression de Kaspersky Endpoint Security l'ordinateur et les données de l'utilisateur ne seront plus protégés.

La suppression de l'application Kaspersky Endpoint Security d'un ordinateur peut s'opérer des manières suivantes :

- localement à l'aide de l'[Assistant d'installation de l'application](#) ;
- localement via la [ligne de commande](#) ;
- à distance à l'aide de Kaspersky Security Center (pour en savoir plus, consultez l'[aide de Kaspersky Security Center](#)) ;

- à distance via l'éditeur de gestion de stratégies de groupe Microsoft Windows (pour en savoir plus, consultez le [site de l'assistance technique de Microsoft](#)).

Si vous avez sélectionné le module Endpoint Agent lors de l'installation de l'application, les deux applications suivantes seront installées sur l'ordinateur : Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Après la suppression de Kaspersky Endpoint Security, l'application Kaspersky Endpoint Agent est également supprimée automatiquement.

Suppression via Kaspersky Security Center

Vous pouvez supprimer une application à distance à l'aide de la tâche *Désinstallation à distance de l'application*. Dans le cadre de cette tâche, Kaspersky Endpoint Security télécharge sur l'ordinateur un utilitaire de suppression de l'application. Une fois l'application supprimée, l'utilitaire est supprimé automatiquement.

[Procédure de suppression d'une application via la Console d'administration \(MMC\)](#)

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Sélectionnez **Serveur d'administration de Kaspersky Security Center** → **Avancé** → **Suppression de l'application à distance**.

Étape 2. Sélection de l'application à supprimer

Sélectionnez **Supprimer une application prise en charge par Kaspersky Security Center**.

Étape 3. Paramètres de suppression de l'application

Choisissez **Kaspersky Endpoint Security for Windows (11.6.0)**.

Étape 4. Paramètres de l'utilitaire de désinstallation

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le chargement de l'utilitaire de désinstallation.** Sélectionnez les modes de livraison des utilitaires :
 - **À l'aide de l'Agent d'administration.** Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est supprimé à l'aide de l'Agent d'administration.
 - **À l'aide des outils de Microsoft Windows à l'aide d'un Serveur d'administration.** Les utilitaires sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.
 - **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution.** L'utilitaire est transmis aux ordinateurs client à l'aide des outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, *consultez [l'aide de Kaspersky Security Center](#)*.
- **Vérifier préalablement la version du système d'exploitation.** Si nécessaire, décochez cette case. Cela permet d'éviter le téléchargement de l'utilitaire de suppression si le système d'exploitation de l'ordinateur ne répond pas à la configuration logicielle requise. Si vous êtes certain que le système d'exploitation est conforme à la configuration logicielle requise, vous pouvez ignorer cette vérification.

Si l'opération de suppression de l'application [est protégée par un mot de passe](#), procédez comme suit :

1. Cochez la case **Utiliser le mot de passe de suppression**.

2. Cliquez sur le bouton **Modifier**.

3. Saisissez le mot de passe du compte utilisateur KLAdmin.

Étape 5. Sélection du paramètre de redémarrage du système d'exploitation

Il faut redémarrer l'ordinateur après la suppression de l'application. Sélectionnez l'action qui sera exécutée pour redémarrer l'ordinateur.

Étape 6. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 7. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour supprimer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 8. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 9. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple `Suppression de Kaspersky Endpoint Security 11.6.0`.

Étape 10. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

L'application est supprimée en mode silencieux.

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste **Application**, choisissez **Kaspersky Security Center**.

2. Dans la liste déroulante **Type de tâche**, choisissez **Suppression à distance de l'application**.

3. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple **Suppression de Kaspersky Endpoint Security sur les ordinateurs du Support Technique**.

4. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

Étape 2. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Par exemple, sélectionnez un groupe d'administration distinct ou effectuez une sélection.

Étape 3. Configuration des paramètres de suppression de l'application

Configurez les paramètres complémentaires de suppression de l'application à cette étape :

1. Sélectionnez le type **Supprimer une application administrée**.

2. Choisissez **Kaspersky Endpoint Security for Windows (11.6.0)**.

3. **Forcer le chargement de l'utilitaire de désinstallation**. Sélectionnez les modes de livraison des utilitaires :

- **À l'aide de l'Agent d'administration**. Si l'Agent d'administration n'est pas installé sur l'ordinateur, il faut l'installer à l'aide des outils du système d'exploitation. Ensuite, Kaspersky Endpoint Security est supprimé à l'aide de l'Agent d'administration.
- **À l'aide des outils de Microsoft Windows à l'aide d'un Serveur d'administration**. Les utilitaires sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.
- **À l'aide des outils du système d'exploitation avec l'assistance de points de distribution**. L'utilitaire est transmis aux ordinateurs client à l'aide des outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez [l'aide de Kaspersky Security Center](#).

4. Dans le champ **Nombre maximum de téléchargements simultanés**, définissez la limite du nombre de requêtes adressées au Serveur d'administration pour le téléchargement de l'utilitaire de suppression de l'application. La restriction des demandes permet d'éviter la surcharge du réseau.
5. Définissez dans le champ **Nombre de tentatives de suppression** la limite de tentatives de suppression de l'application. Si la suppression de Kaspersky Endpoint Security se solde sur une erreur, la tâche lance à nouveau la suppression automatiquement.
6. Le cas échéant, décochez la case **Vérifier préalablement la version du système d'exploitation**. Cela permet d'éviter le téléchargement de l'utilitaire de suppression si le système d'exploitation de l'ordinateur ne répond pas à la configuration logicielle requise. Si vous êtes certain que le système d'exploitation est conforme à la configuration logicielle requise, vous pouvez ignorer cette vérification.

Étape 4. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'assistant d'installation utilise le compte utilisateur suivant. Pour supprimer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches.

Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. L'application est supprimée en mode silencieux. Une fois la suppression terminée, Kaspersky Endpoint Security affiche une demande de redémarrage de l'ordinateur.

Si l'opération de suppression de l'application [est protégée par un mot de passe](#), saisissez le mot de passe du compte KLAdmin dans les propriétés de la tâche *Suppression à distance de l'application*. Sans mot de passe, la tâche ne pourra pas être exécutée.

Pour utiliser le mot de passe du compte utilisateur KLAdmin dans la tâche Suppression de l'application à distance, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.
La liste des tâches s'ouvre.
2. Cliquez sur la tâche de Kaspersky Security Center **Suppression de l'application à distance**.
La fenêtre des propriétés de la tâche s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Cochez la case **Utiliser le mot de passe de suppression**.
5. Saisissez le mot de passe du compte utilisateur KLAdmin.
6. Cliquez sur le bouton **Enregistrer**.

Suppression de l'application à l'aide de l'assistant

La suppression de Kaspersky Endpoint Security s'opère de manière traditionnelle pour le système d'exploitation Windows, à savoir via le Panneau de configuration. L'Assistant d'installation de l'application sera lancé. Suivez les instructions à l'écran.

Vous pouvez indiquer les données de l'application que vous voulez enregistrer en vue d'une utilisation ultérieure lors de la réinstallation de l'application (par exemple, sa version plus récente). Si vous n'indiquez aucune donnée, l'application sera complètement supprimée.

Vous pouvez conserver les données suivantes :

- **Informations sur l'activation** : données qui annulent la nécessité d'activer à nouveau l'application à l'avenir. Kaspersky Endpoint Security ajoute automatiquement une clé de licence si la clé est toujours valide au moment de l'installation.
- **Fichiers de la sauvegarde** : fichiers analysés par l'application et placés dans la Sauvegarde.

L'accès aux fichiers de la Sauvegarde qui ont conservés après la suppression de l'application ne peut être octroyé que par la version de l'application utilisée pour leur sauvegarde.

Si vous souhaitez continuer à utiliser les objets de la sauvegarde après la suppression de l'application, vous devez les restaurer avant la suppression de l'application. Toutefois, les experts de Kaspersky déconseillent de restaurer les objets de la Sauvegarde, car ils peuvent endommager votre ordinateur.

- **Paramètres de fonctionnement de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.
- **Stockage local des clés de chiffrement** : données qui garantissent un accès direct aux fichiers et disques chiffrés avant la suppression de l'application. Pour accéder aux fichiers et aux disques chiffrés, confirmez que vous avez sélectionné la fonctionnalité de chiffrement des données lors de la réinstallation de Kaspersky Endpoint Security. Aucune étape supplémentaire n'est requise pour accéder à des fichiers et des disques chiffrés antérieurement.

Suppression de l'application via la ligne de commande

La suppression de Kaspersky Endpoint Security for Windows via la ligne de commande peut être réalisée d'une des manières suivantes :

- en mode interactif à l'aide de l'Assistant d'installation de l'application.
- En mode silencieux. Une fois que vous aurez lancé la suppression en mode silencieux, vous n'aurez plus à intervenir dans la suppression. Pour supprimer l'application en mode silencieux, utilisez les arguments /s et /qn.

Pour supprimer l'application en mode silencieux, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.

2. Accédez au dossier dans lequel se trouve le paquet de distribution Kaspersky Endpoint Security.

3. Exécutez la commande :

- Si la suppression n'est pas [protégée par un mot de passe](#) :

```
setup_ks.exe /s /x
```

ou

```
msiexec.exe /x <GUID> /qn
```

où <GUID> représente l'identifiant unique de l'application. Vous pouvez obtenir le GUID d'une application à l'aide de la commande :

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber.
```

- Si la suppression [est protégée par un mot de passe](#) :

```
setup_ks.exe /pKLLOGIN=<nom d'utilisateur> /pKLPASSWD=<mot de passe> /s /x
```

ou

```
msiexec.exe /x <GUID> KLLOGIN=<nom d'utilisateur> KLPASSWD=<mot de passe> /qn
```

Exemple :

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```


Licence de l'application

Cette section présente les notions principales relatives à la licence de l'application.

À propos du Contrat de licence

Le *Contrat de licence utilisateur final* est un accord juridique conclu entre vous et AO Kaspersky Lab qui prévoit les conditions d'utilisation du logiciel que vous avez acheté.

Lisez attentivement les conditions du Contrat de licence Utilisateur final avant de commencer à utiliser l'application.

Vous pouvez prendre connaissance des conditions du Contrat de licence Utilisateur final, en utilisant les moyens suivants :

- Pendant [l'installation de Kaspersky Endpoint Security en mode interactif](#).
- en lisant le document license.txt. Ce document est repris dans la [distribution de l'application](#) et se trouve également dans le dossier d'installation de l'application %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\<<locale>\KES.

Vous acceptez les conditions du contrat de licence Utilisateur final, en confirmant votre accord avec le texte du contrat de licence Utilisateur final lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence Utilisateur final, vous devez interrompre l'installation de l'application.

À propos de la licence

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence Utilisateur final.

La licence vous accorde le droit d'obtenir les types de service suivants :

- Utilisation de l'application conformément aux dispositions du Contrat de licence Utilisateur final
- Support Technique

Le volume de services offert et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Les types de licence suivants sont proposés :

- *Evaluation* : une licence gratuite conçue pour découvrir l'application.
En général, la durée de validité d'une licence d'essai est brève. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.
Vous ne pouvez activer l'application avec une licence d'essai qu'une seule fois.
- *Commerciale* : licence payante octroyée à l'achat de l'application.

Les fonctionnalités de l'application accessibles via la licence commerciale varient en fonction de la sélection du produit. Le produit choisi figure dans le [Certificat de licence](#). Les informations sur les produits disponibles sont reprises sur le [site de Kaspersky](#).

Lorsque la licence commerciale expire, les fonctionnalités clés de l'application sont désactivées. Pour continuer à utiliser l'application, vous devez renouveler votre licence commerciale. Si vous ne prévoyez pas de renouveler votre licence, vous devez supprimer l'application de votre ordinateur.

À propos du certificat de licence

Le *certificat de licence* est un document que vous recevez en même temps que le fichier clé et le code d'activation.

Il reprend les informations suivantes relatives à la licence octroyée :

- la clé de licence ou le numéro de commande ;
- les informations relatives à l'utilisateur qui a obtenu la licence ;
- les informations relatives à l'application qu'il faut activer à l'aide de la licence octroyée ;
- les restrictions sur le nombre d'unités couvertes par la licence (par exemple, les appareils sur lesquels l'utilisation de l'application sous la licence octroyée est autorisée) ;
- la date de début de validité de la licence ;
- la date de fin de la durée de validité de la licence ou la durée de validité de la licence ;
- le type de licence.

À propos de l'abonnement

L'*abonnement à Kaspersky Internet Security* constitue une commande pour l'utilisation de l'application selon des paramètres sélectionnés (date d'expiration, nombre d'appareils protégés). Il est possible d'enregistrer un abonnement à Kaspersky Endpoint Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur Internet). L'abonnement peut être renouvelé manuellement ou automatiquement. Il peut également être refusé. L'administration de l'abonnement est accessible sur le site Internet du fournisseur de services.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour prolonger l'action de Kaspersky Endpoint Security après la date d'expiration d'un abonnement limité, il est nécessaire de renouveler ce dernier. L'abonnement illimité se renouvelle automatiquement selon les conditions en vigueur au moment du paiement au prestataire de services.

Si l'abonnement est limité, une période de grâce de renouvellement vous est proposée après sa date d'expiration. Pendant cette période, l'application continue à fonctionner. C'est le fournisseur du service qui détermine l'existence et la durée de cette période de grâce.

Pour utiliser Kaspersky Endpoint Security sur abonnement, il faut saisir le [code d'activation](#) fourni par le prestataire de services. Une fois que le code d'activation est appliqué, la clé active est ajoutée. La clé active détermine la licence d'utilisation de l'application dans le cadre de l'abonnement. Il n'est pas possible d'ajouter une clé de licence de réserve par abonnement.

Les codes d'activation achetés par abonnement ne peuvent pas être utilisés pour l'activation de versions antérieures de Kaspersky Endpoint Security.

À propos de la clé de licence

La *clé de licence* est une séquence de bits qui vous permet d'activer, puis d'utiliser l'application conformément aux dispositions du Contrat de licence.

Pour une clé installée selon un abonnement, le [certificat de licence](#) n'est pas proposé.

Vous pouvez ajouter une clé de licence à l'application d'une des manières suivantes : appliquer un fichier clé ou saisir un code d'activation.

La clé peut être bloquée par Kaspersky en cas de non-respect du Contrat de licence Utilisateur final. Si la clé est bloquée, il faudra ajouter une autre clé pour utiliser l'application.

Une clé peut être active ou de réserve.

La *clé active* est la clé actuellement utilisée pour faire fonctionner l'application. Une licence d'essai ou une licence commerciale peuvent être ajoutées au titre de clé active. L'application ne peut compter qu'une seule clé active.

Une *clé de licence de réserve* est une clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée pour le moment. Lors de l'expiration de la clé active, la clé de licence de réserve devient automatiquement active. La clé de licence de réserve ne peut être ajoutée que si une clé active existe déjà.

La clé d'une licence d'évaluation ne peut être ajoutée qu'en tant que clé active. Elle ne peut en aucun cas servir de clé de licence de réserve. La clé de la licence d'évaluation ne peut en aucun cas remplacer la clé active d'une licence commerciale.

Si une clé est ajoutée à la liste des clés interdites, les fonctionnalités de l'application définies par la [licence utilisée pour activer l'application](#) restent accessibles pendant huit jours. L'application informe l'utilisateur que la clé a été ajoutée à la liste des clés interdites. Après huit jours, l'application fonctionne comme quand la licence a expiré. Vous pouvez utiliser les modules de la protection et de contrôle et lancer une analyse à l'aide des bases de l'application installées avant l'expiration de la durée de validité de la licence. De plus, le chiffrement sera toujours appliqué aux modifications des fichiers chiffrés avant l'expiration de la licence. Par contre, l'application ne chiffre pas les nouveaux fichiers. L'utilisation de Kaspersky Security Network n'est pas disponible.

À propos du code d'activation

Un *code d'activation* est une séquence unique de 20 caractères alphanumériques. Vous saisissez un code d'activation pour ajouter une clé de licence qui active Kaspersky Endpoint Security. Vous recevrez un code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Endpoint Security.

L'activation de l'application à l'aide du code d'activation requiert l'accès à Internet afin de pouvoir contacter les serveurs d'activation de Kaspersky.

L'activation de l'application à l'aide d'un code d'activation entraîne l'ajout d'une clé active. Il est possible d'installer une clé de licence de réserve uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé.

Si vous perdez le code d'activation après l'activation de l'application, vous pouvez le récupérer. Le code d'activation est nécessaire pour ouvrir un [Kaspersky CompanyAccount](#), par exemple. Si le code d'activation a été perdu après l'activation de l'application, contactez le partenaire Kaspersky auprès duquel vous avez acheté la licence.

À propos du fichier clé

Un *fichier clé* est un fichier portant l'extension key que Kaspersky vous fournit. Le fichier clé permet d'ajouter une clé de licence pour activer l'application.

Vous recevez le fichier clé à l'adresse e-mail que vous avez indiquée après l'achat de Kaspersky Endpoint Security ou après la commande d'une version d'essai de Kaspersky Endpoint Security.

Pour activer l'application à l'aide du fichier clé, il n'est pas nécessaire de se connecter aux serveurs d'activation de Kaspersky.

En cas de suppression accidentelle du fichier clé, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer un fichier clé, réalisez une des actions suivantes :

- Contacter le vendeur de la licence.
- Obtenir un fichier clé sur le [site Internet de Kaspersky](#) sur la base du code d'activation en votre possession.

L'activation de l'application à l'aide d'un fichier clé entraîne l'ajout d'une clé active. Il est possible d'installer une clé de licence de réserve uniquement à l'aide d'un fichier clé et non pas à l'aide d'un code d'activation.

Activation de l'application

L'*activation* est une procédure qui consiste à insérer un code dans le logiciel Kaspersky afin d'en activer sa [licence](#). Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence. L'activation de l'application consiste à ajouter une [clé de licence](#).

Vous pouvez activer l'application selon un des modes suivants :

- Localement, à partir de l'interface de l'application, en utilisant l'[Assistant d'activation](#), vous pouvez ajouter la clé active et la clé de réserve de cette façon.
- À distance via la [suite Kaspersky Security Center](#) et la création, puis l'exécution d'une tâche d'ajout de clé de licence. De cette façon, vous pouvez ajouter la clé active et la clé de licence de réserve.
- À distance via la diffusion sur les postes clients de fichiers clés et de codes d'activation placés dans le stockage des clés du Serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur la diffusion des clés, consultez l'[aide de Kaspersky Security Center](#). De cette façon, vous pouvez ajouter la clé active et la clé de licence de réserve.

Le code d'activation acheté par abonnement est utilisé en priorité.

- Via la [ligne de commande](#).

Lors de l'activation à distance de l'application ou lors de l'activation de l'application en mode silencieux à l'aide du code d'activation, un retard aléatoire lié à la diffusion de la charge sur les serveurs d'activation de Kaspersky est possible. Pour une installation immédiate du programme, vous pouvez interrompre l'activation en cours et lancer l'activation de l'application via l'assistant d'activation de l'application.

Activation de l'application via Kaspersky Security Center

Vous pouvez activer l'application à distance via Kaspersky Security Center d'une des façons suivantes :

- Avec l'aide de la tâche *Ajouter une clé*.

Ce mode permet d'ajouter une clé sur un ordinateur concret ou sur des ordinateurs appartenant à un groupe d'administration.

- Via la diffusion sur les ordinateurs de la clé, conservée dans le Serveur d'administration de Kaspersky Security Center.

Ce moyen permet d'ajouter automatiquement a clé sur des ordinateurs déjà connecté à Kaspersky Security Center, ainsi que sur les nouveaux ordinateurs. Pour pouvoir utiliser ce moyen, il faut d'abord ajouter la clé dans le Serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur l'ajout de clés dans le Serveur d'administration de Kaspersky Security Center, consultez l'[aide de Kaspersky Security Center](#).

Une version d'essai est prévue pour Kaspersky Security Center Cloud Console. *La version d'essai* est une version spéciale de Kaspersky Security Center Cloud Console conçue pour familiariser l'utilisateur avec les fonctions de Kaspersky Security Center Cloud Console. Dans cette version, vous pouvez réaliser des opérations dans l'espace de travail pendant 30 jours. Toutes les applications administrées sont lancées automatiquement sous une licence d'essai de Kaspersky Security Center Cloud Console, y compris Kaspersky Endpoint Security. Toutefois, il n'est pas possible d'activer Kaspersky Endpoint Security sous sa propre licence d'essai après l'expiration de la licence d'essai de Kaspersky Security Center Cloud Console. Pour obtenir de plus amples informations sur les licences de Kaspersky Security Center Cloud Console, consultez l'[aide de Kaspersky Security Center Cloud Console](#).

La version d'essai de Kaspersky Security Center Cloud Console ne permet pas de passer ultérieurement à la version commerciale. Tout espace de travail d'essai sera automatiquement supprimé avec tout son contenu après une période de 30 jours.

Vous pouvez contrôler l'utilisation des licences d'une des méthodes suivantes :

- Consulter le *Rapport sur les clés utilisées* dans l'infrastructure de l'organisation (**Surveillance et rapports** → **Rapports**).
- Consulter les états des ordinateurs sous l'onglet **Appareils** → **Appareils administrés**. Si l'application n'est pas activée, l'ordinateur affiche l'état  et la description de l'état **Application inactive**.
- Consulter les informations sur la licence dans les propriétés de l'ordinateur.
- Consulter les propriétés de la clé (**Opérations** → **Licence**).

[Procédure d'activation de l'application dans la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Choisissez **Kaspersky Endpoint Security for Windows (11.6.0)** → **Ajout d'une clé**.

Étape 2. Ajout de la clé

Saisissez un [code d'activation](#) ou sélectionnez un fichier clé.

Pour en savoir plus sur l'ajout de clé dans le stockage de Kaspersky Security Center, consultez l'[aide de Kaspersky Security Center](#).

Étape 3. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 4. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 5. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple **Activer de Kaspersky Endpoint Security for Windows**.

Étape 6. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. Cette action entraîne l'activation de l'application Kaspersky Endpoint Security sur les ordinateurs des utilisateurs en mode silencieux.

[Procédure d'activation de l'application dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

2. Dans la liste déroulante **Type de tâche**, choisissez **Ajout d'une clé**.

3. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple **Activation de Kaspersky Endpoint Security for Windows**.

4. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

Étape 2. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 3. Sélection de la licence

Sélectionnez la licence selon laquelle vous souhaitez activer l'application. Cliquez sur le bouton **Suivant**.

Vous pouvez ajouter des clés dans Web Console (**Opérations** → **Licence**).

Étape 4. Fin de la création de la tâche

Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. Cette action entraîne l'activation de l'application Kaspersky Endpoint Security sur les ordinateurs des utilisateurs en mode silencieux.

Il est possible d'ajouter une clé de licence de réserve sur l'ordinateur via les propriétés de la tâche *Ajouter une clé*. La *clé de licence de réserve* devient active soit à l'expiration de la validité de la clé active, soit en cas de suppression de celle-ci. La présence d'une clé de licence de réserve permet d'éviter la restriction des fonctions de l'application lorsque la licence arrive à échéance.

Procédure d'ajout automatique d'une clé de licence sur ordinateurs via la Console d'administration (MMC)

1. Dans la console d'administration, accédez au dossier **Serveur d'administration** → **Licences de Kaspersky**. Une liste de clés de licence s'ouvre.
2. Ouvrez les propriétés de la clé de licence.
3. Dans la section **Général**, cochez la case **Clé de licence distribuée automatiquement**.
4. Enregistrez vos modifications.

La clé se propage alors automatiquement aux ordinateurs auxquels elle convient. Lors de la diffusion automatique d'une clé active ou d'une clé de licence de réserve, les restrictions de licence en matière de nombre d'appareils définies dans les propriétés de la clé sont prises en compte. Dès que la restriction de licence est atteinte, la diffusion de la clé sur les ordinateurs cesse automatiquement. Vous pouvez consulter la quantité d'ordinateurs sur lesquels une clé a été ajoutée ainsi que d'autres données dans les propriétés de la clé, dans la section **Appareils**.

Procédure d'ajout automatique d'une clé de licence aux ordinateurs via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, choisissez **Opérations** → **Licence** → **Licences de Kaspersky**. Une liste de clés de licence s'ouvre.
2. Ouvrez les propriétés de la clé de licence.
3. Sous l'onglet **Général**, cochez la case **Distribuer la clé automatiquement**.
4. Enregistrez vos modifications.

La clé se propage alors automatiquement aux ordinateurs auxquels elle convient. Lors de la diffusion automatique d'une clé active ou d'une clé de licence de réserve, les restrictions de licence en matière de nombre d'appareils définies dans les propriétés de la clé sont prises en compte. Dès que la restriction de licence est atteinte, la diffusion de la clé sur les ordinateurs cesse automatiquement. Vous pouvez consulter la quantité d'ordinateurs sur lesquels une clé a été ajoutée ainsi que d'autres données dans les propriétés de la clé, sous l'onglet **Appareils**.

Activation de l'application à l'aide de l'assistant d'activation de l'application

Pour activer Kaspersky Endpoint Security à l'aide de l'Assistant d'activation de l'application, procédez comme suit :

1. Cliquez sur le bouton **Licence** situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Activer l'application à l'aide d'une nouvelle licence**.

L'Assistant d'activation de l'application sera lancé. Suivez les instructions de l'Assistant d'activation de l'application.

Activation de l'application à l'aide de la ligne de commande

Pour activer l'application à l'aide de la ligne de commande,

saisissez dans la ligne de commande :

```
avp.com license /add <code d'activation ou fichier clé> [/login=<nom d'utilisateur> /password=<mot de passe>]
```

Les identifiants du compte utilisateur (`/login=<nom d'utilisateur> /password=<mot de passe>`) doivent être saisis si la [protection par mot de passe est activée](#).

Consultation des informations relatives à la licence

Pour consulter les informations sur la licence,

Cliquez sur le bouton **Licence** situé dans la partie inférieure de la fenêtre principale de l'application.

La fenêtre **Licence** s'ouvre. Cette fenêtre affiche les informations relatives à la licence (cf. ill. ci-après).



Clé

| | |
|------------------------------|--|
| Clé : | 4E1F78FD-EA69-4436-89C8-00402EB2B450 |
| Licence : | Licence commerciale pour 1 ordinateur |
| Date de création : | 02/10/2020 |
| Nom de l'application : | Kaspersky Endpoint Security pour postes de travail et serveurs de fichiers |
| Fonctionnalité : | <input checked="" type="checkbox"/> Sécurité <input checked="" type="checkbox"/> Contrôles de sécurité <input checked="" type="checkbox"/> Chiffrement des données |
| Identificateur du ticket : | C9BE7BE7-10B2-443D-A65C-154899644352 |
| Identificateur de la série : | 9600BB30-408D-4422-8985-4E7803C27117 |

La licence est activée depuis le 02/10/2020 jusqu'au 01/11/2020 03:00.

Votre licence pour Kaspersky Endpoint Security est sur le point d'expirer. 30 jours restants.

Supprimer la clé

Renouveler la licence


Visitez la boutique en ligne pour renouveler la licence.

Activer l'application à l'aide d'une nouvelle licence

Lancez l'Assistant d'activation de Kaspersky Endpoint Security.

Fenêtre Licence

La fenêtre **Licence** contient les informations suivantes :

- **État de la clé.** Il peut y avoir plusieurs [clés](#) sur l'ordinateur. Une clé peut être active ou de réserve. L'application ne peut compter qu'une seule clé active. La clé de licence de réserve peut devenir active seulement après l'expiration du délai de validité de la clé active ou après la suppression de la clé active à l'aide du bouton .
- **Clé.** La *clé* est une succession unique de caractères alphanumériques, formée au départ du code d'activation ou du fichier clé.
- **Licences.** Les [types de licence](#) suivants sont prévus : évaluation et commercial.
- **Nom de l'application.** Le nom complet de l'application de Kaspersky achetée.
- **Fonctionnalité(s).** Les fonctions de l'application accessibles sous votre licence. Les fonctions suivantes sont prévues : Protection, Contrôles de sécurité, Chiffrement des données et d'autres. La liste des fonctions accessibles figure également dans le certificat de licence.
- **Informations complémentaires sur la licence.** Le type de licence, la quantité d'ordinateurs couverts par la licence, la date de début et la date et l'heure de fin de la durée de validité de la licence (seulement pour la clé active).

L'heure de la fin de la durée de validité de la licence est exprimée dans le fuseau horaire configuré dans le système d'exploitation.

Les actions suivantes sont également disponibles dans la fenêtre Licence :

- **Acheter une licence/Renouveler la licence.** Ouvre le site Internet de la boutique en ligne de Kaspersky où vous pouvez acheter une licence ou renouveler la licence existante. Pour ce faire, il faut saisir les données de l'entreprise et payer la commande.
- **Activer l'application avec une nouvelle licence.** L'Assistant d'activation de l'application est lancé. L'assistant permet d'ajouter une clé avec l'aide du code d'activation ou le fichier clé. L'assistant d'activation de l'application permet d'ajouter une clé active et une seule clé de licence de réserve.

Achat d'une licence

Vous pouvez acheter une licence après avoir installé l'application. L'achat de la licence vous permet de recevoir un code d'activation ou un fichier clé pour activer l'application.

Pour acheter une licence, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Licence**.
2. Dans la fenêtre **Licence**, réalisez une des opérations suivantes :
 - Cliquez sur le bouton **Acheter une licence** si aucune clé n'a été installée ou si une clé pour licence d'évaluation a été installée.
 - Cliquez sur le bouton **Renouveler la licence** si vous avez ajouté une clé pour licence commerciale.

Le site Internet du magasin en ligne de Kaspersky où vous pouvez acheter la licence s'ouvre.

Renouvellement de l'abonnement

Si vous utilisez l'application par abonnement, Kaspersky Endpoint Security se connecte automatiquement au serveur d'activation à des intervalles définis jusqu'à la fin de l'abonnement.

Si vous utilisez l'application sous un abonnement illimité, Kaspersky Endpoint Security vérifie automatiquement en arrière-plan la présence éventuelle d'une clé mise à jour sur le serveur d'activation. Si la clé se trouve sur le serveur d'activation, l'application l'ajoute en mode de remplacement de la clé précédente. C'est ainsi que l'abonnement illimité à Kaspersky Endpoint Security se renouvelle sans votre participation.

Si vous utilisez l'application avec un abonnement limité, Kaspersky Endpoint Security vous préviendra le jour de l'expiration de l'abonnement ou de la période de grâce après l'expiration de l'abonnement et les tentatives de renouvellement automatique seront interrompues. Le comportement de Kaspersky Endpoint Security dans ce cas est identique à celui observé à l'échéance de la [licence commerciale de l'application](#) : l'application fonctionne sans mises à jour et Kaspersky Security Network est inaccessible.

Vous pouvez renouveler l'abonnement sur le site Internet du prestataire de services.

Vous pouvez mettre à jour l'état de l'abonnement manuellement dans la fenêtre **Licence**. Cette opération peut être requise si l'abonnement est renouvelé après l'expiration de la période de grâce et que l'application a arrêté de mettre à jour automatiquement l'état de l'abonnement.

Pour accéder au site Internet du fournisseur de services à partir de l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Licence**.
2. Dans la fenêtre **Licence**, cliquez sur le bouton **Contactez le fournisseur de l'abonnement**.

À propos des données

À propos des données dans le cadre du Contrat de licence utilisateur final

Si vous avez activé Kaspersky Endpoint Security à l'aide d'un [code d'activation](#), vous acceptez de transmettre automatiquement les informations suivantes à Kaspersky en vue de confirmer la légalité de l'utilisation de l'application :

- type, version et localisation de Kaspersky Endpoint Security ;
- versions des mises à jour installées de Kaspersky Endpoint Security ;
- identifiant de l'ordinateur et l'identifiant de l'installation de Kaspersky Endpoint Security sur l'ordinateur ;
- numéro de série et identificateur de la clé active ;
- type, version et nombre de bits du système d'exploitation, nom de l'environnement virtuel, installation ou non de l'application Kaspersky Endpoint Security dans l'environnement virtuel ;
- identifiants des composants de Kaspersky Endpoint Security actifs au moment de l'octroi des informations.

Kaspersky peut aussi utiliser ces informations pour générer des statistiques sur la diffusion et l'utilisation de l'application de Kaspersky.

En utilisant le code d'activation, vous acceptez de transmettre automatiquement les données citées ci-dessus. Si vous ne voulez pas envoyer ces informations à Kaspersky, vous pouvez activer Kaspersky Endpoint Security à l'aide du [fichier clé](#).

En acceptant les dispositions du Contrat de licence, vous acceptez de transmettre automatiquement les informations suivantes :

- Lors de la mise à jour de Kaspersky Endpoint Security :
 - version de Kaspersky Endpoint Security ;
 - identifiant de Kaspersky Endpoint Security ;
 - clé active ;
 - identifiant unique du lancement de la tâche de mise à jour ;
 - identifiant unique d'installation de Kaspersky Endpoint Security.
- Lors de la navigation via les liens de l'interface de Kaspersky Endpoint Security :
 - version de Kaspersky Endpoint Security ;
 - version du système d'exploitation ;
 - date d'activation de Kaspersky Endpoint Security ;
 - date de fin de la durée de validité de la licence ;

- date de création de la clé ;
- date d'installation de Kaspersky Endpoint Security ;
- identifiant de Kaspersky Endpoint Security ;
- identifiant de la vulnérabilité du système d'exploitation détectée ;
- identifiant de la dernière mise à jour installée pour Kaspersky Endpoint Security ;
- hachage du fichier détecté qui constitue une menace et nom de cet objet selon la classification de Kaspersky ;
- catégorie d'erreur d'activation de Kaspersky Endpoint Security ;
- code d'erreur d'activation de Kaspersky Endpoint Security ;
- nombre de jours restant avant l'expiration de la clé ;
- nombre de jours écoulés depuis l'ajout de la clé ;
- nombre de jours écoulés depuis l'expiration de la licence ;
- nombre d'ordinateurs couverts par la licence active ;
- clé active ;
- durée de validité de la licence de Kaspersky Endpoint Security ;
- état actuel de la licence ;
- type de licence active ;
- type de l'application ;
- identifiant unique du lancement de la tâche de mise à jour ;
- identifiant unique d'installation de Kaspersky Endpoint Security sur l'ordinateur ;
- langue de l'interface de Kaspersky Endpoint Security.

Les informations obtenues par Kaspersky sont protégées conformément à la législation en vigueur et aux politiques de Kaspersky. Les données sont transmises via des canaux de communication chiffrés.

Pour en savoir plus sur l'obtention, le traitement, la conservation et la suppression des informations relatives à l'utilisation de l'application après l'acceptation du Contrat de licence et de la Déclaration de Kaspersky Security Network, veuillez lire le contenu de ces derniers ou rendez-vous sur le [site Internet de Kaspersky](#). Les fichiers license.txt et ksn_<ID de la langue>.txt qui contiennent les textes du Contrat de licence et de la Déclaration de Kaspersky Security Network figurent dans le [kit de distribution](#).

Collecte des données dans le cadre de l'utilisation de Kaspersky Security Network

L'ensemble des données que Kaspersky Endpoint Security envoie à Kaspersky dépend du type de licence et des paramètres d'utilisation de Kaspersky Security Network.

Utilisation de KSN sous licence sur un maximum de 4 ordinateurs

En acceptant la Déclaration de Kaspersky Security Network, vous acceptez de transmettre automatiquement les informations suivantes :

- informations relatives à la mise à jour de la configuration de KSN : identifiant de la configuration active, identifiant de la configuration reçue, code d'erreur de mise à jour de la configuration ;
- informations sur les fichiers et les adresses Internet analysés : sommes de contrôle du fichier analysé (MD5, SHA2-256, SHA1) et profils de fichier (MD5), taille du profil, type de menace détectée et son nom conformément à la classification du Titulaire des droits, identifiant des bases antivirus, adresse Internet pour laquelle la réputation est sollicitée, adresse Internet depuis laquelle l'accès à l'adresse Internet à analyser a eu lieu, identifiant du protocole de connexion et numéro du port utilisé ;
- identifiant de la tâche d'analyse qui a détecté la menace ;
- informations sur les certificats numériques utilisés requises pour vérifier leur authenticité : sommes de contrôle du certificat (SHA256) utilisé pour signer l'objet à analyser, clé publique du certificat ;
- identificateur du module de l'application qui exécute l'analyse ;
- identificateurs des bases antivirus et enregistrements dans les bases antivirus ;
- informations relatives à l'activation de l'application sur l'ordinateur ; en-tête signé du ticket du service d'activation (identificateur du centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identificateur unique du ticket, version du ticket, état de la licence, date et heure du début de fin de validité du ticket, identificateur unique de licence, version de la licence), identificateur du certificat utilisé pour signer les en-têtes du ticket, somme de contrôle (MD5) du fichier clé ;
- informations relatives à l'application du Titulaire des droits : version complète, type, version du protocole utilisé dans le cadre de la connexion aux services de Kaspersky.

Utilisation de KSN sous licence sur 5 ordinateurs ou plus

En acceptant la Déclaration de Kaspersky Security Network, vous acceptez de transmettre automatiquement les informations suivantes :

Si la case **Kaspersky Security Network** est cochée alors que la case **Activer le mode étendu du KSN** est décochée, l'application transmet les informations suivantes :

- informations relatives à la mise à jour de la configuration de KSN : identifiant de la configuration active, identifiant de la configuration reçue, code d'erreur de mise à jour de la configuration ;
- informations sur les fichiers et les adresses Internet analysés : sommes de contrôle du fichier analysé (MD5, SHA2-256, SHA1) et profils de fichier (MD5), taille du profil, type de menace détectée et son nom conformément à la classification du Titulaire des droits, identifiant des bases antivirus, adresse Internet pour laquelle la réputation est sollicitée, adresse Internet depuis laquelle l'accès à l'adresse Internet à analyser a eu lieu, identifiant du protocole de connexion et numéro du port utilisé ;
- identifiant de la tâche d'analyse qui a détecté la menace ;

- informations sur les certificats numériques utilisés requises pour vérifier leur authenticité : sommes de contrôle du certificat (SHA256) utilisé pour signer l'objet à analyser, clé publique du certificat ;
- identificateur du module de l'application qui exécute l'analyse ;
- identificateurs des bases antivirus et enregistrements dans les bases antivirus ;
- informations relatives à l'activation de l'application sur l'ordinateur ; en-tête signé du ticket du service d'activation (identificateur du centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identificateur unique du ticket, version du ticket, état de la licence, date et heure du début de fin de validité du ticket, identificateur unique de licence, version de la licence), identificateur du certificat utilisé pour signer les en-têtes du ticket, somme de contrôle (MD5) du fichier clé ;
- informations relatives à l'application du Titulaire des droits : version complète, type, version du protocole utilisé dans le cadre de la connexion aux services de Kaspersky.

Si en plus de la case **Kaspersky Security Network** vous cochez la case **Activer le mode étendu du KSN**, l'application transmet en plus les informations suivantes :

- informations sur les résultats du classement en catégories des ressources Internet sollicitées. Celui contient l'adresse Internet à analyser et l'adresse IP de l'hôte, la version du module de l'application qui réalise le classement en catégories, le mode de classement utilisé et la sélection de catégories définies pour la ressource Internet ;
- informations sur l'application installée sur l'Ordinateur : nom de l'application et son éditeur, clés de registre utilisée et leurs valeurs, informations relatives aux fichiers des modules de l'application installée (sommes de contrôle (MD5, SHA2-256, SHA1), nom, chemin du fichier sur l'Ordinateur, taille, version et signature numérique) ;
- informations sur l'état de la protection antivirus de l'Ordinateur : versions, dates et heures de publication des bases antivirus utilisées, identifiant de la tâche et identifiant du Logiciel qui effectue l'analyse ;
- informations relatives aux fichiers téléchargés par l'Utilisateur final : URL et adresses IP depuis lesquelles le téléchargement a eu lieu et adresse Internet de la page de transfert à la page de téléchargement du fichier, identifiant du protocole de téléchargement et numéro du port de connexion, indice de caractère malveillant des adresses, attributs et taille du fichier ainsi que ses sommes de contrôle (MD5, SHA2-256, SHA1), informations sur le processus qui a chargé le fichier (sommes de contrôle (MD5, SHA2-256, SHA1), date et heure de création et d'association, indice de présence dans le démarrage automatique, attributs, nom des compacteurs, informations relatives à la signature, indice du fichier exécutable, identifiant du format, type du compte utilisateur sous lequel le processus a été lancé), informations sur le fichier du processus (nom, chemin du fichier et taille), nom du fichier, chemin d'accès au fichier sur l'Ordinateur, signature numérique du fichier et informations sur l'exécution de la signature, adresse Internet où a eu lieu la détection, nombre de scripts suspects sur la page considérée comme suspecte ou malveillante, informations sur les requêtes HTTP générées et la réponse à celles-ci ;
- informations sur les applications lancées et leurs modules : données sur les processus exécutés dans le système (identifiant du processus dans le système (PID), nom du processus, données relatives au compte utilisateur sous lequel le processus a été lancé, données relatives à l'application et à la commande qui a lancé le processus, ainsi que l'indice de confiance de l'application ou du processus, chemin d'accès complet aux fichiers du processus et leur somme de contrôle (MD5, SHA2-256, SHA1), ligne de commande de lancement, niveau d'intégrité du processus, description du produit auquel se rapporte le processus (nom du produit et données relatives à l'éditeur), données relatives aux certificats numériques utilisés et informations indispensables à la vérification de leur authenticité ou données relatives à l'absence de signature numérique du fichier), informations sur les modules chargés dans le processus (nom, taille, type, date de création, attributs, sommes de contrôle (MD5, SHA2-256, SHA1), chemin d'accès), informations de l'en-tête des fichiers PE, nom du compacteur (si le fichier était compacté) ;

- informations relatives à l'ensemble des objets et actions potentiellement malveillants : nom de l'objet détecté et chemin d'accès complet à l'objet sur l'Ordinateur, sommes de contrôle des fichiers traités (MD5, SHA2-256, SHA1), date et heure de la détection, nom et taille des fichiers traités et chemin d'accès à ceux-ci, code du modèle de chemin d'accès, indice de fichier exécutable, identification de l'objet en tant que conteneur ou non, nom du compacteur (si le fichier a été compacté), code du type de fichier, identifiant du format de fichier, identificateurs des bases antivirus et des enregistrements dans ces bases sur la base desquels l'application a été mise en évidence, indice d'objet potentiellement malveillant, nom de la menace détectée conformément à la classification du Titulaire des droits, état et mode de détection, cause de l'inclusion dans le contexte à analyser et position du fichier dans le contexte, sommes de contrôle (MD5, SHA2-256, SHA1), nom et attributs du fichier exécutable de l'application via laquelle le message infecté ou le lien est arrivé, adresses IP (IPv4 et IPv6) de l'hôte de l'objet bloqué, entropie du fichier, indice de la présence du fichier dans le démarrage automatique, heure de la première détection du fichier dans le système, nombre de lancements du fichier depuis le dernier envoi des statistiques, type de compilateur, informations relatives au nom, aux sommes de contrôle (MD5, SHA2-256, SHA1) et à la taille du client de messagerie via lequel l'objet malveillant a été reçu, identifiant de la tâche de l'application qui a réalisé l'analyse, indice de vérification de la réputation ou signature du fichier, résultats de l'analyse statistique du contenu de l'objet, résultats du traitement du fichier, profils de l'objet et taille du profil en octets, caractéristiques techniques des technologies de détection appliquée ;
- informations sur les objets analysés : groupe de confiance attribué dans lequel le fichier est placé et/ou hors duquel il est déplacé, cause du placement du fichier dans cette catégorie, identifiant de la catégorie, informations relatives à la source des catégories et à la version des bases de catégories, indice de la présence dans le fichier d'un certificat de confiance, nom de l'éditeur du fichier, version du fichier, nom et version de l'application dont le fichier fait partie ;
- informations sur les vulnérabilités détectées : identifiant de la vulnérabilité dans la base des vulnérabilités, classe du danger de la vulnérabilité ;
- informations sur l'exécution de l'émulation du fichier exécutable : taille du fichier et ses sommes de contrôle (MD5, SHA2-256, SHA1), version du module d'émulation, profondeur de l'émulation, vecteur des caractéristiques des blocs logiques et des fonctions à l'intérieur des blocs logiques obtenu lors de l'émulation, données issues de la structure de l'en-tête PE du fichier exécutable ;
- adresses IP de l'ordinateur à l'origine de l'attaque (IPv4 et IPv6), numéro du port de l'Ordinateur cible de l'attaque de réseau, identifiant du protocole du paquet IP contenant l'attaque, cible de l'attaque (nom de l'entreprise, site Web), indicateur de la réaction à l'attaque, poids de l'attaque, niveau de confiance ;
- informations relatives aux attaques liées à la substitution de ressources réseau, DNS et adresses IP (IPv4 ou IPv6) des sites Internet visités ;
- adresses Internet et adresses IP (IPv4 ou IPv6) de la ressource Internet sollicitée, informations relatives au fichier et/ou au client Internet qui a contacté la ressource Internet : nom, taille, sommes de contrôle (MD5, SHA2-256, SHA1) du fichier, chemin d'accès complet à celui-ci et code du modèle de chemin d'accès, résultat de la vérification de sa signature numérique et son état dans KSN ;
- informations sur l'exécution du retour à l'état antérieur aux actions du programme malveillant : données relatives au fichier, activité soumise à la tâche (nom du fichier, son chemin d'accès complet, sa taille et les sommes de contrôle (MD5, SHA2-256, SHA1)), données sur les actions réussies ou non au niveau de la suppression, du changement de nom et de la copie des fichiers et de la restauration des valeurs dans le registre (nom des clés du registre et leurs valeurs), informations sur les fichiers système modifiés par le programme malveillant avant et après le retour à l'état antérieur ;
- informations sur les exclusions pour les règles du module Contrôle évolutif des anomalies : identificateur et état de la règle déclenchée, action de l'application lors du déclenchement de la règle, type de compte utilisateur sous lequel le processus ou le flux exécute les actions suspectes, informations sur le processus qui exécute les actions suspectes ou qui en fait l'objet (identificateur du script ou nom du fichier du processus, chemin d'accès complet du processus, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du processus), informations sur l'objet au nom duquel les actions suspectes ont été réalisées et sur l'objet sur lequel les actions suspectes ont été réalisées (nom de la clé du registre ou nom du fichier, chemin du fichier complet, code du modèle de chemin et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier).

- informations relatives aux modules de l'application à charger : nom, taille et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du module, son chemin d'accès complet et code du modèle de chemin d'accès, paramètres de la signature numérique du fichier du module, date et heure de création de la signature, nom du sujet et de l'organisation qui ont signé le fichier du module, identifiant du processus dans lequel le module a été chargé, nom du fournisseur du module, numéro de position du module dans la file de chargement ;
- informations sur les exclusions pour les règles du module Contrôle évolutif des anomalies : date et heure de début et de fin de la période de collecte des statistiques, informations sur la qualité des requêtes et de la connexion avec chacun des services de KSN utilisés (identificateur du service KSN, nom de requêtes réussies, nombre de requêtes avec des réponses issues du cache, nombre de requêtes en échec (problèmes de réseau, désactivation de KSN dans les paramètres de l'application, parcours incorrect), répartition dans le temps des requêtes qui ont réussi, répartition dans le temps des requêtes qui ont été annulées, répartition dans le temps des requêtes qui ont dépassé le délai d'attente, nombre de connexion au KSN tirées du cache, nombre de connexions à KSN réussies, nombre de connexions à KSN ratées, nombre de transactions réussies, nombre de transactions ratées, répartition dans le temps des connexions à KSN réussie, répartition dans le temps des connexions à KSN ratées, répartition dans le temps des transactions réussies, répartition dans le temps des transactions ratées) ;
- si un objet potentiellement malveillant est détecté, les informations relatives aux données présentes dans la mémoire des processus (éléments de la hiérarchie système des objets (ObjectManager), données de la mémoire BIOS UEFI, noms et valeurs des clés de Registre) seront fournies ;
- informations relatives aux événements dans les journaux système : heure de l'événement, nom du journal dans lequel l'événement est détecté, type et catégorie de l'événement, nom de la source de l'événement et sa description ;
- informations relatives aux connexions réseau : version et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier à partir desquels le processus qui a ouvert le port a été démarré, chemin d'accès au fichier du processus et sa signature numérique, adresses IP locale et distante, numéros des ports de connexion local et distant, état de la connexion, horodatage de l'ouverture du port ;
- informations sur la date d'installation et d'activation du Logiciel sur l'Ordinateur : identifiant du partenaire qui a vendu la licence, numéro de série de la licence, en-tête signé du ticket du service d'activation (identifiant d'un centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identifiant unique du ticket, version du ticket, état de la licence, date et heure de début/fin du ticket, identifiant unique de la licence, version de la licence), identifiant du certificat utilisé pour signer l'en-tête du ticket, somme de contrôle (MD5) du fichier clé, identifiant unique de l'installation du Logiciel sur l'Ordinateur, type et identifiant de l'application qui est mise à jour, identifiant de la tâche de mise à jour ;
- informations sur l'ensemble des mises à jour installées ainsi que sur l'ensemble des dernières mises à jour installées et/ou supprimées, type d'événement ayant provoqué l'envoi des informations relatives aux mises à jour, durée écoulée depuis l'installation de la dernière mise à jour, informations relatives aux bases antivirus téléchargées au moment de la remise des informations ;
- Information sur le fonctionnement de l'application sur l'Ordinateur : données sur l'utilisation du processeur (CPU), donnée sur l'utilisation de la mémoire (Private Bytes, Non-Page Pool, Paged Pool), nombre de flux actifs dans le processus de l'application et de flux en attente, durée de fonctionnement de l'application jusqu'à l'erreur, indice de fonctionnement de l'application en mode interactif ;
- nombre de plantages de l'application et de plantages du système (BSOD) depuis l'installation de l'application et depuis la dernière mise à jour, identifiant et version du module de l'application dans lequel l'échec s'est produit, pile de la mémoire dans le processus de produit et informations relatives aux bases antivirus au moment de l'échec ;
- données relatives au plantage du système (BSOD) : indice de l'apparition du BSOD sur l'Ordinateur, nom du pilote qui a provoqué le BSOD, adresse et pile de la mémoire dans le pilote, indice de la longueur de la session du système d'exploitation avant le BSOD, pile de la mémoire de chute du pilote, type de dump de mémoire conservé, indice que la session du système d'exploitation avant le BSOD avait duré plus de 10 minutes, identifiant unique du dump, date et heure du BSOD ;

- données sur les erreurs ou les problèmes de performances survenus pendant le fonctionnement des modules de l'application : identificateur de l'état de l'application, code et cause de l'erreur, ainsi que son heure d'apparition, identificateurs du module, du module et du processus de l'application dans lequel l'erreur s'est produite, identificateur de la tâche ou de la catégorie de mise à jour au cours de laquelle l'erreur s'est produite, journaux des pilotes utilisés par l'application (code d'erreur, nom du module, nom du fichier source et ligne sur laquelle l'erreur s'est produite) ;
- données relatives aux mises à jour des bases antivirus et des modules de l'application : noms, dates et heures des fichiers d'index chargés suite à la dernière mise à jour et présents dans la mise à jour actuelle ;
- informations sur les pannes de l'application : date et heure de création du dump, son type, type d'événement à l'origine de l'arrêt accidentel de l'application (coupure accidentelle de l'alimentation, plantage de l'application d'un éditeur tiers), date et heure de la coupure accidentelle de l'alimentation ;
- informations sur la compatibilité des pilotes de l'application avec la configuration matérielle et logicielle : informations sur les propriétés du système d'exploitation qui imposent des limites sur les fonctions des modules de l'application (Secure Boot, KPTL, WHQL Enforce, BitLocker, Case Sensitivity), type de chargement de l'application intégré (UEFI BIOS), indice de la présence d'un module de plateforme de confiance (Trusted Platform Module, TPM), version de la spécification de la TPM, informations sur l'unité centrale (CPU) installée sur l'ordinateur, mode et paramètres de fonctionnement de Code Integrity et Device Guard, mode de fonctionnement des pilotes et raison de l'utilisation du mode actif, version des pilotes de l'application, état de la prise en charge des outils logiciels et matériel de virtualisation de l'Ordinateur par les pilotes ;
- informations sur les applications tierces qui ont provoqué l'erreur : leur nom, version et localisation, code d'erreur et informations à son sujet tirées du journal système des applications, adresse où l'erreur est apparue et pile de mémoire de l'application tierce, signe d'apparition de l'erreur dans le module de l'application, durée de fonctionnement de l'application avant l'erreur, sommes de contrôle (MD5, SHA2-256, SHA1) de l'image du processus de l'application dans lequel l'erreur s'est produite, chemins d'accès à cette image du processus de l'application et code du modèle de chemin, informations du journal système du système d'exploitation avec la description de l'erreur liée à l'application, les informations sur le module de l'application dans lequel l'erreur s'est produite (identifiant de l'exception, adresse de l'erreur comme déplacement dans le module, nom et version du module, identifiant de la panne de l'application dans le plug-in du Titulaire de droit et pile de la mémoire de cette panne, durée de fonctionnement de l'application jusqu'à l'erreur) ;
- version du module de la mise à jour de l'application, nombre d'arrêts sur échec du module de mise à jour de l'application lors de l'exécution des tâches de mise à jour après le fonctionnement du module, identifiant du type de tâche de mise à jour, nombre d'échecs de tâches de mise à jour du module de mise à jour de l'application ;
- informations sur le fonctionnement des modules de surveillance du système : versions complètes des modules, date et heure de lancement des modules, code de l'événement qui a fait déborder la file d'attente d'événement et le nombre de ces événements, total des débordements de la file d'attente d'événement, informations sur le fichier du processus à l'origine de l'événement (nom du fichier et son chemin d'accès sur l'Ordinateur, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du processus lié au fichier, version du fichier), identificateur de l'interception de l'événement réalisée, version complète du filtre de l'intercepteur, identificateur du type d'événement intercepté, taille de la file d'attente d'événements et nombre d'événements entre le premier de la file et l'actuel, nombre d'événements dépassés dans la file d'attente, informations sur le processus à l'origine de l'événement actuel (nom du fichier du processus et son chemin sur l'Ordinateur, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du processus), durée de traitement de l'événement, durée maximale autorisée pour le traitement de l'événement, valeur de la probabilité d'envoi des données, informations sur les événements du système d'exploitation pour lesquels l'application a dépassé la limite du délai d'attente (date et heure de la réception de l'événement, nombre d'initialisations répétées des bases antivirus, date et heure de la dernière initialisation répétée des bases antivirus après leur mise à jour, durée du retard de traitement des événements par chaque module de surveillance du système, nombre d'événements en attente, nombre d'événements traités, nombre d'événements du type actuel retenus, total du retard pour les événements du type actuel, total du retard pour tous les événements) ;
- informations sur l'outil de trace des événements Windows (Event Tracing for Windows, ETW) lors de problèmes de performances de l'application, fournisseurs d'événements SysConfig/SysConfigEx/WinSATAssessment de

Microsoft : données sur l'ordinateur (modèle, fabricant, facteur de forme, version), données sur les indicateurs de performance Windows (données de l'évaluation WinSAT, indice de performance Windows), nom du domaine, données sur les processus physiques et logiques (nombre de processeurs physiques et logiques, fabricant, modèle, stepping, nombre de noyaux, fréquence d'horloge, identificateur de processeur (CPUID), caractéristiques du cache, caractéristiques du processeur logique, indice de prise en charge des modes et des instructions), données sur les modules de la mémoire vive (type, facteur de forme, fabricant, modèle, volume, granularité de l'allocation de la mémoire), données sur les interfaces réseau (adresses IP et MAC, nom, description, configuration des interfaces réseau, répartition du nombre et du volume de paquets réseau par type, vitesse de l'échange réseau, distribution du nombre d'erreurs réseau par type), configuration du contrôleur IDE, adresses IP des serveurs DNS, données sur la carte vidéo (modèle, description, fabricant, compatibilité, volume de mémoire vidéo, résolution de l'écran, nombre de bits par pixel, version du BIOS), données sur les appareils Plug-and-Play (nom, description, identificateur d'appareil [PnP, ACPI]), données relatives aux disques et supports (nombre de disques ou de clés USB, fabricant, modèle, volume de disque, nombre de tambours, nombre de pistes par tambour, nombre de partitions par piste, volume de secteur, caractéristiques du cache, numéro de séquence, nombre de partitions, configuration du contrôleur SCSI), données sur les disques logiques (numéro de séquence, volume de la partition, taille du volume, lettre du volume, type de partition, type de système de fichiers, nombre de clusters, taille du cluster, nombre de secteurs dans un cluster, nombre de clusters occupés et disponibles, lettre du volume d'amorçage, déplacement de la partition par rapport au début du disque), données sur le BIOS de la carte-mère (fabricant, date de fabrication, version), données sur la mémoire physique (volume total et disponible), données sur les services du système d'exploitation (nom, description, état, tag, données sur les processus [nom et identificateur PID]), paramètres de consommation de l'ordinateur, configuration du contrôleur d'interruptions, chemin d'accès aux dossiers système Windows (Windows et System32), données sur le système d'exploitation (version, build, date d'édition, nom, type, date d'installation), taille du fichier de débogage, données sur les écrans (nombre, fabricant, résolution de l'écran, pouvoir de résolution, type), données sur le pilote de la carte vidéo (fabricant, date de sortie, version) ;

- informations fournies par ETW, fournisseurs d'événements EventTrace/EventMetadata de Microsoft : données sur la séquence des événements système (type, heure, date, fuseau horaire), métadonnées du fichier avec les résultats du traçage (nom, structure, paramètres de traçage, distribution du nombre d'opérations de traçage par type), données sur le système d'exploitation (nom, type, version, build, date de publication, heure de lancement) ;
- informations fournies par l'ETW, fournisseurs d'événements Process/Microsoft-Windows-Kernel-Process/Microsoft-Windows-Kernel-Processor-Power de Microsoft : données sur les processus à lancer et à arrêter (nom, identificateur PID, paramètres de lancement, ligne de commande, code de retour, paramètres d'administration de l'alimentation, heure de lancement et de fin, type de marqueur d'accès, identificateur de sécurité SID, identificateur de séance SessionID, nombre de descripteurs installés), données sur la modification des priorités de flux (identificateur de flux TID, priorité, heure), données sur les opérations du processus sur le disque (type, heure, volume, nombre), historique de la modification de la structure et volume de processus utilisé ;
- informations fournies par ETW, fournisseurs d'événements StackWalk/Perfinfo de Microsoft : données des compteurs de performance (performances de segments distincts du code, séquence des appels de fonction, identificateur du processus PID, identificateur du flux TID, adresses et attributs des gestionnaires d'interruption ISR et des appels différés des procédures DPC) ;
- informations fournies par ETW, fournisseur d'événements KernelTraceControl-ImageID de Microsoft : données sur les fichiers exécutables et les bibliothèques dynamiques (nom, taille de l'image, chemin d'accès complet), données sur les fichiers PDB (nom, identificateur), données de la ressource VERSIONINFO du fichier exécutable (nom, description, éditeur, locale, version et identificateur de l'application, version et identificateur du fichier) ;
- informations fournies par ETW, fournisseurs d'événements FileIo/DiskIo/Image/Windows-Kernel-Disk de Microsoft : données sur les opérations relatives aux fichiers et aux disques (type, volume, heure de début, heure de fin, durée, état de l'arrêt, identificateur de processus PID, identificateur de flux TID, adresses des appels de fonction du pilote, paquet de requête d'E/S (IRP), attributs d'objet de fichier Windows), données sur les fichiers impliqués dans les opérations relatives aux fichiers et aux disques (nom, version, taille, chemin d'accès complet, attribut, déplacement, somme de contrôle de l'image, options d'ouverture et d'accès) ;

- informations fournies par ETW, fournisseur d'événements PageFault de Microsoft : données sur les erreurs d'accès aux pages de la mémoire (adresse, heure, volume, identificateur du processus PID, identificateur de flux TID, attributs de l'objet de fichier Windows, paramètres d'allocation de mémoire) ;
- informations fournies par ETW, fournisseur d'événements Thread de Microsoft : données sur la création/la fin de flux, données sur les flux lancés (identificateur de processus PID, identificateur de flux TID, taille de la pile, priorité et distribution des ressources de l'unité centrale, ressources d'entrée et de sortie, pages de mémoire entre les flux, adresse de la pile, adresse de la fonction initiale, adresse du bloc d'environnement de flux (Thread Environment Block, TEB), tag du service Windows) ;
- informations fournies par ETW, fournisseur d'événements Microsoft-Windows-Kernel-Memory de Microsoft : données sur les opérations d'administration de la mémoire (état de la fin, heure, nombre, identificateur de processus PID), structure de distribution de la mémoire (type, volume, identificateur de session SessionID, identificateur de processus PID) ;
- informations sur le fonctionnement de l'application en cas de problème de productivité : identificateur d'installation de l'application, type et valeur de réduction des performances, données sur la séquence des événements internes de l'application (heure, fuseau horaire, type, état d'arrêt, identificateur de module de l'application, identificateur de scénario de fonctionnement de l'application, identificateur de flux TID, identificateur de processus PID, adresses d'appels de fonctions), données sur les fichiers PDB (nom, identificateur, taille de l'image du fichier exécutable), données sur les fichiers à analyser (nom, chemin complet, somme de contrôle), paramètres de surveillance des performances de l'application ;
- informations sur le dernier redémarrage en échec du système d'exploitation : nombre de redémarrages en échec depuis l'installation du système d'exploitation, données relatives au crash du système (code et paramètres de l'erreur, nom, version et somme de contrôle (CRC32) du module ayant entraîné l'erreur dans le fonctionnement du système d'exploitation, adresse de l'erreur comme déplacement dans le module, sommes de contrôle (MD5, SHA2-256, SHA1) du vidage du système) ;
- informations de vérification de l'authenticité des certificats qui signent les fichiers : empreinte du certificat, algorithme de calcul de la somme de contrôle, clé publique et numéro de série du certificat, nom de l'autorité de certification, résultat du contrôle du certificat et identifiant de la base de certificats ;
- informations sur le processus à l'origine de l'attaque contre l'autodéfense de l'application : nom et taille du fichier du processus, ses sommes de contrôle (MD5, SHA2-256, SHA1), chemin d'accès complet à celui-ci et modèle de chemin, date et heure de création et de configuration du fichier du processus, code du type de fichier de processus, indice de fichier exécutable, attribut de fichier du processus, informations relatives au certificat utilisé pour signer le fichier du processus, type du compte utilisateur sous lequel le processus ou le flux réalise l'action suspecte, identifiant des opérations réalisées pour accéder au processus, type de ressource à partir de laquelle l'opération a été réalisée (processus, fichier, objet du registre, fenêtre de recherche à l'aide de la fonction FindWindow), nom de la ressource depuis laquelle l'opération est exécutée, indice de réussite de l'opération, état du fichier du processus et sa signature dans KSN ;
- informations sur le Logiciel du Titulaire des droits : version complète, type, localisation et état de fonctionnement du Logiciel utilisé, versions des modules du Logiciel installés et leur état de fonctionnement, informations sur les mises à jour du Logiciel installé, valeur du filtre TARGET, version du protocole utilisé pour se connecter aux services du Titulaire des droits ;
- informations sur le matériel installé sur l'Ordinateur : type, nom, modèle, version du micrologiciel, caractéristiques des appareils intégrés et connectés, identifiant unique de l'Ordinateur sur lequel est installée l'application ;
- informations relatives à la version du système d'exploitation installée sur l'Ordinateur et aux paquets de mises à jour installés, version, rédaction et paramètres du mode de fonctionnement du système d'exploitation, version et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du noyau du système d'exploitation et date et heure de lancement du système d'exploitation ;
- fichiers exécutables et non exécutables, en tout ou en partie ;

- parties de la mémoire RAM de l'Ordinateur ;
- les secteurs impliqués dans le processus d'amorçage du système d'exploitation ;
- les paquets de données du trafic réseau ;
- les pages Web et les e-mails contenant des objets malveillants et suspects ;
- la description des classes et instances de classes du référentiel WMI ;
- rapports d'activités des applications :
 - nom, taille et version du fichier à envoyer, sa description et ses sommes de contrôle (MD5, SHA2-256, SHA1), identifiant du format, nom de son éditeur, nom du produit associé au fichier, chemin d'accès complet au fichier sur l'Ordinateur et code du modèle de chemin, date et heure de création et de modification du fichier ;
 - date et heure de début et de fin de validité du certificat (si le fichier possède une signature numérique), date et heure de la signature, nom de l'émetteur du certificat, informations relatives au détenteur du certificat, empreinte, clé publique et algorithmes appropriés du certificat, numéro de série du certificat ;
 - nom du compte utilisateur sous lequel le processus a été lancé ;
 - sommes de contrôle (MD5, SHA2-256, SHA1) du nom de l'Ordinateur sur lequel le processus est lancé ;
 - titres des fenêtres du processus ;
 - identifiant des bases antivirus, nom de la menace détectée conformément à la classification de Détenteur des droits ;
 - données relatives à la licence installée, son identifiant, son type et sa date d'expiration ;
 - heure locale de l'Ordinateur au moment de la collecte des informations ;
 - noms et chemins d'accès aux fichiers auxquels le processus a accédé ;
 - noms des clés du registre, ainsi que leurs valeurs, auxquelles le processus a accédé ;
 - URL et adresses IP auxquelles le processus a accédé ;
 - URL et adresses IP à partir desquelles le fichier en cours d'exécution a été téléchargé.

Respect de la législation de l'Union européenne (RGPD)

Il se peut que Kaspersky Endpoint Security transmette des données à Kaspersky dans les cas suivants :

- Utilisation de Kaspersky Security Network
- Activation de l'application à l'aide d'un code d'activation
- Mise à jour des modules d'application et des bases antivirus
- Consultation de liens dans l'interface de l'application

- Enregistrement des fichiers dump

Indépendamment de la classification des données et du territoire à partir duquel les données sont reçues, Kaspersky adhère à des normes élevées de sécurité des données et emploie diverses mesures juridiques, organisationnelles et techniques pour protéger les données des utilisateurs, pour garantir la sécurité et la confidentialité des données, mais également pour assurer le respect des droits des utilisateurs, conformément à la législation applicable. Le texte de la politique de confidentialité est inclus dans le [kit de distribution de l'application](#) et est accessible sur le [site Internet de Kaspersky](#).

Avant d'utiliser Kaspersky Endpoint Security, veuillez lire attentivement la description des données transmises dans le [Contrat de licence utilisateur final](#) et la [Déclaration de Kaspersky Security Network](#). Si des données particulières transmises par Kaspersky Endpoint Security dans l'un des cas de figure décrits peuvent être classées comme des données personnelles selon la législation ou la norme locale, vous devez vous assurer que ces données sont traitées légalement et obtenir le consentement des utilisateurs finaux pour collecter et transmettre ces données.

Pour en savoir plus sur l'obtention, le traitement, la conservation et la suppression des informations relatives à l'utilisation de l'application après l'acceptation du Contrat de licence et de la Déclaration de Kaspersky Security Network, veuillez lire le contenu de ces derniers ou rendez-vous sur le [site Internet de Kaspersky](#). Les fichiers license.txt et ksn_<ID de la langue>.txt qui contiennent les textes du Contrat de licence et de la Déclaration de Kaspersky Security Network figurent dans le [kit de distribution](#).

Si vous ne souhaitez pas transmettre de données à Kaspersky, vous pouvez désactiver la collecte de données.

Utilisation de Kaspersky Security Network

En utilisant Kaspersky Security Network, vous acceptez de fournir automatiquement les données mentionnées dans la [Déclaration de Kaspersky Security Network](#). Si vous n'acceptez pas de fournir ces données à Kaspersky, utilisez KSN privé ou [désactivez l'utilisation de KSN](#). Pour en savoir plus sur le fonctionnement du KSN local, reportez-vous à la *documentation de Kaspersky Private Security Network*.

Activation de l'application à l'aide d'un code d'activation

En utilisant un code d'activation, vous acceptez de fournir automatiquement les données mentionnées dans le [Contrat de licence utilisateur final](#). Si vous ne voulez pas fournir ces données à Kaspersky, [activez Kaspersky Endpoint Security à l'aide du fichier clé](#).

Mise à jour des modules d'application et des bases antivirus

En utilisant les serveurs de Kaspersky, vous acceptez de fournir automatiquement les données mentionnées dans le [Contrat de licence utilisateur final](#). Kaspersky demande ces informations pour vérifier que Kaspersky Endpoint Security est utilisé de manière légitime. Si vous n'acceptez pas de fournir ces informations à Kaspersky, utilisez [Kaspersky Update Utility](#) ou [Kaspersky Security Center pour mettre à jour les bases de données](#).

Consultation de liens dans l'interface de l'application

En utilisant les liens figurant dans l'interface de l'application, vous acceptez de fournir automatiquement les données mentionnées dans le [Contrat de licence utilisateur final](#). La liste exacte des données transmises dans chaque lien concret dépend de l'emplacement exact du lien dans l'interface de l'application et du problème qu'il est censé résoudre. Si vous n'acceptez pas de fournir ces données à Kaspersky, utilisez l'[interface simplifiée de l'application](#) ou [masquez l'interface de l'application](#).

Enregistrement des fichiers dump

Si vous avez [activé l'enregistrement des fichiers de vidage](#), Kaspersky Endpoint Security créera un fichier de vidage qui contiendra toutes les données en mémoire des processus d'application au moment où ce fichier de vidage a été créé.

Guide de démarrage

Après avoir installé Kaspersky Endpoint Security, vous pouvez gérer l'application à l'aide des interfaces suivantes :

- [Interface locale de l'application.](#)
- Console d'administration de Kaspersky Security Center.
- Kaspersky Security Center 12 Web Console.
- Kaspersky Security Center Cloud Console.

Console d'administration de Kaspersky Security Center

Kaspersky Security Center permet d'installer, de supprimer, de lancer et d'arrêter Kaspersky Endpoint Security à distance, de configurer les paramètres de fonctionnement de l'application, de modifier la sélection des modules, d'ajouter des clés et de lancer et d'arrêter les tâches de mise à jour et d'analyse.

L'administration de l'application via Kaspersky Security Center s'opère à l'aide du plug-in d'administration Kaspersky Endpoint Security.

Pour en savoir plus sur l'administration de l'application via Kaspersky Security Center, consultez l'[aide de Kaspersky Security Center](#).

Kaspersky Security Center 12 Web Console et Kaspersky Security Center Cloud Console

Kaspersky Security Center 12 Web Console (ci-après aussi "*Web Console*") est une application (application Internet) prévue pour la réalisation centralisée des principales tâches d'administration et de maintenance des systèmes de protection du réseau de l'organisation. Web Console est un module de Kaspersky Security Center qui propose une interface utilisateur. Pour obtenir de plus amples informations sur Kaspersky Security Center 12 Web Console, veuillez consulter l'[aide de Kaspersky Security Center](#).

Kaspersky Security Center Cloud Console (ci-après "*Cloud Console*") est une solution cloud qui permet de protéger et de contrôler le réseau de l'entreprise. Pour obtenir de plus amples informations sur Kaspersky Security Center Cloud Console, consultez l'[aide de Kaspersky Security Center Cloud Console](#).

Web Console et Cloud Console permettent de réaliser les opérations suivantes :

- contrôler l'état du système de sécurité de votre entreprise ;
- installer des applications de Kaspersky sur les appareils de votre réseau ;
- administrer les applications installées ;
- consulter les rapports sur l'état du système de la sécurité.

Il existe des différences dans l'administration de Kaspersky Endpoint Security via Web Console, Cloud Console et la Console d'administration de Kaspersky Security Center. La [liste des modules et tâches disponibles](#) varie également.

À propos du plug-in d'administration de Kaspersky Endpoint Security for Windows

Le plug-in d'administration de Kaspersky Endpoint Security for Windows permet à Kaspersky Endpoint Security d'interagir avec Kaspersky Security Center. Le plug-in d'administration permet d'administrer Kaspersky Endpoint Security à l'aide des outils suivants : les [stratégies](#), les [tâches](#), ainsi que les [paramètres locaux de l'application](#). Un plug-in Internet est prévu pour interagir avec Kaspersky Security Center 12 Web Console.

La version du plug-in d'administration peut différer de la version de Kaspersky Endpoint Security installée sur l'ordinateur client. Si la version installée du plug-in d'administration prévoit moins de fonctions que dans la version installée de Kaspersky Endpoint Security, les paramètres des fonctions manquantes ne sont pas régis par le plug-in d'administration. Ces paramètres peuvent être modifiés par l'utilisateur dans l'interface locale de Kaspersky Endpoint Security.

Le plug-in Internet n'est pas installé par défaut dans Kaspersky Security Center 12 Web Console. À la différence du plug-in d'administration pour la Console d'administration de Kaspersky Security Center qui est installé sur le poste de travail de l'administrateur, le plug-in d'administration doit être installé sur un ordinateur doté de Kaspersky Security Center 12 Web Console. Dans ce cas, les fonctions du plug-in Internet sont accessibles à tous les administrateurs qui ont accès à la Web Console dans le navigateur. Vous pouvez consulter la liste des plug-ins Internet installés dans l'interface de Web Console (**Paramètres de la console** → **Plug-ins**). Pour en savoir plus sur la compatibilité des versions des plug-ins Internet et de Web Console, consultez l'[aide de Kaspersky Security Center](#).

Installation d'un plug-in Internet

Vous pouvez installer le plug-in Internet selon un des moyens suivants :

- Installer le plug-in Internet à l'aide de l'assistant de configuration initiale de Kaspersky Security Center 12 Web Console.

Web Console propose automatiquement de lancer l'Assistant de configuration initiale lors de la première connexion de Web Console au Serveur d'administration. Vous pouvez aussi lancer l'Assistant de configuration initiale dans l'interface de Web Console (**Détection d'appareils et déploiement** → **Déploiement et cible** → **Assistant de configuration initiale**). L'Assistant de configuration initiale peut également vérifier l'actualité des plug-ins Internet installés et charger les mises à jour indispensables. Pour en savoir plus sur l'Assistant de configuration initiale de Kaspersky Security Center 12 Web Console, consultez l'[aide de Kaspersky Security Center](#).

- Installer le plug-in Internet de la liste des paquets de distribution accessibles dans Web Console.

Pour installer un plug-in Internet, il faut choisir le paquet de distribution du plug-in Internet Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console** → **Plug-ins**). La liste des paquets de distribution disponibles se renouvelle automatiquement après l'émission des nouvelles versions des applications de Kaspersky.

- Télécharger les paquets de distribution dans Web Console depuis une source externe.

Pour installer le plug-in Internet, il faut ajouter l'archive ZIP du paquet de distribution de plug-in de Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console** → **Plug-ins**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site Internet de Kaspersky.

Mise à jour du plug-in d'administration

Pour mettre à jour le plug-in d'administration de Kaspersky Endpoint Security for Windows, vous devez télécharger sa dernière version (incluse dans [le paquet de distribution](#)) et exécuter l'assistant d'installation du plug-in.

Quand une nouvelle version d'un plug-in Internet apparaît, Web Console affiche la notification *Mises à jour disponibles pour les plug-ins utilisés*. Vous pouvez passer à la mise à jour de la version du plug-in Internet depuis la notification de Web Console. Vous pouvez aussi rechercher la présence éventuelle de mises à jour du plug-in Internet manuellement dans l'interface de Web Console (**Paramètres de la Console** → **Plug-ins**). La version précédente du plug-in Internet est automatiquement supprimée pendant la mise à jour.

Lors de la mise à jour du plug-in Internet, les éléments existants sont conservés (par exemple, les stratégies ou les tâches). Les nouveaux paramètres des éléments qui remplissent de nouvelles fonctions de Kaspersky Endpoint Security apparaissent dans les éléments existants et affichent une valeur par défaut.

Vous pouvez mettre à jour le plug-in Internet d'une des manières suivantes :

- Mettre à jour le plug-in Internet en ligne dans la liste des plug-ins Internet.

Pour mettre à jour un plug-in Internet, il faut choisir le paquet de distribution du plug-in Internet Kaspersky Endpoint Security dans l'interface de Web Console et lancer la mise à jour (**Paramètres de la Console** → **Plug-ins**). Web Console recherche la présence éventuelle de mises à jour sur les serveurs de Kaspersky et télécharge les mises à jour nécessaires.

- Mettre à jour le plug-in Internet depuis un fichier.

Pour mettre à jour le plug-in Internet, il faut sélectionner l'archive ZIP du paquet de distribution de plug-in de Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console** → **Plug-ins**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site Internet de Kaspersky. Vous pouvez mettre à jour le plug-in Internet de Kaspersky Endpoint Security seulement jusqu'à une version plus récente. Il est impossible de mettre à jour le plug-in Internet jusqu'à une version plus ancienne.

À l'ouverture de n'importe quel élément (par exemple, une stratégie ou une tâche), le plug-in Internet analyse les informations sur la compatibilité. Si la version du plug-in Internet est égale ou supérieure à la version indiquée dans les informations sur la compatibilité, vous pouvez modifier les paramètres de cet élément. Dans le cas contraire, la modification des paramètres de l'élément sélectionné via le plug-in Internet est inaccessible. Il est conseillé de mettre à jour le plug-in Internet.

Particularités de l'utilisation de plug-ins d'administration de différentes versions

Pour administrer l'application Kaspersky Endpoint Security via Kaspersky Security Center, il faut disposer d'un plug-in d'administration d'une version égale ou supérieure à celle indiquée dans les informations de compatibilité de Kaspersky Endpoint Security avec le plug-in d'administration. Vous pouvez regarder la version minimale requise du plug-in d'administration dans le fichier installer.ini qui fait partie de la [distribution](#).

À l'ouverture de n'importe quel élément (par exemple, une stratégie ou une tâche), le plug-in d'administration vérifie les informations sur la compatibilité. Si la version du plug-in d'administration est égale ou supérieure à la version indiquée dans les informations sur la compatibilité, vous pouvez modifier les paramètres de cet élément. Dans le cas contraire, la modification des paramètres de l'élément sélectionné via le plug-in d'administration est inaccessible. Il est recommandé de mettre à jour le plug-in d'administration.

Mise à jour du plug-in d'administration de Kaspersky Endpoint Security 10 for Windows

Si le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows est installé dans la Console d'administration, l'installation du plug-in d'administration pour Kaspersky Endpoint Security 11 for Windows possède les particularités suivantes :


- Le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows n'est pas supprimé et demeure disponible pour l'utilisation. Par conséquent, vous aurez accès à deux plug-ins d'administration pour utiliser les versions 10 et 11 de l'application.
- Le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows ne prend pas en charge l'administration de l'application Kaspersky Endpoint Security 10 for Windows sur les ordinateurs des utilisateurs.
- Le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows ne prend pas en charge les éléments (par exemple, une stratégie ou une tâche), créés à l'aide du plug-in d'administration Kaspersky Endpoint Security 10 for Windows.

Vous pouvez utiliser l'Assistant de conversion de masse des stratégies et des tâches pour convertir les stratégies et les tâches de la version 10 à la version 11. Pour en savoir plus sur la conversion de stratégies et de tâches, veuillez consulter l'[aide de Kaspersky Security Center](#).



Mise à jour du plug-in d'administration de Kaspersky Endpoint Security 11 for Windows

Si le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows est installé dans la Console d'administration, l'installation de la nouvelle version du plug-in d'administration pour Kaspersky Endpoint Security 11 for Windows possède les particularités suivantes :

- La version précédente du plug-in d'administration de Kaspersky Endpoint Security 11 for Windows est supprimée.
- Le plug-in d'administration de Kaspersky Endpoint Security 11 pour Windows d'une nouvelle version prend en charge l'administration de l'application Kaspersky Endpoint Security 11 for Windows de la version antérieure sur les ordinateurs des utilisateurs.
- Grâce au plug-in d'administration de la nouvelle version, vous pouvez modifier les paramètres dans les stratégies, les tâches etc., créée par le plug-in d'administration de la version antérieure.
- Pour les nouveaux paramètres, le plug-in d'administration de la nouvelle version définit les valeurs par défaut lors du premier enregistrement d'une stratégie, d'un profil de stratégie ou d'une tâche.

Après la mise à jour du plug-in d'administration, il est conseillé de vérifier et d'enregistrer les valeurs des nouveaux paramètres dans les stratégies et les profils de stratégie. Dans le cas contraire, les nouveaux groupes de paramètres de Kaspersky Endpoint Security sur l'ordinateur de l'utilisateur prendront les valeurs par défaut et pourront être modifiés (attribut ). Il est conseillé de débiter le contrôle par les stratégies et les profils de stratégie du niveau supérieur de la hiérarchie. Il est également recommandé d'utiliser le compte utilisateur autorisé à accéder à toutes les zones fonctionnelles Kaspersky Security Center.

Pour en savoir plus sur les nouvelles fonctions de l'application, consultez les Notes de version ou l'[aide de l'application](#).

- Si un nouveau paramètre a été ajouté à un groupe de paramètres dans la nouvelle version du plug-in d'administration, l'attribut /  affecté antérieurement à ce groupe ne change pas.

- Lors de la mise à niveau du plug-in d'administration vers la version 11.2.0, vous devez ouvrir une stratégie pour procéder à une conversion automatique. Dans ce cas, Kaspersky Endpoint Security vous demandera de confirmer votre participation à KSN. Si vous avez déjà mis à niveau l'application vers la version 11.20 sur les ordinateurs de votre organisation, la participation à KSN sera désactivée jusqu'à ce que vous acceptiez les conditions de participation à KSN.

Considérations particulières lors de l'utilisation de protocoles chiffrés pour l'interaction avec des services externes

Kaspersky Endpoint Security et Kaspersky Security Center utilisent un canal de communication chiffré avec le protocole TLS (Transport Layer Security) pour travailler avec les services externes de Kaspersky. Kaspersky Endpoint Security utilise des services externes pour les fonctionnalités suivantes :

- Mise à jour des bases de données et des modules de l'application ;
- Activation de l'application à l'aide d'un code d'activation (activation 2.0) ;
- Utilisation de Kaspersky Security Network.

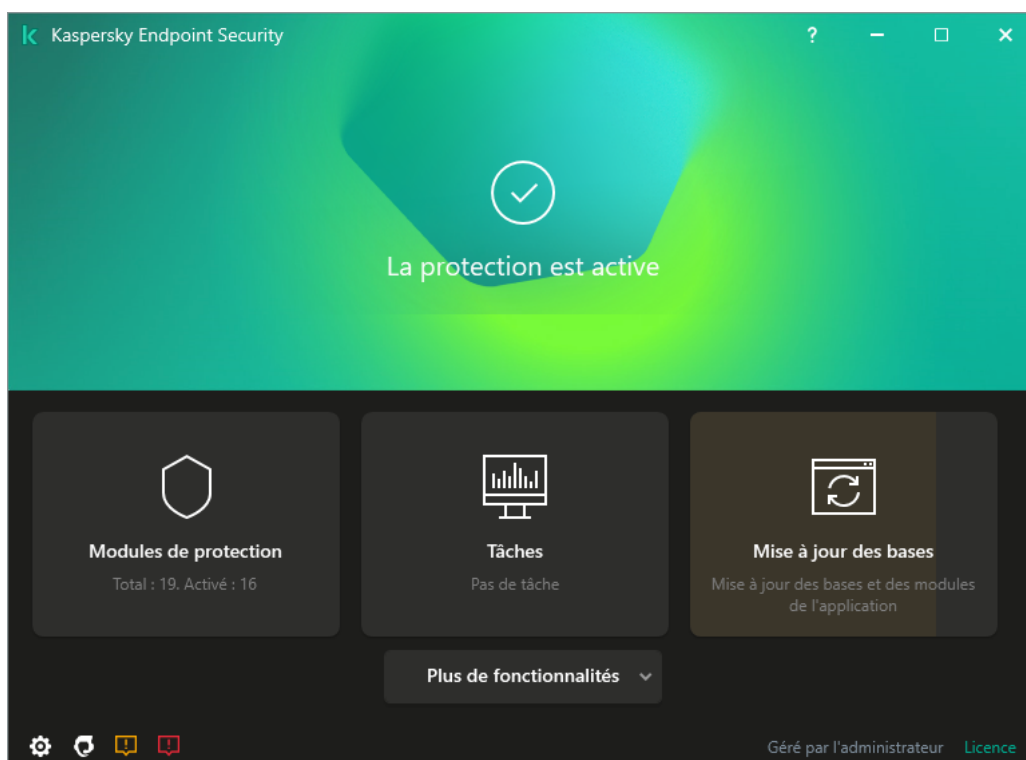
L'utilisation du protocole TLS sécurise l'application et offre les fonctionnalités suivantes :

- Chiffrement. Le contenu des messages est confidentiel et n'est pas divulgué aux utilisateurs tiers.
- Intégrité. Le destinataire du message est certain que le contenu du message n'a pas été modifié depuis que le message a été transmis par l'expéditeur.
- Authentification. Le destinataire est certain que la communication est établie uniquement avec un serveur Kaspersky de confiance.

Kaspersky Endpoint Security utilise des certificats à clé publique pour l'authentification des serveurs. Une infrastructure à clés publiques (ICP) est requise pour pouvoir travailler avec les certificats. Une autorité de certification fait partie d'une ICP. Kaspersky utilise sa propre autorité de certification, car les services de Kaspersky sont très techniques et non publics. Dans ce cas, lorsque les certificats racines de Thawte, VeriSign, GlobalTrust et autres sont révoqués, l'ICP de Kaspersky reste opérationnelle sans interruption.




Les environnements dotés de MITM (outils logiciels et matériels qui prennent en charge l'analyse du protocole HTTPS) sont considérés comme étant peu sûrs par Kaspersky Endpoint Security. Il se peut que des erreurs se produisent lors de l'utilisation des services de Kaspersky. Par exemple, il peut y avoir des erreurs concernant l'utilisation de certificats auto-signés. Ces erreurs peuvent se produire parce qu'un outil d'inspection HTTPS de votre environnement ne reconnaît pas l'ICP de Kaspersky. Pour remédier à ces problèmes, vous devez configurer des [exclusions portant sur l'interaction avec les services externes](#).

Interface de l'application



Fenêtre principale de l'application

| | |
|---------------------------------|---|
| Modules de la protection | <p>État de fonctionnement des modules installés. Vous pouvez également procéder à la configuration de tous les modules installés, à l'exception des modules de chiffrement.</p> |
| Tâches | <p>Gérez les tâches d'analyse de Kaspersky Endpoint Security. Vous pouvez effectuer une analyse antivirus et un contrôle d'intégrité de l'application. Un administrateur peut masquer des tâches à un utilisateur ou restreindre la gestion des tâches.</p> |
| Mise à jour des bases | <p>Gérez les tâches de mise à jour de Kaspersky Endpoint Security. Vous pouvez mettre à jour les bases de données antivirus et les modules d'application, et annuler la dernière mise à jour. Un administrateur peut masquer des tâches à un utilisateur ou restreindre la gestion des tâches.</p> |
| Plus de fonctionnalités | <p>Passez aux autres fonctionnalités de l'application.</p> <ul style="list-style-type: none"> • Rapports. Consultez les événements qui se sont produits pendant le fonctionnement de l'application, les modules individuels et les tâches. • Sauvegarde et restauration. Consultez la liste des copies sauvegardées des fichiers infectés que l'application a supprimés. • Technologies de détection des menaces. Consultez les informations relatives aux technologies de détection des menaces et au nombre de menaces détectées par ces technologies. • Kaspersky Security Network. État de la connexion entre Kaspersky Endpoint Security et Kaspersky Security Network, et statistiques globales de KSN. <i>Kaspersky Security Network (KSN)</i> est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite. Si vous participez au Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la catégorie et la réputation des fichiers analysés, ainsi que sur la réputation des adresses Internet analysées. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Surveillance du système. Consultez les informations relatives au fonctionnement des applications installées. La Surveillance du système contrôle les événements liés à l'application qui implique des fichiers, la base de registre ou le système d'exploitation. • Surveillance du réseau. Consultez les informations relatives à l'activité réseau de l'ordinateur en temps réel. • Surveillance du chiffrement. Surveille en temps réel le processus de chiffrement ou de déchiffrement du disque. L'outil Surveillance du chiffrement est accessible si le module Kaspersky Disk Encryption ou le module BitLocker Drive Encryption est installé. |
|  | Configurez l'application. Un administrateur peut interdire la modification des paramètres de Kaspersky Security Center . |
|  | Informations relatives à l'application : version actuelle de Kaspersky Endpoint Security, date de publication de la base de données, clé et autres informations. Vous pouvez également consulter les ressources d'information de Kaspersky qui proposent des renseignements utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. |
|  | Messages contenant des informations sur les mises à jour disponibles, et les demandes d'accès à des fichiers et à des appareils chiffrés. |
| Licence | Licence de l'application. Vous pouvez acheter une licence , activer l'application ou renouveler un abonnement . Vous pouvez également afficher des informations sur la licence actuelle . |





Icône de l'application dans la zone de notification

Dès que Kaspersky Endpoint Security a été installé, l'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows.

L'icône de l'application remplit les fonctions suivantes :

- elle indique le fonctionnement de l'application ;
- elle permet d'accéder au menu contextuel de l'icône de l'application et à la fenêtre principale de l'application.

Les états suivants de l'icône de l'application renseignent l'utilisateur sur le fonctionnement de l'application :

- L'icône  indique que tous les modules de la protection de l'application critiques sont activés. Kaspersky Endpoint Security affiche un avertissement  si l'utilisateur doit effectuer une action, par exemple, redémarrer l'ordinateur après la mise à jour de l'application.
- L'icône  indique que le fonctionnement des modules de la protection de l'application critiques a été suspendu ou interrompu. Le fonctionnement des modules de la protection peut être interrompu, par exemple, si la licence a expiré ou si un dysfonctionnement est survenu dans l'application. Kaspersky Endpoint Security affiche un avertissement  qui décrit le problème de protection de l'ordinateur.

Le menu contextuel de l'icône de l'application reprend les options suivantes :

- **Kaspersky Endpoint Security for Windows.** Ouvre la fenêtre principale de l'application. Cette fenêtre permet de gérer le fonctionnement des modules et des tâches de l'application, et de consulter les statistiques relatives aux fichiers traités et aux menaces détectées.

- **Suspendre la protection/Rétablir la protection.** Suspension de tous les modules de la protection et de contrôle qui ne sont pas accompagnés d'un cadenas dans la stratégie (🔒). Avant de réaliser cette opération, il est conseillé de désactiver la stratégie de Kaspersky Security Center.

Avant la suspension des modules de la protection et de contrôles, l'application sollicite le [mot de passe d'accès à Kaspersky Endpoint Security](#) (mot de passe du compte utilisateur ou mot de passe temporaire). Ensuite, vous pouvez sélectionner la période de suspension : à l'heure indiquée, avant le redémarrage ou à la demande de l'utilisateur.

Cet élément du menu contextuel est disponible si la [protection par mot de passe est activée](#). Pour réactiver les modules de la protection et de contrôle, sélectionnez l'option **Rétablir la protection** dans le menu contextuel de l'application.

La suspension des modules de la protection et de contrôle n'affecte pas l'exécution des tâches de mise à jour et d'analyse. L'application continue également à utiliser Kaspersky Security Network.

- **Désactiver la stratégie/Activer la stratégie.** Désactive la stratégie de Kaspersky Security Center sur l'ordinateur. Tous les paramètres de Kaspersky Endpoint Security peuvent être configurés, même les paramètres accompagnés d'un cadenas dans la stratégie (🔒). Lors de la désactivation de la stratégie, l'application sollicite le [mot de passe d'accès à Kaspersky Endpoint Security](#) (mot de passe du compte utilisateur ou mot de passe temporaire). Cet élément du menu contextuel est disponible si la [protection par mot de passe est activée](#). Pour activer une stratégie, sélectionnez l'élément **Activation de la stratégie** dans le menu contextuel de l'application.
- **Paramètres.** La fenêtre de configuration de l'application s'ouvre.
- **Assistance.** Ouverture de la fenêtre **Assistance** qui contient les informations requises pour contacter le Support Technique de Kaspersky.
- **À propos de l'application.** Ouvre une fenêtre contenant des informations sur l'application.
- **Quitter.** Entraîne l'arrêt de Kaspersky Endpoint Security. Si vous choisissez cette option du menu contextuel, l'application est déchargée de la mémoire vive de l'ordinateur.



Menu contextuel de l'icône de l'application

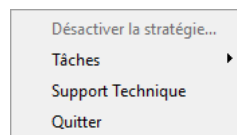
Interface de l'application simplifiée

Si l'ordinateur client doté de l'application Kaspersky Endpoint Security est soumis à une stratégie de Kaspersky Security Center qui prévoit [l'affichage de l'interface tronquée de l'application](#), la fenêtre principale de l'application n'est pas accessible sur ce poste client. D'un clic droit, l'utilisateur peut ouvrir le menu contextuel de l'icône de Kaspersky Endpoint Security (cf. ill. ci-dessous) qui contient les options suivantes :

- **Désactiver la stratégie/Activer la stratégie.** Désactive la stratégie de Kaspersky Security Center sur l'ordinateur. Tous les paramètres de Kaspersky Endpoint Security peuvent être configurés, même les paramètres accompagnés d'un cadenas dans la stratégie (🔒). Lors de la désactivation de la stratégie, l'application sollicite le [mot de passe d'accès à Kaspersky Endpoint Security](#) (mot de passe du compte utilisateur ou mot de passe temporaire). Cet élément du menu contextuel est disponible si la [protection par mot](#)

[de passe est activée](#). Pour activer une stratégie, sélectionnez l'élément **Activation de la stratégie** dans le menu contextuel de l'application.

- **Tâches**. Liste déroulante contenant les éléments suivants :
 - **Vérification de l'intégrité**.
 - **Restauration de la dernière mise à jour**.
 - **Analyse complète**.
 - **Analyse personnalisée**.
 - **Analyse des zones critiques**.
 - **Mise à jour**.
- **Assistance**. Ouverture de la fenêtre **Assistance** qui contient les informations requises pour contacter le Support Technique de Kaspersky.
- **Quitter**. Entraîne l'arrêt de Kaspersky Endpoint Security. Si vous choisissez cette option du menu contextuel, l'application est déchargée de la mémoire vive de l'ordinateur.



Menu contextuel de l'icône de l'application lors de l'affichage de l'interface simplifiée de l'application

Configuration de l'affichage de l'interface de l'application

Vous pouvez configurer l'affichage de l'interface de l'application pour l'utilisateur de l'ordinateur. L'utilisateur peut interagir avec l'application des manières suivantes :

- **Avec interface simplifiée**. La fenêtre principale de l'application n'est pas disponible sur l'ordinateur client. Seule [l'icône de la zone de notification Windows est disponible](#). Le menu contextuel de l'icône permet à l'utilisateur d'[effectuer une série limitée d'opérations avec Kaspersky Endpoint Security](#). Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.
- **Avec interface complète**. La fenêtre principale de Kaspersky Endpoint Security et [l'icône de la zone de notification Windows sont](#) disponibles sur l'ordinateur client. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer des opérations avec Kaspersky Endpoint Security. Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.
- **Sans interface**. L'ordinateur client n'affiche aucun élément pouvant indiquer le fonctionnement de Kaspersky Endpoint Security. De même, [l'icône dans la zone de notification Windows](#) et les notifications ne sont pas disponibles.

[Configuration de l'affichage de l'interface de l'application dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.
6. Dans le groupe **Interaction avec l'utilisateur**, exécutez une des actions suivantes :
 - Cochez la case **Afficher l'interface de l'application** si vous souhaitez que les éléments suivants de l'interface s'affichent sur l'ordinateur client :
 - le dossier portant le nom de l'application dans le menu **Démarrer** ;
 - [l'icône de Kaspersky Endpoint Security](#) dans la zone de notification de la barre des tâches de Microsoft Windows ;
 - les pops-ups de notification.
 - Décochez la case **Afficher l'interface de l'application** si vous voulez cacher tous les signes de fonctionnement de Kaspersky Endpoint Security sur l'ordinateur client.
7. Dans le groupe **Interaction avec l'utilisateur**, cochez la case **Interface de l'application simplifiée** si vous voulez que [l'interface de l'application simplifiée](#) s'affiche sur l'ordinateur client doté de Kaspersky Endpoint Security.

[Configuration de l'affichage de l'interface de l'application dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez activer l'utilisation du mode portable.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez **Paramètres généraux** → **Interface**.
5. Dans la section **Interaction avec l'utilisateur**, configurez l'affichage de l'interface de l'application :
 - **Avec interface simplifiée.** La fenêtre principale de l'application n'est pas disponible sur l'ordinateur client. Seule l'[icône de la zone de notification Windows est disponible](#). Le menu contextuel de l'icône permet à l'utilisateur d'[effectuer une série limitée d'opérations avec Kaspersky Endpoint Security](#). Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.
 - **Avec interface complète.** La fenêtre principale de Kaspersky Endpoint Security et l'[icône de la zone de notification Windows sont](#) disponibles sur l'ordinateur client. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer des opérations avec Kaspersky Endpoint Security. Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.
 - **Sans interface.** L'ordinateur client n'affiche aucun élément pouvant indiquer le fonctionnement de Kaspersky Endpoint Security. De même, l'[icône dans la zone de notification Windows](#) et les notifications ne sont pas disponibles.
6. Cliquez sur le bouton **OK**.

Guide de démarrage

Après le déploiement de l'application sur les ordinateurs client, il est nécessaire de réaliser les opérations suivantes pour pouvoir utiliser Kaspersky Endpoint Security depuis Kaspersky Security Center :

- Créer et configurer une stratégie.

Les stratégies permettent de définir des valeurs identiques pour les paramètres de fonctionnement de Kaspersky Endpoint Security sur tous les postes clients appartenant au groupe d'administration. L'Assistant de configuration initiale de Kaspersky Security Center crée automatiquement une stratégie pour Kaspersky Endpoint Security.

- Créer les tâches *Mise à jour* et *Recherche de virus*.

La tâche *Mise à jour* est nécessaire pour maintenir l'actualité de la protection de l'ordinateur. Lors de l'exécution de la tâche, Kaspersky Endpoint Security [met à jour les bases antivirus et les modules de l'application](#). La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center. Pour créer la tâche *Mises à jour* pendant l'exécution de l'assistant, installez le plug-in Internet de Kaspersky Endpoint Security for Windows.

La tâche *Recherche de virus* est requise afin de détecter en temps utiles les virus et autres programmes dangereux. Il faut créer la tâche *Recherche de virus* manuellement.

[Procédure de création d'une tâche Recherche de virus dans la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Choisissez **Kaspersky Endpoint Security for Windows (11.6.0)** → **Recherche de virus**.

Étape 2. Zone d'analyse

Composez une liste d'objets que Kaspersky Endpoint Security va analyser pendant l'exécution de la tâche.

Étape 3. Action de Kaspersky Endpoint Security

Choisissez l'action à réaliser en cas de détection d'une menace :

- **Désinfecter ; supprimer si la désinfection est impossible.** Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.
- **Désinfecter ; informer si la désinfection est impossible.** Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.
- **Informer.** Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.
- **Exécuter la désinfection de l'infection active immédiatement.** Quand cette case est cochée, Kaspersky Endpoint Security utilise la technologie désinfection de l'infection active pendant l'analyse.

La *technologie de désinfection avancée* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui empêchent Kaspersky Endpoint Security de les supprimer à l'aide d'autres méthodes. La menace est ainsi neutralisée. Pendant l'exécution de la désinfection de l'infection active, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registre du système d'exploitation. La technologie de désinfection avancée est gourmande en ressource et peut ralentir d'autres applications. À l'issue de la désinfection de l'infection active, Kaspersky Endpoint Security redémarre l'ordinateur sans demander la confirmation de l'utilisateur.

Définissez le mode de lancement de l'analyse à l'aide de la case **Exécuter uniquement lorsque l'ordinateur est inactif**. La case active/désactive la suspension de la tâche *Recherche de virus* si les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security suspend la tâche *Recherche de virus* tant que l'écran de veille n'est pas activé et que l'ordinateur n'a pas été débloqué.

Étape 4. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 5. Sélection du compte utilisateur pour lancer la tâche

Sélectionnez un compte pour exécuter la tâche de *Recherche de virus*. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local. Si la zone d'analyse comprend des disques réseau ou d'autres objets dont l'accès est restreint, sélectionnez un compte utilisateur doté des autorisations requises.

Étape 6. Configuration de la planification du lancement de la tâche

Planifiez le lancement des tâches, par exemple, manuellement ou après le chargement des bases antivirus dans le référentiel.

Étape 7. Définition du nom de la tâche

Saisissez un nom de tâche, par exemple, *Analyse complète quotidiennes*.

Étape 8. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. La recherche de virus est alors exécutée sur les ordinateurs de l'utilisateur conformément à la planification définie.

[Comment créer une tâche Recherche de virus dans Web Console ?](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

b. Dans la liste déroulante **Type de tâche**, choisissez **Recherche de virus**.

c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, **Analyse hebdomadaire**.

d. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

La nouvelle tâche apparaît dans la liste des tâches.

6. Pour configurer la planification de l'exécution de la tâche, accédez aux propriétés de la tâche.

Il est conseillé de planifier l'exécution d'une tâche au moins une fois par semaine.

7. Cochez la case en regard de la tâche.

8. Cliquez sur le bouton **Démarrer**.

Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

La recherche de virus est alors exécutée sur les ordinateurs de l'utilisateur conformément à la planification définie.

Administration des stratégies

La *stratégie* est un ensemble de paramètres du fonctionnement de l'application, défini pour un groupe d'administration. Il est possible de configurer plusieurs stratégies avec des valeurs différentes pour une application. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes d'administration. Une stratégie propre à l'application peut être créée dans chaque groupe d'administration.

Les paramètres de la stratégie sont transmis aux ordinateurs client à l'aide de l'Agent d'administration lors de la *synchronisation*. Par défaut, le Serveur d'administration exécute la synchronisation directement après une modification des paramètres de la stratégie. La synchronisation s'opère via le port UDP 15000 sur l'ordinateur client. Le Serveur d'administration réalise par défaut une synchronisation toutes les 15 minutes. En cas d'échec de la synchronisation après la modification des paramètres d'une stratégie, la prochaine tentative de synchronisation est réalisée selon la planification définie.

Stratégie active et inactive

La stratégie est prévue pour un groupe d'appareils administrés et peut être activée ou inactivée. Les paramètres de la stratégie active sont conservés sur les ordinateurs clients lors de la synchronisation. Il est impossible d'appliquer simultanément plusieurs stratégies à un ordinateur et pour cette raison, il ne peut y avoir qu'une stratégie active par groupe.



Vous pouvez créer une quantité non limitée de stratégies inactives. Une stratégie inactive n'a aucun impact sur les paramètres de l'application sur les ordinateurs du réseau. Les stratégies inactives sont prévues pour faire face à des situations extraordinaires, comme une attaque de virus. Ainsi, en cas d'attaque via des disques flash, vous pouvez activer une stratégie qui bloque l'accès aux disques flash. Dans ce cas, la stratégie active devient automatiquement inactive.

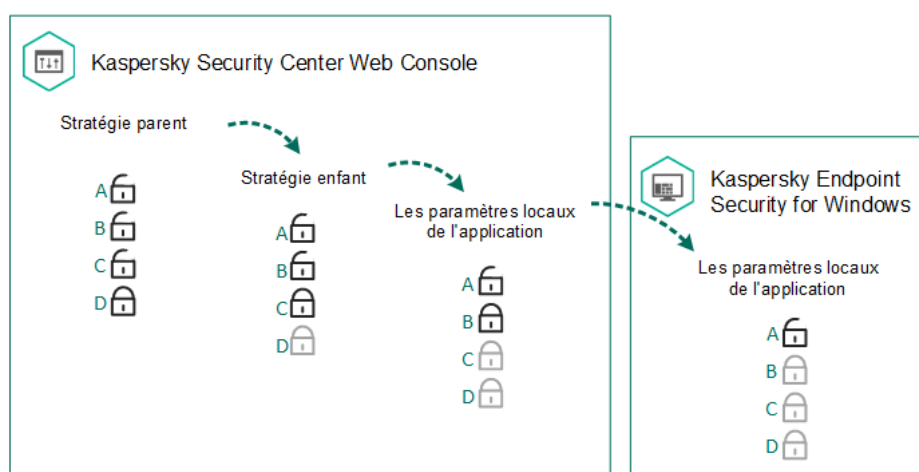
Stratégie pour les utilisateurs autonomes

La stratégie pour les utilisateurs autonomes est activée quand l'ordinateur quitte le périmètre du réseau de l'organisation.

Héritage des paramètres

Les stratégies, à l'instar des groupes d'administration, ont une hiérarchie. Par défaut, une stratégie enfant hérite des paramètres de la stratégie parent. La *stratégie enfant* est une stratégie de niveau inférieur, à savoir une stratégie pour les sous-groupes d'administration et les Serveur d'administration secondaires. Vous pouvez désactiver l'héritage des paramètres de la stratégie parent.

Chaque paramètre présenté dans une stratégie possède l'attribut  qui indique si la modification du paramètre dans les stratégies enfant et dans les [paramètres locaux de l'application](#) est autorisée. L'attribut  fonctionne uniquement si l'héritage des paramètres de la stratégie parent est activé dans la stratégie enfant. Les stratégies pour les utilisateurs autonomes ne fonctionnent pas selon la hiérarchie des groupes d'administration sur d'autres stratégies.



Héritage des paramètres




Les autorisations d'accès aux paramètres de la stratégie (lecture, modification, exécution) sont définies pour chaque utilisateur qui a accès au Serveur d'administration de Kaspersky Security Center, et séparément pour chaque zone de fonction de Kaspersky Endpoint Security. Pour configurer les autorisations d'accès aux paramètres de la stratégie, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration de Kaspersky Security Center.

Création d'une stratégie

Création d'une stratégie dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients qui vous intéressent.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Cliquez sur le bouton **Nouvelle stratégie**.
L'Assistant de création de la stratégie démarre.
5. Suivez les instructions de l'Assistant de création de stratégie.

Création d'une stratégie dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le bouton **Ajouter**.
L'Assistant de création de la stratégie démarre.
3. Choisissez l'application Kaspersky Endpoint Security, puis cliquez sur **Suivant**.
4. Lisez la Déclaration de Kaspersky Security Network (KSN) et acceptez-la, puis cliquez sur **Suivant**.
5. Sous l'onglet **Général**, exécutez les actions suivantes :
 - modifier le nom de la stratégie ;
 - Sélectionner l'état d'une stratégie :
 - **Active**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.
 - **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.
 - **Pour les utilisateurs autonomes**. La stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.
 - configurer l'héritage des paramètres :
 - **Hériter des paramètres de la stratégie parent**. Si le commutateur est activé, les paramètres de la stratégie sont hérités de la stratégie du niveau supérieur de la hiérarchie. Les paramètres de la stratégie ne peuvent être modifiés si  est activé dans la stratégie parent.
 - **Appliquer l'héritage forcé des paramètres pour les stratégies enfants**. Si le commutateur est activé, les paramètres de la stratégie sont appliqués aux stratégies enfants. Dans les propriétés de la stratégie enfant, le commutateur **Hériter des paramètres de stratégie parent** est automatiquement activé et ne peut pas être désactivé. Les paramètres de la stratégie enfant sont hérités de la stratégie parent, sauf les paramètres accompagnés de . Les paramètres des stratégies enfant ne peuvent pas être modifiés si  est activé dans la stratégie parent.
6. L'onglet **Paramètres de l'application** permet de configurer les [paramètres de la stratégie de Kaspersky Endpoint Security](#).
7. Cliquez sur le bouton **Enregistrer**.

Les paramètres de Kaspersky Endpoint Security sont configurés sur les ordinateurs client à la synchronisation suivante. Vous pouvez afficher des informations sur la stratégie appliquée à l'ordinateur dans l'interface de Kaspersky Endpoint Security en cliquant sur le bouton **Assistance** de l'écran principal (par exemple, le nom de la stratégie). Pour ce faire, dans les paramètres de la stratégie de l'Agent d'administration, vous devez activer l'obtention de données de stratégie étendues. Pour en savoir plus sur la stratégie de l'Agent d'administration, consultez l'[aide de Kaspersky Security Center](#).

Indicateur du niveau de protection

L'indicateur du niveau de protection apparaît dans la partie supérieure de la fenêtre **Propriétés : <Nom de la stratégie>**. L'indicateur peut prendre une des valeurs suivantes :

- **Niveau de protection élevé.** L'indicateur prend cette valeur et devient vert si tous les modules des catégories suivantes sont activés :
 - **Critique.** Cette catégorie contient les modules suivants :
 - Protection contre les fichiers malicieux.
 - Détection comportementale.
 - Protection contre les Exploits.
 - Réparation des actions malicieuses.
 - **Importants.** Cette catégorie contient les modules suivants :
 - Kaspersky Security Network.
 - Protection contre les menaces Internet.
 - Protection contre les menaces par emails.
 - Prévention des intrusions.
- **Niveau de protection moyen.** L'indicateur prend cette valeur et devient jaune si un module important est désactivé.
- **Niveau de protection faible.** L'indicateur prend cette valeur et devient rouge dans un des cas suivants :
 - un ou plusieurs modules critiques sont désactivés ;
 - deux ou plusieurs modules importants sont désactivés.

Si l'indicateur possède la valeur **Niveau de protection moyen** ou **Niveau de protection faible**, un lien qui permet d'ouvrir la fenêtre **Modules de la protection recommandés** apparaît à droite. Cette fenêtre permet d'activer n'importe quel module de la protection recommandé.

Gestion de la tâche

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration ;
- des tâches pour la sélection d'ordinateurs.

Vous pouvez créer n'importe quelle quantité de tâches de groupe, de tâches pour une sélection d'ordinateurs et de tâches locales. Pour en savoir plus sur l'utilisation des groupes d'administration et des sélections d'ordinateurs, consultez l'[aide de Kaspersky Security Center](#).

Kaspersky Endpoint Security prend en charge l'exécution des tâches suivantes :

- **Recherche de virus.** Kaspersky Endpoint Security recherche la présence éventuelle de virus et d'autres programmes dangereux dans les secteurs de l'ordinateur définis via les paramètres de la tâche. La tâche *Recherche de virus* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale. Il est conseillé de planifier l'exécution d'une tâche au moins une fois par semaine.
- **Ajout d'une clé.** Kaspersky Endpoint Security ajoute la clé pour l'activation des applications, y compris une clé complémentaire. Avant d'exécuter une tâche, confirmez que le nombre d'ordinateurs auxquels la tâche sur lesquels la tâche va être exécutée ne dépasse pas le nombre d'ordinateurs couverts par la licence.
- **Modification du contenu du module de l'application.** Kaspersky Endpoint Security installe ou supprime les modules sur les ordinateurs client selon la liste des modules indiquée dans les paramètres de la tâche. Il est impossible de supprimer le module Protection contre les fichiers malicieux. La composition optimale de modules de Kaspersky Endpoint Security permet d'économiser les ressources de l'ordinateur.
- **Inventaire.** Kaspersky Endpoint Security récupère des informations sur tous les fichiers exécutables des applications de l'ordinateur. La tâche *Inventaire* est à charge du module Contrôle des applications. Si le module Contrôle des applications n'est pas installé, la tâche se solde sur un échec.
- **Mise à jour.** Kaspersky Endpoint Security met à jour les bases et les modules de l'application. La tâche *Mise à jour* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale. Il est recommandé de planifier l'exécution d'une tâche au moins une fois par jour.
- **Suppression des données.** Kaspersky Endpoint Security supprime les fichiers et les dossiers des ordinateurs des utilisateurs immédiatement ou en cas d'absence prolongée d'une connexion avec Kaspersky Security Center.
- **Restauration de la mise à jour.** Kaspersky Endpoint Security revient à la dernière mise à jour des bases de données et des modules de l'application. Cela peut être nécessaire, par exemple, si les nouvelles bases contiennent des données incorrectes qui pourraient amener Kaspersky Endpoint Security à bloquer une application inoffensive.
- **Vérification de l'intégrité.** Kaspersky Endpoint Security analyse les fichiers de l'application, vérifie si les fichiers ont été endommagés ou modifiés et vérifie les signatures numériques des fichiers d'application.
- **Administration des comptes de l'Agent d'authentification.** Kaspersky Endpoint Security configure les paramètres des comptes utilisateur de l'Agent d'authentification. L'Agent d'authentification est nécessaire pour utiliser les disques chiffrés. L'utilisateur doit s'authentifier à l'aide de l'agent avant le chargement du système d'exploitation.

Les tâches sont lancées sur l'ordinateur uniquement si [l'application Kaspersky Endpoint Security est lancée](#).

Création d'une tâche

[Création d'une tâche dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Choisissez le dossier **Tâches** dans l'arborescence de la Console de l'administration.
3. Cliquez sur le bouton **Nouvelle tâche**.
L'Assistant de création de tâche démarre.
4. Suivez les instructions de l'Assistant de création de tâche.

Création d'une tâche d'installation à distance dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.
La liste des tâches s'ouvre.
2. Cliquez sur le bouton **Ajouter**.
L'Assistant de création de tâche démarre.
3. Configurez les paramètres de la tâche :
 - a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.
 - b. Dans la liste déroulante **Type de tâche**, choisissez la tâche que vous voulez lancer sur les ordinateurs des utilisateurs.
 - c. Dans le champ **Nom de tâche**, saisissez une courte description, par exemple, **Mise à jour de l'application de comptabilité**.
 - d. Dans le groupe **Sélection d'appareils auxquels la tâche sera affectée**, choisissez la zone d'action de la tâche.
4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.
5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

La nouvelle tâche apparaît dans la liste des tâches. La tâche utilise les paramètres par défaut. Pour configurer les paramètres de tâche, vous devez accéder aux propriétés de celle-ci. Pour exécuter une tâche, cochez la case en regard de celle-ci, puis cliquez sur le bouton **Démarrer**. Une fois que la tâche a été lancée, vous pouvez l'arrêter et la reprendre plus tard.

La liste des tâches permet de contrôler le résultat de l'exécution d'une tâche : état de la tâche et statistiques d'exécution de la tâche sur les ordinateurs. Vous pouvez aussi créer une sélection d'événements pour le contrôle de l'exécution des tâches (**Surveillance et rapports** → **Sélections d'événements**). Pour en savoir plus sur la sélection d'événements, consultez l'[aide de Kaspersky Security Center](#). Les résultats de l'exécution des tâches sont enregistrés localement sur l'ordinateur dans le journal des événements Windows et dans les [rapports de Kaspersky Endpoint Security](#).

Administration de l'accès aux tâches

Les autorisations d'accès aux tâches de Kaspersky Endpoint Security (lecture, modification, exécution) sont définies pour chaque utilisateur qui a accès au Serveur d'administration de Kaspersky Security Center via les paramètres d'accès aux zones de fonction de Kaspersky Endpoint Security. Pour configurer l'accès aux zones de fonction de Kaspersky Endpoint Security, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur le concept de la gestion des tâches via Kaspersky Security Center, consultez l'[aide de Kaspersky Security Center](#).

Vous pouvez configurer les droits d'accès aux tâches pour les utilisateurs des ordinateurs à l'aide d'une stratégie (*mode d'utilisation des tâches*). Par exemple, vous pouvez masquer les tâches de groupe dans l'interface de Kaspersky Endpoint Security.

Configuration du mode d'utilisation des tâches dans l'interface de Kaspersky Endpoint Security via la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Tâches locales** → **Gestion de la tâche**.
6. Configurez le mode d'utilisation des tâches (cf. tableau ci-dessous).
7. Enregistrez vos modifications.

Configuration du mode d'utilisation des tâches dans l'interface locale de Kaspersky Endpoint Security


1. Dans la fenêtre principale de Web Console, choisissez l'onglet **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez activer l'utilisation du mode portable.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Accédez à la section **Tâches locales** → **Gestion de la tâche**.
5. Configurez le mode d'utilisation des tâches (cf. tableau ci-dessous).
6. Cliquez sur le bouton **OK**.
7. Confirmez la modification via le bouton **Enregistrer**.

Paramètres de gestion des tâches

| Paramètre | Description |
|--------------------------------|---|
| Autoriser l'utilisation | Si la case est cochée, les tâches locales sont affichées dans l'interface locale de Kaspersky |

| | |
|--|--|
| <p>des tâches locales</p> | <p>Endpoint Security. L'utilisateur, en l'absence de restrictions complémentaires de la stratégie, peut configurer les tâches et les lancer. Cependant, la configuration de la planification de l'exécution des tâches reste indisponible pour l'utilisateur. L'utilisateur ne peut exécuter des tâches que manuellement.</p> <p>Si la case est décochée, l'utilisation des tâches locales est interrompue. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. Les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de Kaspersky Endpoint Security ou via la ligne de commande.</p> <p>L'utilisateur peut toujours lancer la recherche de virus dans un fichier ou un dossier en choisissant l'option Rechercher d'éventuels virus dans le menu contextuel du fichier ou le dossier. Dans ce cas, la tâche d'analyse sera lancée selon les valeurs de paramètres définies par défaut pour la tâche d'analyse personnalisée.</p> |
| <p>Autoriser l'affichage des tâches de groupe</p> | <p>Si la case est cochée, les tâches de groupe sont affichées dans l'interface locale de Kaspersky Endpoint Security. L'utilisateur peut consulter la liste complète des tâches dans l'interface de l'application.</p> <p>Si cette case n'est pas cochée, Kaspersky Endpoint Security affiche une liste de tâches vide.</p> |
| <p>Autoriser la gestion des tâches de groupe</p> | <p>Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans Kaspersky Security Center. L'utilisateur peut lancer et arrêter des tâches dans l'interface de l'application ou dans l'interface simplifiée de l'application.</p> <p>Si cette case n'est pas cochée, Kaspersky Endpoint Security lance automatiquement les tâches selon la planification ou l'administrateur les lance manuellement dans Kaspersky Security Center.</p> |

Configuration des paramètres locaux de l'application

Kaspersky Security Center vous permet de configurer les paramètres de Kaspersky Endpoint Security sur un ordinateur en particulier. Il s'agit des *paramètres locaux de l'application*. La modification de certains paramètres peut être impossible. Ces paramètres sont bloqués par l'attribut  dans [les propriétés de la stratégie](#).

[Configuration des paramètres locaux de l'application dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
 2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
 3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
 4. Choisissez l'ordinateur pour lequel vous souhaitez configurer les paramètres de Kaspersky Endpoint Security.
 5. Dans le menu contextuel de l'ordinateur client, sélectionnez l'option **Propriétés**.
La fenêtre des propriétés du poste client s'ouvre.
 6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.
Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky installées sur le poste client.
 7. Choisissez l'application Kaspersky Endpoint Security.
 8. Cliquez sur le bouton **Propriétés** sous la liste des applications de Kaspersky.
La fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows** s'ouvre.
 9. Dans la section **Paramètres généraux**, configurez les paramètres de fonctionnement de Kaspersky Endpoint Security, ainsi que les paramètres des rapports et des stockages.
Les autres sections de la fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows** sont les mêmes que les sections standards de Kaspersky Security Center. Elles sont décrites en détail dans l'aide de Kaspersky Security Center.
- Si l'application est soumise à une stratégie qui interdit la modification de certains paramètres, ceux-ci ne seront pas accessibles lors de la configuration des paramètres de l'application dans la section **Paramètres généraux**.
10. Dans la fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows**, cliquez sur le bouton **OK** afin d'enregistrer les modifications.

[Configuration des paramètres locaux de l'application dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez configurer les paramètres locaux de l'application.
Les propriétés de l'ordinateur s'ouvrent.
3. Choisissez l'onglet **Applications**.
4. Cliquez sur **Kaspersky Endpoint Security for Windows**.
La fenêtre des paramètres locaux de l'application s'ouvre.
5. Choisissez l'onglet **Paramètres de l'application**.
6. Configurez les paramètres locaux de l'application.
7. Les paramètres locaux de l'application sont identiques aux [paramètres de la stratégie](#), excepté les paramètres de chiffrement.

Lancement et arrêt de Kaspersky Endpoint Security

Une fois installé sur l'ordinateur de l'utilisateur, Kaspersky Endpoint Security se lance automatiquement. Par la suite, le lancement de Kaspersky Endpoint Security a lieu par défaut directement après celui du système d'exploitation. Il n'est pas possible de configurer le lancement automatique de l'application dans les paramètres du système d'exploitation.

Le chargement des bases antivirus de Kaspersky Endpoint Security après le chargement du système d'exploitation peut durer jusqu'à deux minutes en fonction des performances (capacités techniques) de l'ordinateur. Pendant cette période, le niveau de la protection de l'ordinateur est réduit. Le chargement des bases antivirus au lancement de l'application Kaspersky Endpoint Security quand le système d'exploitation est déjà chargé n'entraîne pas de réduction du niveau de la protection de l'ordinateur.


[Configuration du lancement de Kaspersky Endpoint Security dans la Console d'administration \(MMC\)](#) ²

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Paramètres généraux** → **Paramètres de l'application**.
6. La case **Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur** permet de configurer le lancement de l'application.
7. Enregistrez vos modifications.

Configuration du lancement de Kaspersky Endpoint Security dans Web Console ?

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez configurer le lancement de l'application.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez **Paramètres généraux**.
5. Cliquez sur le lien **Paramètres de l'application**.
6. La case **Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur** permet de configurer le lancement de l'application.
7. Cliquez sur le bouton **OK**.
8. Confirmez la modification via le bouton **Enregistrer**.



Configuration du lancement de Kaspersky Endpoint Security dans l'interface d'application ?

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Utilisez la case **Lancer au démarrage de l'ordinateur** pour configurer la façon dont l'application démarre.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Les experts de Kaspersky déconseillent de quitter Kaspersky Endpoint Security car cela exposerait votre ordinateur et vos données à des risques. Le cas échéant, vous pouvez [suspendre la protection de l'ordinateur](#) pendant l'intervalle que vous souhaitez, sans quitter l'application.

Vous pouvez contrôler l'état de fonctionnement de l'application à l'aide du widget **État de la protection**.

[Lancement ou arrêt de Kaspersky Endpoint Security dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sélectionnez l'ordinateur sur lequel vous souhaitez lancer ou arrêter l'application.
5. Cliquez-droit pour ouvrir le menu contextuel de l'ordinateur client, puis choisissez l'option **Propriétés**.
6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.
Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky installées sur le poste client.
7. Choisissez l'application Kaspersky Endpoint Security.
8. Procédez comme suit :
 - Si vous souhaitez lancer l'application, cliquez sur le bouton  à droite de la liste des applications Kaspersky.
 - Si vous souhaitez arrêter l'application, cliquez sur le bouton  à droite de la liste des applications Kaspersky.

[Lancement ou arrêt de Kaspersky Endpoint Security dans Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez lancer ou arrêter Kaspersky Endpoint Security.
La fenêtre des propriétés de l'ordinateur s'ouvre.
3. Choisissez l'onglet **Applications**.
4. Cochez la case en regard de l'application **Kaspersky Endpoint Security for Windows**.
5. Cliquez sur le bouton **Démarrer** ou **Arrêter**.

[Lancement ou arrêt de Kaspersky Endpoint Security via la ligne de commande](#)

Pour quitter l'application via la ligne de commande, il faut [activer la gestion externe des services système](#).



Pour démarrer ou quitter l'application via la ligne de commande, il faut le fichier klpsm.exe qui figure dans le kit de distribution de Kaspersky Endpoint Security.

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.
3. Pour lancer l'application via la ligne de commande, saisissez `klpsm.exe start_avp_service`.
4. Pour arrêter l'application via la ligne de commande, saisissez `klpsm.exe stop_avp_service`.

Suspension et rétablissement de la protection et du contrôle de l'ordinateur

Par suspension de la protection de l'ordinateur et du contrôle, il faut entendre la désactivation pendant un certain temps de tous les modules de la protection et de tous les modules de contrôle de Kaspersky Endpoint Security.

L'état de l'application est illustré par l'[icône de l'application dans la zone de notifications de la barre de tâches](#) :

- L'icône  signale la suspension de la protection et du contrôle de l'ordinateur.
- L'icône  indique que la protection et le contrôle de l'ordinateur sont activés.

La suspension et le rétablissement de la protection de l'ordinateur et du contrôle n'ont aucune influence sur l'exécution des tâches d'analyse et de mise à jour de l'application.

Si des connexions réseau étaient ouvertes au moment de la suspension et du rétablissement du contrôle de l'ordinateur, un message s'affiche pour indiquer l'interruption de ces connexions.

Pour rétablir la protection et le contrôle de l'ordinateur, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Sélectionnez **Suspendre la protection** dans le menu contextuel (cf. ill. ci-après).
Cet élément du menu contextuel est disponible si la [protection par mot de passe est activée](#).
3. Choisissez l'une des options suivantes :
 - **Suspendre pour <période>** : la protection de l'ordinateur et le contrôle seront activés à l'issue de l'intervalle de temps défini dans la liste déroulante en dessous.
 - **Suspendre jusqu'au redémarrage du programme** : la protection de l'ordinateur et le contrôle sont rétablis après le redémarrage de l'application ou du système d'exploitation. Pour pouvoir utiliser cette fonctionnalité, le lancement automatique de l'application doit être activé.
 - **Pause** : la protection et le contrôle de l'ordinateur sont activés quand vous décidez de les rétablir.

4. Cliquez sur le bouton **Suspendre la protection**.

Kaspersky Endpoint Security suspend tous les modules de la protection et de contrôle qui ne sont pas accompagnés d'un cadenas dans la stratégie (🔒). Avant de réaliser cette opération, il est conseillé de désactiver la stratégie de Kaspersky Security Center.



Menu contextuel de l'icône de l'application

Pour rétablir la protection de l'ordinateur et le contrôle, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Sélectionnez **Rétablir la protection** dans le menu contextuel.

Vous pouvez rétablir la protection et le contrôle de l'ordinateur à n'importe quel moment, quelle que soit l'option de suspension de la protection et du contrôle de l'ordinateur vous aviez choisi auparavant.

Analyse de l'ordinateur

La recherche de virus est un élément important dans la protection de l'ordinateur. Elle doit être réalisée régulièrement pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de la protection en raison, par exemple, d'un niveau de sécurité faible ou pour toute autre raison.

Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive et crée des entrées de journal indiquant que ces fichiers n'ont pas été analysés.

Analyse complète

Analyse minutieuse de tout le système. Kaspersky Internet Endpoint analyse les objets suivants :

- Mémoire du noyau
- Objets chargés au lancement du système d'exploitation
- Secteurs d'amorçage
- Sauvegarde du système d'exploitation
- Tous les disques durs et amovibles

Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse de la tâche *Analyse complète*.

Pour économiser les ressources de l'ordinateur, il est conseillé de lancer la tâche d'analyse en arrière-plan au lieu de la tâche d'analyse complète. Le niveau de sécurité de l'ordinateur ne change pas.

Analyse des zones critiques

Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse de la tâche *Analyse des zones critiques*.

Analyse personnalisée

Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :

- Mémoire du noyau
- Objets chargés au lancement du système d'exploitation
- Sauvegarde du système d'exploitation

- Boîte aux lettres Microsoft Outlook
- Disques durs, disques amovibles et disques réseau
- N'importe quel fichier sélectionné

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage, le secteur d'amorçage, la mémoire du système et la partition du système.

Vérification de l'intégrité

Kaspersky Endpoint Security vérifie si les modules de l'application ont été endommagés ou modifiés.

Lancement et arrêt de la tâche d'analyse

Quel que soit le mode d'exécution de la tâche d'analyse sélectionné, vous pouvez lancer ou arrêter la tâche à tout moment.

Pour lancer ou arrêter la tâche d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Cliquez sur le bouton **Lancer l'analyse** si vous voulez lancer la tâche d'analyse.

Kaspersky Endpoint Security commencera à analyser l'ordinateur. L'application indiquera la progression de l'analyse, le nombre de fichiers analysés ainsi que la durée d'analyse restante. Vous pouvez arrêter la tâche à tout moment en cliquant sur le bouton **Arrêt**.


Pour lancer ou arrêter la tâche d'analyse lors de l'affichage de l'interface simplifiée de l'application, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :
 - Choisissez une tâche d'analyse non-lancée pour la lancer.
 - Choisissez une tâche d'analyse lancée pour l'arrêter.
 - Choisissez une tâche d'analyse arrêtée pour la reprendre ou la relancer.

Modification du niveau de sécurité

Kaspersky Endpoint Security peut utiliser différents groupes de paramètres pour lancer une analyse. Les ensembles de paramètres enregistrés dans l'application sont dénommés *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont les paramètres optimaux. Ils sont recommandés par les spécialistes de Kaspersky. Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

Afin de modifier le niveau de sécurité, procédez comme suit :


1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Dans le groupe **Niveau de protection**, exécutez une des actions suivantes :
 - Pour appliquer un des niveaux prédéfinis de sécurité, sélectionnez-le à l'aide du curseur :
 - **Élevé**. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse de fichiers composés, Kaspersky Endpoint Security analyse également les fichiers au format de messagerie.
 - **Recommandé**. Kaspersky Endpoint Security analyse uniquement les fichiers de formats déterminés sur tous les disques durs, les disques amovibles et les disques réseau de l'ordinateur ainsi que les objets OLE intégrés. Kaspersky Endpoint Security n'analyse pas les archives et les fichiers d'installation.
 - **Faible**. Kaspersky Endpoint Security analyse uniquement les nouveaux fichiers et les fichiers modifiés aux extensions définies sur tous les disques durs, amovibles ou réseau de votre ordinateur. Kaspersky Endpoint Security n'analyse pas les fichiers composés.
 - Si vous souhaitez configurer un niveau de sécurité personnalisé, cliquez sur le bouton **Paramètres avancés** et définissez vos propres paramètres du module.

Vous pouvez restaurer les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut** dans la partie supérieure de la fenêtre.
4. Enregistrez vos modifications.

Modification de l'action sur les fichiers infectés

Par défaut, en cas de détection de fichiers infectés, Kaspersky Endpoint Security tente de les désinfecter ou les supprime, si la désinfection est impossible.

Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Dans le groupe **Action en cas de détection d'une menace**, choisissez une des options suivantes :
 - **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.
 - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si

désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.

- **Informer.** Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.


Avant de tenter de désinfecter ou de supprimer un fichier infecté, Kaspersky Endpoint Security crée une copie de sauvegarde du fichier au cas où vous auriez besoin de [restaurer le fichier ou au cas où il pourrait être désinfecté à l'avenir](#).

En cas de détection de fichiers infectés qui appartiennent à une application de Windows Store, Kaspersky Endpoint Security tente de supprimer le fichier.

4. Enregistrez vos modifications.

Composition de la liste des objets à analyser

Pour composer une liste des objets à analyser, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le lien **Modifier la zone d'analyse**.
4. Dans la fenêtre qui s'ouvre, sélectionnez les objets que vous souhaitez ajouter à la zone d'analyse ou exclure de celle-ci.

Vous ne pouvez pas supprimer ou modifier les objets repris par défaut dans la zone d'analyse.

5. Si vous voulez ajouter un nouvel objet à la zone d'analyse, procédez comme suit :

- a. Cliquez sur le bouton **Ajouter**.
L'arborescence des dossiers s'ouvre.
- b. Choisissez l'objet et cliquez sur le bouton **Sélectionner**.

Dans la zone d'analyse, vous pouvez exclure un objet des analyses sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.




6. Enregistrez vos modifications.

Sélection du type de fichiers à analyser

Au moment de choisir le type d'objet à analyser, il convient de tenir compte des éléments suivants :

1. La probabilité d'introduction d'un code malveillant dans des fichiers de certains formats et son activation ultérieure est faible (par exemple, le format TXT). Mais il existe également des formats de fichiers qui contiennent un code exécutable (par exemple, les formats EXE, DLL, DOC). Le code exécutable peut également se retrouver dans des formats de fichiers qui ne sont pas destinés à cela (par exemple, le format DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.
2. Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, l'application ignorera ce fichier lors de l'analyse. Si l'analyse des fichiers selon le format a été sélectionnée, Kaspersky Endpoint Security analyse l'en-tête du fichier, quelle que soit son extension. S'il s'avère que le fichier possède un format de fichier exécutable (par exemple, EXE), l'application l'analyse.

Pour sélectionner les types d'objets à analyser, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Paramètres avancés**.
4. Sélectionnez dans le groupe **Types de fichiers** le type de fichiers que vous souhaitez analyser pendant l'exécution de la tâche d'analyse :
 - **Tous les fichiers**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension).
 - **Fichiers analysés par format**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les [fichiers infectables](#) . Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte.
 - **Fichiers analysés selon l'extension**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les [fichiers infectables](#) . Le format du fichier sera déterminé sur la base de son extension.

Les fichiers sans extension sont considérés par Kaspersky Endpoint Security comme des fichiers exécutables. Kaspersky Endpoint Security analyse toujours les fichiers exécutables, quel que soit le type de fichiers que vous avez sélectionné pour l'analyse.


5. Enregistrez vos modifications.

Optimisation de l'analyse des fichiers

Vous pouvez optimiser l'analyse des fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. Vous pouvez également réduire la période d'analyse d'un fichier. À l'issue du temps défini, Kaspersky Endpoint Security exclut le fichier de l'analyse en cours (sauf les archives et les objets qui incluent plusieurs fichiers).

Vous pouvez aussi [activer les technologies iChecker et iSwift](#). Les technologies iChecker et iSwift permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.


Pour optimiser l'analyse des fichiers, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Optimisation de l'analyse**, configurez les paramètres d'analyse :
 - **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. Analysez uniquement les nouveaux fichiers et les fichiers qui ont été modifiés depuis la dernière fois qu'ils ont été analysés. Cela permettra de réduire la durée de l'analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.
 - **Ignorer les fichiers si l'analyse dure plus de X secondes**. Limitez la durée de numérisation d'un seul objet. À l'issue du temps indiqué, Kaspersky Endpoint Security termine l'analyse du fichier. Cela permettra de réduire la durée de l'analyse.
5. Enregistrez vos modifications.

Analyse des fichiers composés

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulée de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter les types de fichiers composés à analyser pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Paramètres avancés**.
4. Sélectionnez dans le groupe **Analyse des fichiers composés** les fichiers composés à analyser : archives, paquets d'installation, fichiers aux formats Office, fichiers au format de messagerie ou fichiers protégés par un mot de passe.
5. Si [l'analyse des fichiers nouveaux et modifiés uniquement est désactivée](#), configurez les paramètres d'analyse pour chaque type de fichier composé : analysez tous les fichiers de ce type ou uniquement les nouveaux fichiers.
Si l'analyse des fichiers nouveaux et modifiés uniquement est activée, Kaspersky Endpoint Security n'analyse que les fichiers nouveaux et modifiés de tous les types de fichiers composés.
6. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :
 - Si vous ne souhaitez pas décompresser les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

- Si vous souhaitez décompresser les fichiers composés quelle que soit leur taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.


7. Enregistrez vos modifications.

Utilisation des méthodes d'analyse

Pendant qu'elle fonctionne, l'application Kaspersky Endpoint Security utilise la méthode d'analyse Machine learning et l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Endpoint Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.


Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.

Pour utiliser les méthodes d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Paramètres avancés**.
4. Si vous souhaitez que l'application utilise l'analyse heuristique lors de l'exécution de la tâche d'analyse, cochez la case **Analyse heuristique** dans le groupe **Méthodes d'analyse**. Ensuite, définissez le niveau de l'analyse heuristique à l'aide du curseur : **niveau superficiel**, **niveau intermédiaire** ou **niveau minutieux**.
5. Enregistrez vos modifications.

Utilisation des technologies d'analyse

Pour utiliser des technologies d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Technologies d'analyse**, cochez les cases à côté des noms des technologies que vous souhaitez utiliser pendant une analyse :
 - **Technologie iSwift**. La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases

de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.

- **Technologie iChecker.** La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).


5. Enregistrez vos modifications.

Sélection du mode de lancement de la tâche d'analyse

Si l'exécution de la tâche d'analyse est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche d'analyse ignorée dès que cela est possible.

Vous pouvez reporter le démarrage de la tâche d'analyse après le démarrage de l'application si l'heure de début de la tâche d'analyse correspond à l'heure de démarrage de Kaspersky Endpoint Security. La tâche d'analyse ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

Pour sélectionner le mode d'exécution de la tâche d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur le bouton **Planification de l'analyse**.
4. Dans la fenêtre qui s'ouvre, configurez la planification de l'exécution des tâches d'analyse.
5. En fonction de la fréquence sélectionnée, configurez les paramètres complémentaires afin d'affiner la planification du lancement de la tâche.
 - a. Sélectionnez l'option **Lancer l'analyse programmée le jour suivant si l'ordinateur est éteint** si vous voulez que Kaspersky Endpoint Security exécute les tâches d'analyse manquées à la première occasion.

Si l'élément **Chaque minute, Chaque heure, Après le lancement de l'application** ou **Après chaque mise à jour** est sélectionné dans la liste déroulante **Lancer l'analyse**, la case **Exécuter l'analyse programmée le jour suivant si l'ordinateur est éteint** n'est pas disponible.

- b. Cochez la case **Exécuter lorsque l'ordinateur celui-ci est inactif** si vous voulez que Kaspersky Endpoint Security suspende la tâche quand les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security lance la tâche d'analyse si l'ordinateur est verrouillé ou si l'écran de veille est activé.


Cette option de planification permet d'économiser la puissance de calcul de l'ordinateur pendant l'utilisation de celui-ci.

6. Enregistrez vos modifications.

Configuration du lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur

Par défaut, la tâche d'analyse est lancée avec les privilèges du compte utilisateur employé pour ouvrir la session dans le système d'exploitation. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche d'analyse sous les privilèges d'un autre utilisateur. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de la tâche d'analyse et lancer la tâche d'analyse au nom de cet utilisateur.


Pour configurer le lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Cliquez sur **Paramètres avancés** → **L'analyse en tant que**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'utilisateur qui requiert les droits pour lancer la tâche d'analyse.
5. Enregistrez vos modifications.

Analyse des disques amovibles lors de leur connexion à l'ordinateur

Kaspersky Endpoint Security analyse tous les fichiers que vous exécutez ou copiez, même si le fichier se trouve sur un lecteur amovible (module Protection contre les fichiers malicieux). Pour empêcher la propagation de virus et autres logiciels malveillants, vous pouvez configurer des analyses automatiques des lecteurs amovibles lorsqu'ils sont connectés à l'ordinateur. Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. Le module assure la sécurité d'un ordinateur en exécutant des analyses qui implémentent l'apprentissage automatique, l'analyse heuristique (haut niveau) et l'analyse des signatures. Kaspersky Endpoint Security utilise également les technologies d'optimisation des analyses iSwift et iChecker. Les technologies sont toujours actives et ne peuvent pas être désactivées.

Pour configurer l'analyse des disques amovibles lors de leur connexion à l'ordinateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse du disque amovible et cliquez sur le bouton .
3. Utilisez le commutateur **Analyse des disques amovibles** pour activer ou désactiver l'analyse des disques amovibles lors de leur connexion à l'ordinateur.
4. Sélectionnez le mode d'analyse des disques amovibles lors de leur connexion :
 - **Analyse approfondie** Si cette option est sélectionnée, lorsqu'un lecteur amovible est connecté, Kaspersky Endpoint Security analyse tous les fichiers situés sur le lecteur amovible, y compris les fichiers incorporés dans des objets composés, des archives, des archives de distribution et des fichiers au format bureautique. Kaspersky Endpoint Security n'analyse pas les fichiers dans les formats de messagerie ou les archives protégées par mot de passe.
 - **Analyse rapide** Si vous choisissez cette option, Kaspersky Endpoint Security analyse uniquement les [fichiers de certains formats](#) les plus exposés à l'infection et il ne décompacte pas les objets composés dès

que le disque amovible a été connecté.

5. Si vous souhaitez que Kaspersky Endpoint Security analyse uniquement les disques amovibles dont la taille ne dépasse pas la valeur indiquée, cochez la case **Taille maximale du disque amovible**, puis définissez la valeur en mégaoctets dans le champ à côté.
6. Configurez la façon dont la progression de l'analyse d'un disque amovible sera affichée. Exécutez une des actions suivantes :
 - Si vous souhaitez que l'application Kaspersky Endpoint Security affiche l'état d'avancement de l'analyse des disques amovibles dans une nouvelle fenêtre, cochez la case **Afficher la progression de l'analyse**.
La fenêtre d'analyse du disque amovible permet d'arrêter l'analyse. Pour rendre l'analyse des lecteurs amovibles obligatoire et empêcher l'utilisateur d'arrêter celle-ci, cochez la case **Interdire l'arrêt de la tâche d'analyse**.
 - Si vous souhaitez que l'application Kaspersky Endpoint Security lance l'analyse des disques amovibles en arrière-plan, décochez la case **Afficher la progression de l'analyse**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage, le secteur d'amorçage, la mémoire du système et la partition du système. L'Analyse en arrière-plan est lancée dans les cas suivants :

- après la mise à jour des bases antivirus ;
- trente minutes après le lancement de Kaspersky Endpoint Security ;
- toutes les six heures ;
- lorsque l'ordinateur est inactif pendant cinq minutes ou plus (l'ordinateur est verrouillé ou l'écran de veille est allumé).

L'analyse en arrière-plan réalisée quand l'ordinateur est en veille est interrompue lorsque l'une des conditions suivantes est remplie :


- L'ordinateur est réactivé.

Si l'analyse en arrière-plan n'a pas été réalisée depuis plus de dix jours, l'analyse n'est pas interrompue.

- L'ordinateur (ordinateur portable) est passé en mode batterie.

Lors de l'analyse en arrière-plan, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.

Pour désactiver l'analyse en arrière-plan de l'ordinateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton .
3. Utilisez le commutateur **Analyse en arrière-plan** pour activer ou désactiver les analyses en arrière-plan.
4. Enregistrez vos modifications.

Vérification de l'intégrité de l'application

Kaspersky Endpoint Security vérifie si les fichiers de l'application, situés dans le dossier d'installation de l'application, ont été endommagés ou modifiés. Par exemple, si la bibliothèque de l'application possède une signature numérique incorrecte, cette bibliothèque est considérée comme endommagée. La tâche *Vérification de l'intégrité* sert à l'analyse des fichiers de l'application. Exécutez la tâche *Vérification de l'intégrité* si Kaspersky Endpoint Security a détecté un objet malveillant et ne l'a pas neutralisé.

Vous pouvez créer la tâche *Vérification de l'intégrité* dans Kaspersky Security Center 12 Web Console et dans la Console d'administration. Il est impossible de créer une tâche dans Kaspersky Security Center Cloud Console.

[Lancement de la vérification de l'intégrité d'une application via la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Choisissez **Kaspersky Endpoint Security for Windows (11.6.0)** → **Vérification de l'intégrité**.

Étape 2. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 3. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou suite à la détection d'une attaque de virus.

Étape 4. Définition du nom de la tâche

Saisissez le nom de la tâche, par exemple, **Vérification de l'intégrité de l'application après l'infection de l'ordinateur**.

Étape 5. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. Kaspersky Endpoint Security vérifie alors l'intégrité de l'application. Vous pouvez également planifier l'exécution de la vérification de l'intégrité de l'application dans les propriétés de la tâche.

[Lancement de la vérification de l'intégrité de l'application via Web Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

b. Dans la liste déroulante **Type de tâche**, choisissez **Vérification de l'intégrité**.

c. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple **Vérification de l'intégrité de l'application après l'infection de l'ordinateur**.

d. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

La nouvelle tâche apparaît dans la liste des tâches.

6. Cochez la case en regard de la tâche.

Kaspersky Endpoint Security vérifie alors l'intégrité de l'application. Vous pouvez également planifier l'exécution de la vérification de l'intégrité de l'application dans les propriétés de la tâche.

L'intégrité de l'application peut être compromise par exemple dans les cas suivants :

- Un objet malveillant a modifié les fichiers de Kaspersky Endpoint Security. Dans ce cas, lancez la procédure de récupération pour Kaspersky Endpoint Security à l'aide des outils du système d'exploitation. Après la récupération, exécutez une analyse complète de l'ordinateur et répétez la vérification de l'intégrité.
- La signature numérique a expiré. Dans ce cas, mettez à jour Kaspersky Endpoint Security.

Mise à jour des bases de données et des modules de l'application

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

Pour une mise à jour régulière, il faut une licence valide de l'application. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Les serveurs de mise à jour de Kaspersky sont la principale source de mise à jour pour Kaspersky Endpoint Security.

Pour réussir le téléchargement du paquet de mise à jour depuis les serveurs de mise à jour de Kaspersky, l'ordinateur doit être connecté à l'Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, vous devez configurer les paramètres du serveur proxy.

Le téléchargement des mises à jour s'opère selon le protocole HTTPS. Le téléchargement selon le protocole HTTP est possible quand le téléchargement des mises à jour selon le protocole HTTPS est impossible.

Lors de la mise à jour, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Les bases de Kaspersky Endpoint Security. La protection de l'ordinateur est garantie par l'utilisation de bases de données qui contiennent les signatures des virus et autres programmes présentant une menace ainsi que les informations sur les moyens de lutter contre elles. Ces informations sont utilisées par les modules de la protection pour rechercher sur votre ordinateur les objets dangereux et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des menaces qui apparaissent et les moyens de lutter contre celles-ci. Pour cette raison, il est recommandé d'actualiser régulièrement les bases.

En plus des bases de Kaspersky Endpoint Security, la mise à jour concerne également les pilotes réseau qui assurent l'interception du trafic réseau par les modules de la protection.

- Modules de l'application. Outre les bases de Kaspersky Endpoint Security, il est possible d'actualiser les modules de l'application. Les mises à jour des modules de l'application permettent de supprimer les vulnérabilités de Kaspersky Endpoint Security, ajoutent de nouvelles fonctionnalités ou améliorent les fonctionnalités existantes.

Pendant la mise à jour, les bases et les modules de l'application installés sur votre ordinateur sont comparés à la dernière version stockée à la source des mises à jour. Si les bases et les modules de l'application actuels diffèrent de la dernière version, la partie manquante sera installée sur l'ordinateur.

La mise à jour des modules de l'application peut s'accompagner de la mise à jour de l'aide contextuelle de l'application.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Les informations sur l'état actuel des bases de Kaspersky Endpoint Security s'affichent dans le groupe **Mise à jour** de la fenêtre **Tâches**.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le [rapport de Kaspersky Endpoint Security](#).

Schémas de mise à jour des bases de données et des modules de l'application

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

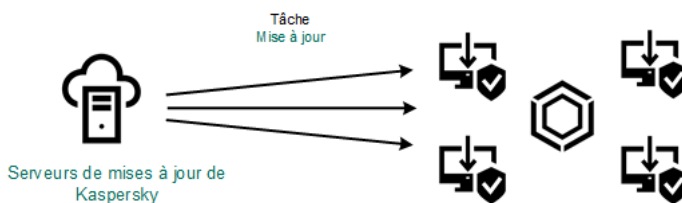
Les éléments suivants sont mis à jour sur les ordinateurs des utilisateurs :

- Bases antivirus. Les bases antivirus contiennent les bases des signatures des programmes malveillants, la description des attaques réseau, les bases des adresses Internet malveillantes et de phishing, les bases des bannières, les bases antisпам et d'autres données.
- Modules de l'application. La mise à jour des modules permet d'éliminer les vulnérabilités de l'application et d'améliorer les méthodes de protection de l'ordinateur. Les mises à jour des modules peuvent modifier le comportement des modules de l'application et ajouter de nouvelles fonctions.

Kaspersky Endpoint Security prend en charge les schémas de mise à jour des bases et des modules de l'application suivants :

- Mise à jour depuis les serveurs de Kaspersky.

Les serveurs de mises à jour de Kaspersky sont répartis à travers le monde. Ceci garantit la haute fiabilité des mises à jour. Si la mise à jour ne peut pas être exécutée depuis un serveur, Kaspersky Endpoint Security passe au serveur suivant.



Mise à jour depuis les serveurs de Kaspersky.

- Mise à jour centralisée.

La mise à jour centralisée permet de réduire le trafic Internet externe et garantit la commodité du contrôle des mises à jour.

La mise à jour centralisée se déroule selon les étapes suivantes :

1. Chargement du paquet de mise à jour dans le stockage au sein du réseau de l'organisation.

Le téléchargement du paquet de mise à jour dans le stockage est réalisé par la tâche du Serveur d'administration *Chargement des mises à jour dans le stockage du Serveur d'administration*.

2. Chargement du paquet de mises à jour dans un dossier partagé (facultatif).

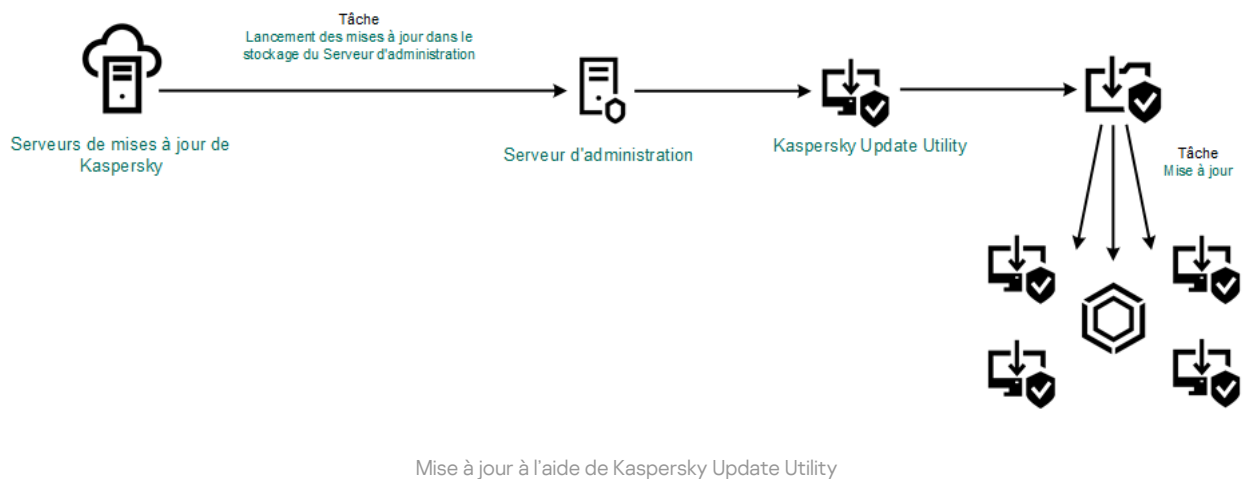
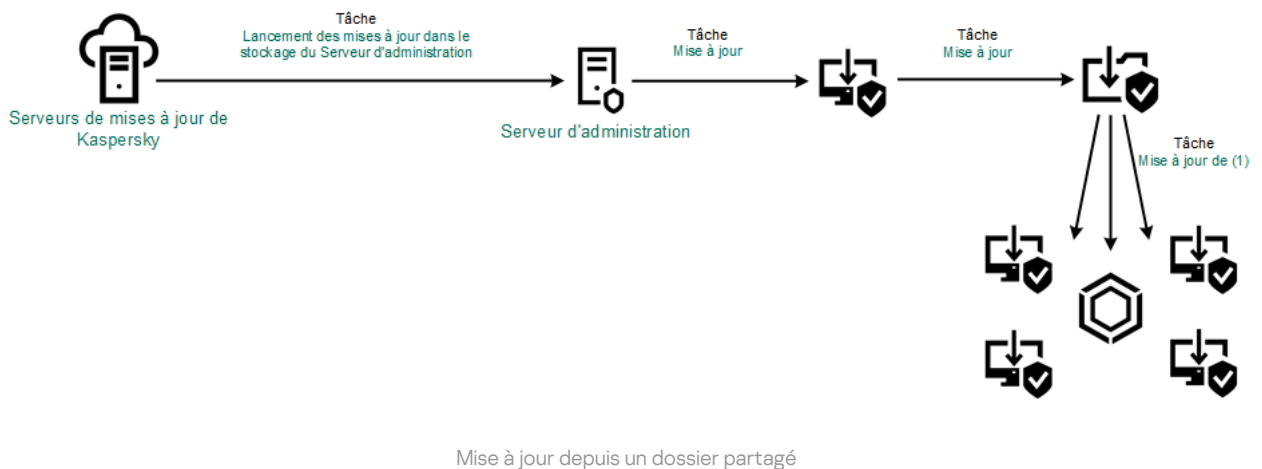
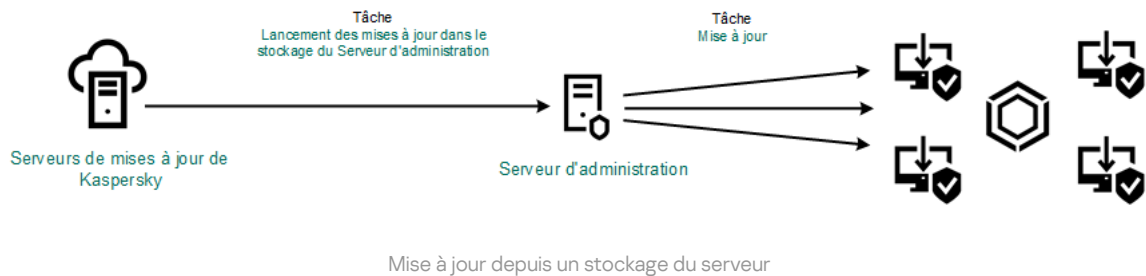
Le chargement du paquet de mise à jour dans le dossier partagé peut s'opérer d'une des manières suivantes :

- À l'aide de la tâche de Kaspersky Endpoint Security *Mise à jour*. La tâche est prévue pour un des ordinateurs du réseau local de l'organisation.

- À l'aide de Kaspersky Update Utility. Les informations détaillées sur l'utilisation de Kaspersky Update Utility sont reprises dans la [Base des connaissances de Kaspersky](#).

3. Diffusion du paquet de mise à jour sur les ordinateurs client.

La diffusion du paquet de mise à jour sur les ordinateurs client est garantie par la tâche *Mise à jour* de Kaspersky Endpoint Security. Vous pouvez créer un nombre illimité de tâches de mise à jour pour chacun des groupes d'administration.



Pour Web Console, la liste des sources des mises à jour contient par défaut le Serveur d'administration de Kaspersky Security Center et les serveurs de mises à jour de Kaspersky. Pour Kaspersky Security Center Cloud Console, la liste des sources de mise à jour contient par défaut des points de distribution et des serveurs de mise à jour de Kaspersky. Pour en savoir plus sur les points de distribution, consultez l'[aide de Kaspersky Security Center Cloud Console](#). Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés. Si la mise à jour ne peut pas être exécutée depuis une source de mise à jour, Kaspersky Endpoint Security passe automatiquement à la suivante

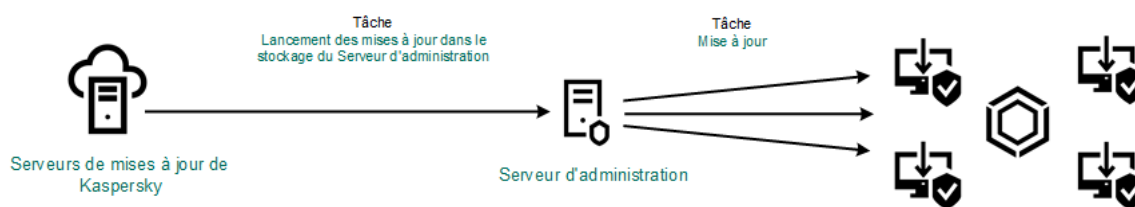
Le chargement des mises à jour depuis les serveurs de mise à jour de Kaspersky ou d'autres serveurs FTP ou HTTP s'opère selon des protocoles réseau standard. Si l'accès à la source des mises à jour requiert une connexion à un serveur proxy, [introduisez les paramètres du serveur proxy dans les propriétés de la stratégie de Kaspersky Endpoint Security](#).

Mise à jour depuis un stockage du serveur

Pour économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local de l'organisation depuis le stockage de serveur. Pour ce faire, Kaspersky Security Center doit charger le paquet de mise à jour dans le stockage (serveur FTP ou HTTP, dossier réseau ou local) des serveurs de mise à jour de Kaspersky. Ainsi, les autres ordinateurs du réseau local de l'organisation pourront recevoir le paquet de mise à jour depuis le stockage de serveur.

La configuration de la mise à jour des bases et des modules de l'application du stockage de serveur comprend les étapes suivantes :

1. Configuration du déplacement du paquet de mise à jour dans le stockage sur le Serveur d'administration (tâche *Chargement des mises à jour dans le stockage du Serveur d'administration*).
2. Configuration de la mise à jour des bases et des modules de l'application depuis le stockage de serveur indiqué sur les autres ordinateurs du réseau local de l'organisation (tâche *Mise à jour*).



Mise à jour depuis un stockage du serveur

Pour configurer le chargement du paquet de mises à jour dans le stockage du serveur, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur la tâche du Serveur d'administration **Chargement des mises à jour dans le stockage du Serveur d'administration**.

La fenêtre des propriétés de la tâche s'ouvre.

La tâche *Chargement des mises à jour dans le stockage du Serveur d'administration* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center 12 Web Console et n'existe qu'en un seul exemplaire.

3. Choisissez l'onglet **Paramètres de l'application**.

4. Dans le groupe **Paramètres divers**, cliquez sur le bouton **Configurer**.

5. Saisissez dans le champ **Dossier d'enregistrement des mises à jour**, saisissez l'adresse du serveur FTP ou HTTP ou du dossier réseau ou local dans lequel Kaspersky Security Center copie le paquet de mise à jour récupéré sur les serveurs de mise à jour de Kaspersky.

Le chemin d'accès à la source des mises à jour est le suivant :

- S'il s'agit d'un serveur FTP ou HTTP, saisissez l'adresse Internet ou l'adresse IP du site.

Par exemple, `http://dn1-01.geo.kaspersky.com/` ou `93.191.13.103`.

S'il s'agit d'un serveur FTP, vous pouvez indiquer les paramètres d'authentification au format `ftp://<nom d'utilisateur>:<mot de passe>@<nœud>:<port>`.

- Pour le dossier réseau, saisissez le chemin UNC.

Par exemple, \\ Server\Share\Update distribution.

- S'il s'agit d'un dossier local, saisissez le chemin d'accès complet à ce dossier.

Par exemple : C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

6. Enregistrez vos modifications.

Pour configurer la mise à jour de Kaspersky Endpoint Security depuis le dossier indiqué, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.

La fenêtre des propriétés de la tâche s'ouvre.

La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center. Pour créer la tâche *Mises à jour* pendant l'exécution de l'assistant, installez le plug-in Internet de Kaspersky Endpoint Security for Windows.

3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.

4. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

5. Dans le champ **Source**, saisissez l'adresse du serveur FTP ou HTTP ou du dossier réseau ou local dans lequel Kaspersky Security Center copie le paquet de mise à jour récupéré sur les serveurs de mise à jour de Kaspersky.

L'adresse de la source doit correspondre à l'adresse indiquée antérieurement dans le champ **Dossier de stockage des mises à jour** lors de la configuration du téléchargement des mises à jour sur le stockage serveur (cf. les *instructions ci-dessus*).

6. Dans le groupe **État**, sélectionnez l'option **Activé(e)**.

7. Cliquez sur le bouton **OK**.

8. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

9. Cliquez sur le bouton **Enregistrer**.

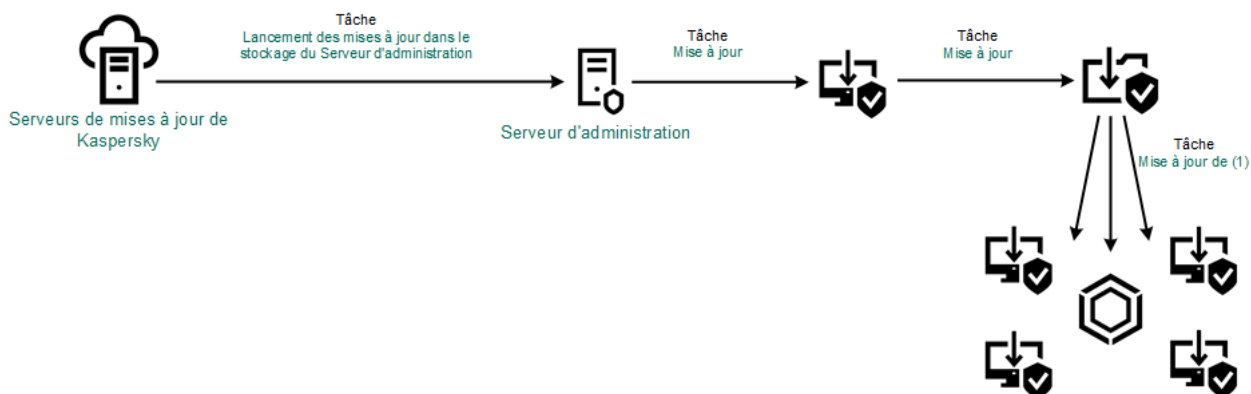
Si la mise à jour ne peut pas être exécutée depuis la première source de mises à jour, Kaspersky Endpoint Security passe automatiquement à la suivante.

Mise à jour depuis un dossier partagé

Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local d'entreprise depuis un dossier partagé. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou les serveurs de mises à jour de Kaspersky et copie le paquet de mise à jour dans le dossier partagé. Ainsi, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

La configuration de la mise à jour des bases et des modules de l'application depuis un dossier partagé comprend les étapes suivantes :

1. [Configuration de la mise à jour des bases et des modules de l'application du stockage de serveur.](#)
2. Activation du mode de copie du paquet des mises à jour vers un dossier partagé sur un des ordinateurs du réseau LAN de l'entreprise (cf. instructions ci-après).
3. Configuration des mises à jour des bases et des modules de l'application à partir du dossier partagé indiqué vers les autres ordinateurs du réseau LAN de l'entreprise (cf. instructions ci-après).



Mise à jour depuis un dossier partagé

Pour activer le mode de copie du paquet des mises à jour vers un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.
La liste des tâches s'ouvre.
2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.
La fenêtre des propriétés de la tâche s'ouvre.
La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center. Pour créer la tâche *Mises à jour* pendant l'exécution de l'assistant, installez le plug-in Internet de Kaspersky Endpoint Security for Windows.
3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.
4. Configurez les sources des mises à jour.
En guise de sources des mises à jour, vous pouvez utiliser les serveurs de mise à jour de Kaspersky, le Serveur d'administration de Kaspersky Security Center ou d'autres serveurs FTP ou HTTP, ainsi que des dossiers locaux ou réseau.
5. Cochez la case **Copier les mises à jour dans le dossier**.
6. Dans le champ **Emplacement**, saisissez le chemin UNC du dossier partagé (par exemple, \\Server\Share\Update distribution).
Si le champ n'est pas rempli, Kaspersky Endpoint Security copie le paquet de mise à jour dans le dossier C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.
7. Cliquez sur le bouton **Enregistrer**.

La tâche *Mise à jour* doit être affectée à un ordinateur qui sera considéré comme la source des mises à jour.

Pour configurer la mise à jour depuis un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

b. Dans la liste déroulante **Type de tâche**, choisissez **Mise à jour**.

c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, **Mise à jour depuis un dossier partagé**.

d. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

La tâche *Mise à jour* doit être attribuée aux ordinateurs restant du réseau local de l'organisation, à l'exception de l'ordinateur considéré comme source de mises à jour.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche, puis cliquez sur **Suivant**.

5. Terminez l'assistant en cliquant sur le bouton **Générer**.

La nouvelle tâche apparaît dans le tableau des tâches.

6. Cliquez sur la tâche *Mise à jour* créée.

La fenêtre des propriétés de la tâche s'ouvre.

7. Passez à la section **Paramètres de l'application**.

8. Sélectionnez l'onglet **Mode local**.

9. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Ajouter**.

10. Indiquez dans le champ **Source** le chemin d'accès au dossier partagé.

L'adresse de la source doit correspondre à l'adresse renseignée au préalable dans le champ **Emplacement** lors de la configuration du mode de copie du paquet de mise à jour dans le dossier partagé (cf. les *instructions ci-dessus*).

11. Cliquez sur le bouton **OK**.

12. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

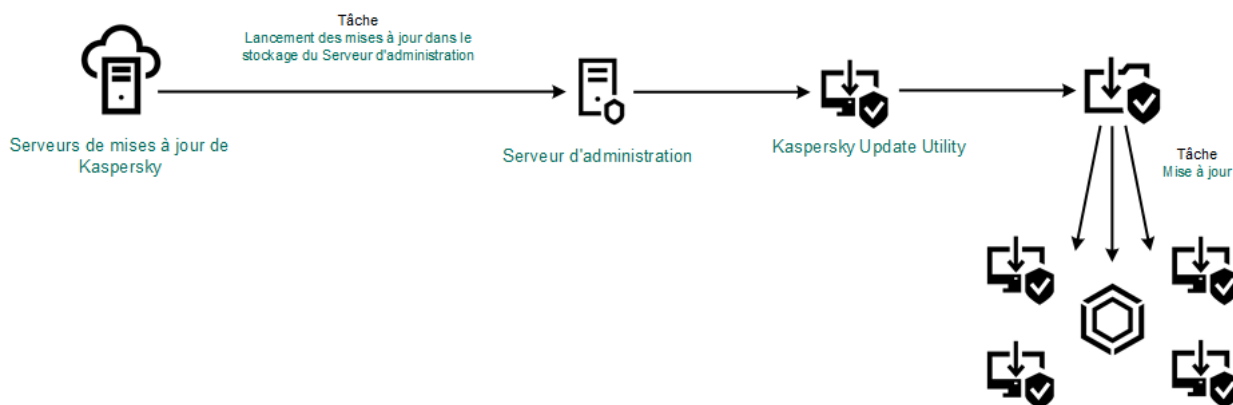
13. Cliquez sur le bouton **Enregistrer**.

Mise à jour à l'aide de Kaspersky Update Utility

Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local d'entreprise depuis un dossier partagé à l'aide de l'utilitaire Kaspersky Update Utility. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou les serveurs de mises à jour de Kaspersky et copie les paquets de mise à jour dans le dossier partagé à l'aide de l'utilitaire. Ainsi, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

La configuration de la mise à jour des bases et des modules de l'application depuis un dossier partagé comprend les étapes suivantes :

1. [Configuration de la mise à jour des bases et des modules de l'application du stockage de serveur.](#)
2. Installation de Kaspersky Update Utility sur un des ordinateurs du réseau local de l'entreprise.
3. Configuration de la copie du paquet de mise à jour dans le dossier partagé des paramètres de Kaspersky Update Utility.
4. Configuration de la mise à jour des bases et des modules de l'application puis le dossier partagé indiqué sur les autres ordinateurs du réseau local d'entreprise.



Mise à jour à l'aide de Kaspersky Update Utility

Vous pouvez télécharger le paquet de distribution de Kaspersky Update Utility depuis le [site Internet du Support Technique de Kaspersky](#). Après avoir installé l'utilitaire, sélectionnez la source de mises à jour (par exemple, le stockage du Serveur d'administration) et le dossier partagé dans lequel Kaspersky Update Utility va copier les paquets de mise à jour. Les informations détaillées sur l'utilisation de Kaspersky Update Utility sont reprises *dans la Base des connaissances de Kaspersky*.

Pour configurer la mise à jour depuis un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.
La liste des tâches s'ouvre.
2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.
La fenêtre des propriétés de la tâche s'ouvre.
La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center. Pour créer la tâche *Mises à jour* pendant l'exécution de l'assistant, installez le plug-in Internet de Kaspersky Endpoint Security for Windows.
3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.
4. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

5. Dans le champ **Source**, saisissez le chemin UNC du dossier partagé (par exemple, \\Server\Share\Update distribution).

L'adresse de la source doit correspondre à l'adresse spécifiée dans les paramètres de Kaspersky Update Utility.

6. Cliquez sur le bouton **OK**.

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

8. Cliquez sur le bouton **Enregistrer**.

Mise à jour en mode mobile

Le *mode mobile* est un mode de fonctionnement de Kaspersky Endpoint Security qui s'applique aux situations où l'ordinateur quitte le périmètre du réseau de l'organisation (*ordinateur déconnecté*). Pour en savoir plus sur les ordinateurs déconnectés et les utilisateurs itinérants, consultez [l'aide de Kaspersky Security Center](#).

L'ordinateur déconnecté qui a quitté le réseau de l'organisation ne peut pas se connecter au Serveur d'administration pour la mise à jour des bases et des modules de l'application. Par défaut, la mise à jour des bases et des modules de l'application en mode mobile s'opère uniquement depuis les Serveurs de mise à jour de Kaspersky désignés comme source des mises à jour. L'utilisation du serveur proxy pour la connexion à Internet est définie par la [stratégie spéciale pour les utilisateurs autonomes](#). La stratégie pour les utilisateurs autonomes est créée séparément. Après le passage de Kaspersky Endpoint Security au mode mobile, les tâches de mise à jour sont lancées une fois toutes les deux heures.

Pour configurer les paramètres de mise à jour en mode mobile, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.

La fenêtre des propriétés de la tâche s'ouvre.

La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center. Pour créer la tâche *Mises à jour* pendant l'exécution de l'assistant, installez le plug-in Internet de Kaspersky Endpoint Security for Windows.

Sélectionnez l'onglet **Paramètres de l'application** → **Mode mobile**.

3. Configurez les sources des mises à jour. En guise de sources des mises à jour, vous pouvez utiliser les serveurs de mise à jour de Kaspersky ou d'autres serveurs FTP ou HTTP, ainsi que des dossiers locaux ou réseau.

4. Cliquez sur le bouton **Enregistrer**.


Ainsi, les bases et les modules de l'application sont mis à jour sur les ordinateurs des utilisateurs lors du passage au mode mobile.

Lancement et arrêt des tâches

Quel que soit le mode d'exécution de la tâche de mise à jour sélectionné, vous pouvez lancer ou arrêter la tâche de mise à jour de Kaspersky Endpoint Security à tout moment.

Pour lancer ou arrêter la tâche de recherche de mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Dans le groupe **Mise à jour des bases et des modules de l'application**, cliquez sur le bouton **Mettre à jour** si vous souhaitez lancer la tâche de mise à jour.

Kaspersky Endpoint Security commencera à mettre à jour les modules de l'application ainsi que les bases de données. L'application affichera la progression de la tâche, la taille des fichiers téléchargés ainsi que la source de la mise à jour. Vous pouvez cliquer sur le bouton  pour arrêter cette tâche à tout moment.

Pour lancer ou arrêter la tâche de mise à jour lors de l'affichage [de l'interface simplifiée de l'application](#), procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :
 - Choisissez une tâche de mise à jour non-lancée pour la lancer.
 - Choisissez une tâche de mise à jour lancée pour l'arrêter.
 - Choisissez une tâche de mise à jour arrêtée pour la reprendre ou la relancer.

Lancement de la tâche de mise à jour avec les privilèges d'un autre utilisateur

Par défaut, la tâche de mise à jour de Kaspersky Endpoint Security est lancée au nom de l'utilisateur que vous avez utilisé pour ouvrir votre session dans le système d'exploitation. Cependant, la mise à jour de Kaspersky Endpoint Security peut se dérouler depuis une source à laquelle l'utilisateur n'a pas accès (par exemple, depuis un dossier partagé contenant le paquet des mises à jour) ou pour laquelle l'utilisation de l'authentification sur le serveur proxy n'a pas été configurée. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de Kaspersky Endpoint Security et lancer la tâche de mise à jour de Kaspersky Endpoint Security au nom de cet utilisateur.

Pour lancer une tâche de mise à jour sous les privilèges d'un autre utilisateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Cliquez sur le bouton **Paramètres du compte**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'option **Lancer les mises à jour des bases avec les privilèges d'utilisateur**.
5. Saisissez les identifiants de compte d'un utilisateur ayant les autorisations nécessaires pour accéder à la source des mises à jour.
6. Enregistrez vos modifications.

Sélection du mode de lancement de la tâche de mise à jour

Si l'exécution de la tâche est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

Vous pouvez reporter le lancement de la tâche de mise à jour par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche de mise à jour **Selon la programmation** et l'heure de lancement de Kaspersky Endpoint Security est le même que l'heure programmée pour le lancement de la tâche de mise à jour. La tâche de mise à jour ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

Pour sélectionner le mode d'exécution de la tâche de mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Cliquez sur le bouton **Définir le mode de mise à jour des bases de données**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le mode d'exécution de la tâche de mise à jour :
 - Sélectionnez l'option **Automatique**, si vous souhaitez que Kaspersky Endpoint Security lance la tâche de mise à jour en fonction de la présence du paquet des mises à jour dans la source de mise à jour. L'intervalle de vérification de la présence du paquet des mises à jour par Kaspersky Endpoint Security est augmenté en cas d'épidémie et réduit en situation normale.
 - Sélectionnez l'option **Manuelle** pour lancer la tâche de mise à jour manuellement.
 - Sélectionnez l'option **<Selon la programmation>** pour programmer l'exécution de la tâche de mise à jour. Configurez les paramètres avancés pour lancer la tâche de mise à jour :
 - Indiquez dans le champ **Reporter le lancement après le démarrage de l'application de** le temps qui doit s'écouler avant l'exécution de la tâche de mise à jour après le lancement de Kaspersky Endpoint Security.
 - Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches de mise à jour non exécutées en temps opportun.
5. Enregistrez vos modifications.

Ajout d'une source des mises à jour

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules de l'application de Kaspersky Endpoint Security.

La source des mises à jour inclut le serveur Kaspersky Security Center, les serveurs de mises à jour de Kaspersky et des dossiers locaux ou réseau.

La liste des sources des mises à jour contient par défaut le serveur Kaspersky Security Center et les serveurs de mises à jour de Kaspersky. Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés.

Kaspersky Endpoint Security ne prend pas en charge les mises à jour des serveurs HTTPS sauf s'il s'agit des serveurs de mise à jour de Kaspersky.

Si plusieurs ressources ont été sélectionnées en tant que sources des mises à jour, Kaspersky Endpoint Security les consultera pendant la mise à jour dans l'ordre de la liste et exécute la tâche de mise à jour en utilisant le paquet de mise à jour de la première source de mise à jour disponible.

Pour ajouter une source des mises à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Cliquez sur le bouton **Sélectionner les sources des mises à jour**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Dans la fenêtre qui s'ouvre, renseignez l'adresse du serveur FTP ou HTTP, le dossier réseau ou local qui contient le package de mise à jour.

Le chemin d'accès à la source des mises à jour est le suivant :

- S'il s'agit d'un serveur FTP ou HTTP, saisissez l'adresse Internet ou l'adresse IP du site.
Par exemple, `http://dn1-01.geo.kaspersky.com/` ou `93.191.13.103`.
S'il s'agit d'un serveur FTP, vous pouvez indiquer les paramètres d'authentification au format `ftp://<nom d'utilisateur>:<mot de passe>@<nœud>:<port>`.
- Pour le dossier réseau, saisissez le chemin UNC.
Par exemple, `\\ Server\Share\Update distribution`.
- S'il s'agit d'un dossier local, saisissez le chemin d'accès complet à ce dossier.
Par exemple : `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Cliquez sur le bouton **Sélectionner**.
7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.
8. Enregistrez vos modifications.

Configuration de la mise à jour depuis un dossier partagé

Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local d'entreprise depuis un dossier partagé. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou les serveurs de mises à jour de Kaspersky et copie le paquet de mise à jour dans le dossier partagé. Ainsi, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

La configuration de la mise à jour des bases et des modules de l'application depuis un dossier partagé comprend les étapes suivantes :

1. Activation du mode de copie du paquet des mises à jour vers un dossier partagé sur un des ordinateurs du réseau local d'entreprise.
2. Configuration de la mise à jour des bases et des modules de l'application puis le dossier partagé indiqué sur les autres ordinateurs du réseau local d'entreprise.

Pour activer le mode de copie du paquet des mises à jour vers un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Dans le groupe **Copie des mises à jour**, cochez la case **Copier les mises à jour dans le dossier**.
4. Saisissez le chemin UNC du dossier partagé (par exemple, \\Server\Share\Update distribution).
5. Enregistrez vos modifications.

Pour configurer la mise à jour depuis un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Cliquez sur le bouton **Sélectionner les sources des mises à jour**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé.

L'adresse de la source doit correspondre à l'adresse renseignée au préalable lors de la configuration du mode de copie du paquet de mise à jour dans le dossier partagé (cf. les *instructions ci-dessus*).

6. Cliquez sur le bouton **Sélectionner**.
7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.
8. Enregistrez vos modifications.

Mise à jour des modules d'application

Les mises à jour du module d'application corrigent les erreurs, améliorent les performances et ajoutent de nouvelles fonctionnalités. Lorsqu'une nouvelle mise à jour du module d'application est disponible, vous devez confirmer l'installation de la mise à jour. Vous pouvez confirmer l'installation d'une mise à jour du module d'application soit dans l'interface de l'application, soit dans Kaspersky Security Center. Lorsqu'une mise à jour est disponible, l'application affiche l'une des notifications suivantes dans la fenêtre principale de Kaspersky Endpoint Security : mise à jour importante (🔔), ou mise à jour critique (🔴). Si la mise à jour des modules de l'application implique la lecture et l'acceptation de dispositions du Contrat de licence utilisateur final, l'application installera ces mises à jour après l'acceptation de ces dispositions. Pour en savoir plus sur le suivi des mises à jour des modules d'application et sur la confirmation d'une mise à jour dans Kaspersky Security Center, *veuillez consulter l'[aide de Kaspersky Security Center](#)*.

Après que vous avez installé une mise à jour de l'application, il peut vous être demandé de redémarrer votre ordinateur.

Pour configurer la mise à jour des modules de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Sélectionnez la tâche *Mise à jour* et cliquez sur le lien **Mode d'exécution : <mode>**.
Les propriétés de la tâche *Mise à jour* s'ouvrent.
3. Dans le groupe **Téléchargement et installation des mises à jour des modules de l'application**, cochez la case **Télécharger les mises à jour des modules de l'application**.
4. Sélectionnez les mises à jour du module d'application que vous souhaitez installer.
 - **Installer les mises à jour critiques et approuvées.** Si cette option est sélectionnée et que des mises à jour des modules de l'application sont disponibles, Kaspersky Endpoint Security installe les mises à jour critiques automatiquement tandis qu'il installera les autres mises à jour uniquement après approbation de leur installation locale via l'interface de l'application ou le Kaspersky Security Center.
 - **Installer uniquement les mises à jour approuvées.** Si cette option est sélectionnée et que des mises à jour des modules sont disponibles, Kaspersky Endpoint Security les installe après approbation de leur application, localement via l'interface de l'application ou depuis le Kaspersky Security Center. Cette option est sélectionnée par défaut.
5. Enregistrez vos modifications.

Utilisation du serveur proxy lors de la mise à jour

Afin de pouvoir télécharger les mises à jour des bases et des modules de l'application depuis une source des mises à jour, il faudra peut-être définir les paramètres du serveur proxy. S'il existe plusieurs sources des mises à jour, les paramètres du serveur proxy sont appliqués à toutes les sources. Si le serveur proxy n'est pas requis pour certaines sources des mises à jour, vous pouvez désactiver l'utilisation du serveur proxy dans les propriétés de la stratégie. Kaspersky Endpoint Security utilisera également le serveur proxy pour accéder au Kaspersky Security Network et aux serveurs d'activation.

Pour configurer la connexion aux sources des mises à jour via un serveur proxy, procédez comme suit :


1. Dans la fenêtre principale de Web Console, cliquez sur .
- La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Passez à la section **Paramètres d'accès au réseau Internet**.
3. Cochez la case **Utiliser un serveur proxy**.
4. Configurez les paramètres de connexion au serveur proxy : l'adresse du serveur proxy, le port et les paramètres d'authentification (le nom d'utilisateur et le mot de passe).
5. Cliquez sur le bouton **Enregistrer**.

Pour désactiver l'utilisation du serveur proxy pour un groupe d'administration défini, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez désactiver l'utilisation du serveur proxy.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Dans la fenêtre **Paramètres du serveur proxy**, sélectionnez l'option **Ne pas utiliser un serveur proxy**.
6. Cliquez sur le bouton **OK**.
7. Confirmez la modification via le bouton **Enregistrer**.

Pour configurer les paramètres du serveur proxy dans l'interface de l'application, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Serveur proxy**, cliquez sur le lien **Paramètres du serveur proxy**.
4. Dans la fenêtre qui s'ouvre, choisissez une des options suivantes pour déterminer l'adresse du serveur proxy :
 - **Définir automatiquement les paramètres du serveur proxy.**
Cette option est sélectionnée par défaut. Kaspersky Endpoint Security utilise les paramètres du serveur proxy qui sont définis dans les paramètres du système d'exploitation.
 - **Utiliser les paramètres indiqués du serveur proxy.**
Si vous avez choisi cette option, configurez les paramètres de connexion au serveur proxy : adresse et port du serveur proxy.
5. Si vous souhaitez activer l'authentification sur le serveur proxy, cochez la case **Utiliser l'authentification sur le serveur proxy** et indiquez les identifiants de votre compte utilisateur.
6. Si vous voulez désactiver l'utilisation du serveur proxy lors de la [mise à jour des bases et des modules de l'application depuis le dossier partagé](#), cochez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
7. Enregistrez vos modifications.

Ainsi, Kaspersky Endpoint Security utilisera le serveur proxy pour télécharger les mises à jour des modules d'application et des bases de données. Kaspersky Endpoint Security utilisera également le serveur proxy pour accéder aux serveurs KSN et aux serveurs d'activation de Kaspersky. Si l'authentification est exigée sur le serveur proxy, mais que les identifiants du compte utilisateur n'ont pas été fournis ou sont incorrects, Kaspersky Endpoint Security vous demandera le nom d'utilisateur ainsi que le mot de passe.


Annulation de la dernière mise à jour

Après la première mise à jour des bases et des modules de l'application, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour des bases et des modules de l'application.

Chaque fois que l'utilisateur lance la mise à jour, Kaspersky Endpoint Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Ceci permet de revenir, le cas échéant, à l'utilisation des bases et des modules de l'application antérieurs. La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sans danger.

Pour restaurer la dernière mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour des bases**.
2. Dans le groupe **Restauration des bases de données à leur version précédente**, cliquez sur le bouton **Exécuter la restauration**.

Kaspersky Endpoint Security commencera à annuler la dernière mise à jour de la base de données. L'application affichera la progression de l'annulation, la taille des fichiers téléchargés ainsi que la source de la mise à jour. Vous pouvez cliquer sur le bouton  pour arrêter cette tâche à tout moment.

Pour lancer ou arrêter la tâche d'annulation de la mise à jour en cas d'affichage [de l'interface simplifiée de l'application](#), procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :
 - choisissez une tâche d'annulation de la mise à jour non-lancée pour la lancer.
 - choisissez une tâche d'annulation de la mise à jour lancée pour l'arrêter.
 - choisissez une tâche d'annulation de la mise à jour arrêtée pour la reprendre ou la relancer.

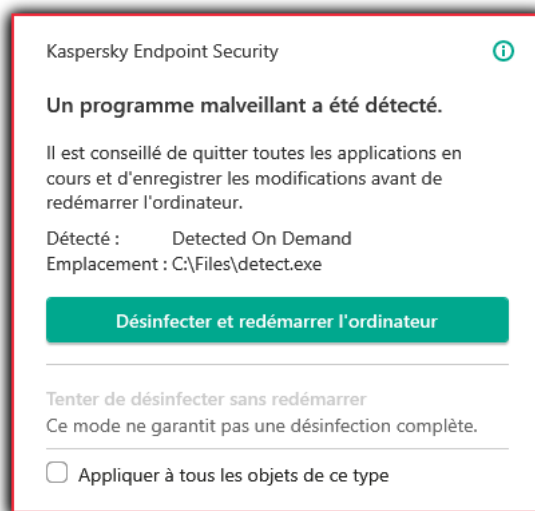
Manipulation des menaces actives

L'application Kaspersky Endpoint Security consigne les informations relatives aux fichiers qu'elle n'a pas traités pour une raison quelconque. Ces informations se présentent sous la forme d'événements dans la liste des menaces actives. Pour faire face aux menaces actives, Kaspersky Endpoint Security utilise la technologie de désinfection active. La désinfection active fonctionne différemment pour les postes de travail et les serveurs. Vous pouvez configurer la technologie de désinfection active dans les [paramètres de la tâche Recherche de virus](#) et dans les [paramètres de l'application](#).

Désinfection des menaces actives sur les postes de travail

Pour traiter les menaces actives sur les postes de travail, [activez la technologie de désinfection active](#) dans les paramètres de l'application. Ensuite, configurez l'expérience utilisateur dans les propriétés de la tâche [Recherche de virus](#). Une case **Activer la désinfection active immédiate** est présente dans les propriétés de la tâche. Si l'indicateur est activé, Kaspersky Endpoint Security effectuera la désinfection sans en informer l'utilisateur. Lorsque la désinfection est terminée, l'ordinateur redémarre. Si l'indicateur est désactivé, Kaspersky Endpoint Security affiche une notification concernant les menaces actives (cf. ill. ci-dessous). Vous ne pouvez pas fermer cette notification sans traiter le fichier.

La désinfection active au cours de l'exécution de la tâche de recherche de virus sur l'ordinateur a lieu uniquement si la [fonction de désinfection active a été activée](#) dans les propriétés de la stratégie appliquée à cet ordinateur.



Notification concernant une menace active

Désinfection des menaces actives sur les serveurs

Pour traiter les menaces actives sur les serveurs, vous devez procéder comme suit :

- [activer la technologie de désinfection active](#) dans les paramètres de l'application ;
- [activer la désinfection active immédiate](#) dans les propriétés de la tâche *Recherche de virus*.

Si Kaspersky Endpoint Security est installé sur un ordinateur fonctionnant sous Windows for Servers, Kaspersky Endpoint Security n'affiche pas la notification. Par conséquent, l'utilisateur ne peut pas sélectionner une action pour désinfecter une menace active. Pour désinfecter une menace, vous devez [activer la technologie de désinfection active](#) dans les paramètres de l'application et [activer la désinfection active immédiate](#) dans les propriétés de la tâche *Recherche de virus*. Ensuite, vous devez démarrer la tâche *Recherche de virus*.

Traitement des menaces actives

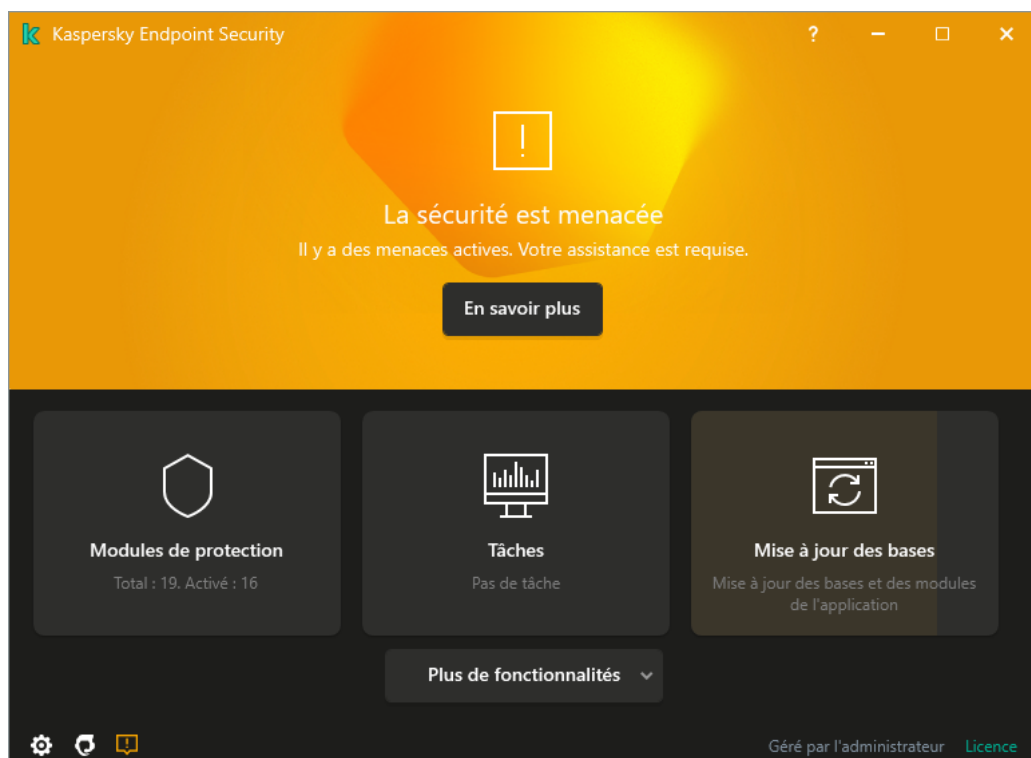
Un fichier infecté est considéré comme *traité* si Kaspersky Endpoint Security, lors de la recherche de la présence éventuelle de virus et autres programmes dangereux, a réalisé une des opérations suivantes sur ce fichier conformément aux paramètres définis de l'application :

- Réparer.
- Supprimer.
- Supprimer si la désinfection est impossible.

Kaspersky Endpoint Security place le fichier dans la liste des menaces actives si, pour une raison quelconque, il n'a pas terminé l'action sur ce fichier conformément à la configuration de l'application lors de la recherche de virus et programmes dangereux sur l'ordinateur.

Cette situation peut se présenter dans les cas suivants :

- Le fichier à analyser n'est pas accessible (par exemple, il se trouve sur un disque réseau ou sur un support externe sans droit en écriture).
- Dans le groupe **Action en cas de détection d'une menace** des paramètres de l'application pour les tâches, l'action **Notifier** a été sélectionnée et lorsque le message relatif au message infecté s'est affiché, l'utilisateur a choisi l'option **Ignorer**.



Fenêtre principale de l'application lorsqu'une menace est détectée

Pour traiter les menaces actives, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **En savoir plus**.

La liste des menaces actives s'ouvre.

2. Sélectionnez l'objet que vous souhaitez traiter.

3. Choisissez la manière dont vous voulez gérer la menace :

- **Éliminer.** Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.
- **Ignorer.** Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'entrée de la liste des menaces actives. S'il n'y a plus de menaces actives dans la liste, l'état de l'ordinateur passera à *OK*. Si l'objet est de nouveau détecté, Kaspersky Endpoint Security ajoutera une nouvelle entrée à la liste des menaces actives.
- **Accéder au fichier.** Si cette option est sélectionnée, Kaspersky Endpoint Security ouvre le dossier contenant l'objet dans le gestionnaire de fichiers. Vous pouvez ensuite supprimer manuellement l'objet ou le déplacer dans un dossier qui n'est pas dans la zone de protection.
- **Plus d'informations.** Si cette option est sélectionnée, Kaspersky Endpoint Security ouvre le [site Internet de l'Encyclopédie des virus de Kaspersky](#).^[2]

Protection de l'ordinateur

Protection contre les fichiers malicieux

Le module Protection contre les fichiers malicieux permet d'éviter l'infection du système de fichiers de l'ordinateur. Par défaut, le module Protection contre les fichiers malicieux se trouve en permanence dans la mémoire vive de l'ordinateur. Le module analyse les fichiers sur tous les disques de l'ordinateur, ainsi que sur les disques connectés. Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.


Le module analyse les fichiers auxquels l'utilisateur ou l'application accède. Si un fichier malveillant est détecté, Kaspersky Endpoint Security bloque l'opération sur le fichier. L'application désinfecte ou supprime ensuite le fichier malveillant, en fonction des paramètres du module Protection contre les fichiers malicieux.

En cas d'accès à un fichier dont le contenu sur OneDrive, Kaspersky Endpoint Security charge et analyse le contenu de ce fichier.

Activation et désactivation de la Protection contre les fichiers malicieux

Par défaut, le module Protection contre les fichiers malicieux est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les fichiers malicieux. Les ensembles de paramètres enregistrés dans l'application sont dénommés *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky (cf. tableau ci-après). Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

Pour activer ou désactiver le module Protection contre les fichiers malicieux, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Utilisez le commutateur **Protection contre les fichiers malicieux** pour activer ou désactiver le module.
4. Si vous avez activé le module, réalisez l'une des opérations suivantes dans la section **Niveau de protection** :
 - Pour appliquer un des niveaux prédéfinis de sécurité, sélectionnez-le à l'aide du curseur :
 - **Élevé**. Niveau de sécurité des fichiers auquel le module Protection contre les fichiers malicieux assure un contrôle maximal sur tous les fichiers ouverts, enregistrés et exécutés. Le module Protection contre les fichiers malicieux analyse tous les types de fichiers sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur. Il scanne aussi des archives, des paquets d'installation et des objets OLE intégrés.
 - **Recommandé**. Ce niveau de protection du fichier est recommandé par les experts de Kaspersky. Le module Protection contre les fichiers malicieux analyse uniquement les formats de fichiers spécifiés sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur, ainsi que les

objets OLE intégrés. Le module Protection contre les fichiers malicieux n'analyse pas les archives ni les paquets d'installation. Les valeurs des paramètres pour le niveau de sécurité recommandé sont fournies dans le tableau ci-dessous.

- **Faible.** Les paramètres de ce niveau de protection du fichier garantissent une vitesse de numérisation maximale. Le module Protection contre les fichiers malicieux analyse uniquement les fichiers avec les extensions spécifiées sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur. Le module Protection contre les fichiers malicieux n'analyse pas les fichiers composés.
- Si vous souhaitez configurer un niveau de sécurité personnalisé, cliquez sur le bouton **Paramètres avancés** et définissez vos propres paramètres du module.

Vous pouvez restaurer les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut** dans la partie supérieure de la fenêtre.

5. Enregistrez vos modifications.

Paramètres recommandés par les experts de Kaspersky pour le module Protection contre les fichiers malicieux (niveau de sécurité recommandé)

| Paramètre | Valeur | Description |
|---|-------------------------------------|--|
| Types de fichiers | Fichiers analysés par format | Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables . Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte. |
| Analyse heuristique | Analyse superficielle | Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu. Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique. |
| Analyser uniquement les nouveaux fichiers et les fichiers modifiés | Activé | Analyse uniquement les nouveaux fichiers et les fichiers qui ont été modifiés depuis la dernière fois qu'ils ont été analysés. Cela permettra de réduire la durée de l'analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. |
| Technologie iSwift | Activé | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS. |
| Technologie iChecker | Activé | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application |


| | | |
|---|---|---|
| | | (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |
| Analyser les fichiers aux formats Microsoft Office | Activé | Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. |
| Mode d'analyse | Intelligente | Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse un objet sur la base de l'analyse des opérations exécutées sur l'objet. Par exemple, dans le cas d'un document Microsoft Office, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse. |
| Action en cas de détection d'une menace | Désinfecter, supprimer si impossible | Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. |

Suspension automatique de la Protection contre les fichiers malicieux

Vous pouvez configurer la suspension automatique de la Protection contre les fichiers malicieux à l'heure indiquée ou en cas d'utilisation d'applications spécifiques.

La suspension de la Protection contre les fichiers malicieux en cas de conflit avec certaines applications est une mesure extrême. Si des conflits surviennent pendant le fonctionnement d'un module, il est conseillé de contacter le [Support Technique de Kaspersky](#). Les experts vous aideront à garantir le fonctionnement de la Protection contre les fichiers malicieux avec d'autres applications sur votre ordinateur.


Pour configurer l'arrêt automatique du module Protection contre les fichiers malicieux, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Suspendre la Protection contre les fichiers malicieux**, cliquez sur le lien **Suspendre la Protection contre les fichiers malicieux**.
5. Dans la fenêtre qui s'ouvre, configurez les paramètres d'interruption de la Protection contre les fichiers malicieux :
 - a. Configurez une planification pour interrompre automatiquement la Protection contre les fichiers malicieux .
 - b. Créez une liste d'applications dont le fonctionnement devrait entraîner l'arrêt de la Protection contre les fichiers malicieux.
6. Enregistrez vos modifications.

Modification de l'action du module Protection contre les fichiers malicieux sur les objets infectés

Par défaut, le module Protection contre les fichiers malicieux tente de désinfecter tous les fichiers infectés détectés. Si la désinfection est impossible, le module Protection contre les fichiers malicieux supprime ces fichiers.

Pour modifier l'action que le module Protection contre les fichiers malicieux va exécuter sur les fichiers infectés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :
 - **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.
 - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.
 - **Interdire**. Si cette option est sélectionnée, le module Protection contre les fichiers malicieux bloque automatiquement les fichiers infectés sans tenter de les désinfecter.

Avant de tenter de désinfecter ou de supprimer un fichier infecté, Kaspersky Endpoint Security crée une copie de sauvegarde du fichier au cas où vous auriez besoin de [restaurer le fichier ou au cas où il pourrait être désinfecté à l'avenir](#).

4. Enregistrez vos modifications.

Composition de la zone de protection du module Protection contre les fichiers malicieux

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection du module Protection contre les fichiers malicieux reprennent l'emplacement et le type de fichiers analysés. Par défaut, le module Protection contre les fichiers malicieux analyse uniquement [les fichiers infectables](#) et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques réseau de l'ordinateur.




Au moment de choisir le type d'objet à analyser, il convient de tenir compte des éléments suivants :

1. La probabilité d'introduction d'un code malveillant dans des fichiers de certains formats et son activation ultérieure est faible (par exemple, le format TXT). Mais il existe également des formats de fichiers qui contiennent un code exécutable (par exemple, les formats EXE, DLL, DOC). Le code exécutable peut également

se retrouver dans des formats de fichiers qui ne sont pas destinés à cela (par exemple, le format DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.

2. Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, l'application ignorera ce fichier lors de l'analyse. Si l'analyse des fichiers selon le format a été sélectionnée, Kaspersky Endpoint Security analyse l'en-tête du fichier, quelle que soit son extension. S'il s'avère que le fichier possède un format de fichier exécutable (par exemple, EXE), l'application l'analyse.

Pour former la zone de protection, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Types de fichiers**, sélectionnez le type de fichiers que vous souhaitez analyser avec le module Protection contre les fichiers malicieux :
 - **Tous les fichiers**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension).
 - **Fichiers analysés par format**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les [fichiers infectables](#) . Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte.
 - **Fichiers analysés par extension**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les [fichiers infectables](#) . Le format du fichier sera déterminé sur la base de son extension.
5. Cliquez sur le lien **Modifier la zone de protection**.
6. Dans la fenêtre qui s'ouvre, sélectionnez les objets que vous souhaitez ajouter à la zone de protection ou exclure de celle-ci.

Vous ne pouvez pas supprimer ni modifier les objets repris par défaut dans la zone de protection.

7. Si vous voulez ajouter un nouvel objet à la zone de protection, procédez comme suit :
 - a. Cliquez sur le bouton **Ajouter**.
L'arborescence des dossiers s'ouvre.
 - b. Choisissez l'objet et cliquez sur le bouton **Sélectionner**.

Dans la zone d'analyse, vous pouvez exclure un objet des analyses sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.


8. Enregistrez vos modifications.

Utilisation des méthodes d'analyse

Pendant qu'elle fonctionne, l'application Kaspersky Endpoint Security utilise la méthode d'analyse Machine learning et l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Endpoint Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.


Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.

Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les fichiers malicieux, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Si vous souhaitez que l'application utilise l'analyse heuristique pour protéger l'appareil contre les fichiers malicieux, cochez la case **Analyse heuristique** dans le groupe **Méthodes d'analyse**. Ensuite, définissez le niveau de l'analyse heuristique à l'aide du curseur : **niveau superficiel**, **niveau intermédiaire** ou **niveau minutieux**.
5. Enregistrez vos modifications.

Utilisation des technologies d'analyse dans le cadre du fonctionnement du module Protection contre les fichiers malicieux

Pour configurer l'utilisation des technologies d'analyse dans le fonctionnement du module Protection contre les fichiers malicieux, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Technologies d'analyse**, cochez les cases à côté des noms des technologies que vous souhaitez utiliser dans le cadre de la protection contre les fichiers malicieux :
 - **Technologie iSwift**. La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.

- **Technologie iChecker.** La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).


5. Enregistrez vos modifications.

Optimisation de l'analyse des fichiers

Vous pouvez optimiser l'analyse des fichiers avec le module Protection contre les fichiers malicieux : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Vous pouvez également [activer les technologies iChecker et iSwift](#) qui permettent d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

Pour optimiser l'analyse des fichiers, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.
5. Enregistrez vos modifications.

Analyse des fichiers composés

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulée de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter les types de fichiers composés à analyser pour accélérer l'analyse.

Le mode de traitement du fichier composé infecté (désinfection ou suppression) dépend du type de fichier.

Le module Protection contre les fichiers malicieux désinfecte les fichiers composés des formats RAR, ARJ, ZIP, CAB, LHA et supprime les fichiers de tous les autres formats (à l'exception des bases de messagerie).

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur le bouton **Paramètres avancés**.

4. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets d'installation ou fichiers au format Office.

5. Si l'[analyse des fichiers nouveaux et modifiés uniquement est désactivée](#), configurez les paramètres d'analyse pour chaque type de fichier composé : analysez tous les fichiers de ce type ou uniquement les nouveaux fichiers.

Si l'analyse des fichiers nouveaux et modifiés uniquement est activée, Kaspersky Endpoint Security n'analyse que les fichiers nouveaux et modifiés de tous les types de fichiers composés.

6. Configurez les paramètres avancés d'analyse des fichiers composés.

- **Ne pas décompresser les fichiers composés de grande taille.**

Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie.

Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille.

Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

- **Décompresser les fichiers composés en arrière-plan.**

Si la case est cochée, Kaspersky Endpoint Security permet d'accéder aux fichiers composés dont la taille est supérieure à la valeur spécifiée avant que ces fichiers ne soient analysés. Dans ce cas, Kaspersky Endpoint Security décompresse et analyse en arrière-plan les fichiers composés.

Kaspersky Endpoint Security permet d'accéder aux fichiers composés qui sont plus petits que cette valeur uniquement après le déballage et l'analyse de ces fichiers.

Si cette case n'est pas cochée, Kaspersky Endpoint Security permet d'accéder aux fichiers composés uniquement après la décompression et l'analyse des fichiers de n'importe quelle taille.

7. Enregistrez vos modifications.

Modification du mode d'analyse des fichiers

Le *mode d'analyse* désigne la condition qui doit être remplie pour que le module Protection contre les fichiers malicieux commencer à analyser les fichiers. Par défaut, Kaspersky Endpoint Security utilise le mode intelligent d'analyse des fichiers. Dans ce mode d'analyse des fichiers, le module Protection contre les fichiers malicieux prend une décision sur la base de l'analyse des opérations exécutées par l'utilisateur, par l'application au nom de l'utilisateur (sous les données duquel la connexion au système d'exploitation a eu lieu, ou sous les données d'un autre utilisateur) ou par le système d'exploitation sur les fichiers. Par exemple, dans le cas d'un fichier Microsoft Office Word, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.

Afin de modifier le mode d'analyse des fichiers, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur le bouton **Paramètres avancés**.

4. Dans le groupe **Mode d'analyse**, sélectionnez le mode requis :

- **Intelligente**. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse un objet sur la base de l'analyse des opérations exécutées sur l'objet. Par exemple, dans le cas d'un document Microsoft Office, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.
- **À l'ouverture et en cas de modification**. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets chaque fois qu'il y a une tentative de les ouvrir ou de les modifier.
- **À l'accès**. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets uniquement lors des tentatives d'ouverture.
- **À l'exécution**. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets uniquement lors des tentatives d'exécution.

5. Enregistrez vos modifications.

Protection contre les menaces Internet

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants via Internet. Il bloque également l'accès aux sites Internet malveillants et de phishing. Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.

Kaspersky Endpoint Security analyse le trafic HTTP, HTTPS et FTP. Kaspersky Endpoint Security analyse les adresses Internet et IP. Vous pouvez [définir les ports que Kaspersky Endpoint Security va surveiller](#) ou sélectionner tous les ports.

Pour contrôler le trafic HTTPS, vous devez [activer l'analyse des connexions sécurisées](#).

Lorsqu'un utilisateur tente d'ouvrir un site Internet malveillant ou de phishing, Kaspersky Endpoint Security bloque l'accès et affiche un avertissement (cf. figure ci-dessous).



Accès interdit

L'URL demandée ne peut pas être affichée.

http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe

Raison :

objet infecté : [UDS:DangerousObject.Multi.Generic](#)

Date de création du message : 10/5/2020 3:52:54 PM


kaspersky

Message sur l'interdiction de l'accès à la page Internet

Activation et désactivation de la Protection contre les menaces Internet

Par défaut, le module Protection contre les menaces Internet est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les menaces Internet. Les ensembles de paramètres enregistrés dans l'application sont dénommés *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres **recommandés** du niveau de sécurité du trafic Internet sont considérés comme optimaux, ils sont recommandés par les experts de Kaspersky (cf. tableau ci-après). Vous pouvez sélectionner un des niveaux prédéfinis de protection du trafic Internet reçus ou envoyés via les protocoles HTTP et FTP, ou personnaliser le niveau de sécurité du trafic Internet. Après avoir modifié les paramètres du niveau de sécurité du trafic Internet, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du trafic Internet.

Pour activer ou désactiver le module Protection contre les menaces Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces Internet**.
3. Utilisez le commutateur **Protection contre les menaces Internet** pour activer ou désactiver le module.
4. Si vous avez activé le module, réalisez l'une des opérations suivantes dans la section **Niveau de protection** :
 - Pour appliquer un des niveaux prédéfinis de sécurité, sélectionnez-le à l'aide du curseur :
 - **Élevé**. Niveau de sécurité du trafic Internet auquel le module Protection contre les menaces Internet garantit l'analyse maximale du trafic Internet transmis à l'ordinateur via les protocoles HTTP et FTP. Le module Protection contre les menaces Internet analyse en détail tous les objets du trafic Internet à l'aide

de la sélection complète des bases de l'application et réalise également une [analyse heuristique](#) très minutieuse.

- **Recommandé.** Le niveau de sécurité du trafic Internet qui garantit l'équilibre optimum entre les performances de Kaspersky Endpoint Security et la sécurité du trafic Internet. Le module Protection contre les menaces Internet exécute l'analyse heuristique au niveau de valeur **moyenne**. Le niveau de sécurité du trafic Internet recommandé par les experts de Kaspersky. Les valeurs des paramètres pour le niveau de sécurité recommandé sont fournies dans le tableau ci-dessous.
- **Faible.** Niveau de sécurité du trafic Internet dont les paramètres garantissent l'analyse la plus rapide. Le module Protection contre les menaces Internet exécute l'analyse heuristique au niveau de valeur **superficielle**.
- Si vous souhaitez configurer un niveau de sécurité personnalisé, cliquez sur le bouton **Paramètres avancés** et définissez vos propres paramètres du module.

Vous pouvez restaurer les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut** dans la partie supérieure de la fenêtre.

5. Enregistrez vos modifications.

Paramètres recommandés par les experts de Kaspersky pour le module Protection contre les menaces Internet (niveau de sécurité recommandé)


| Paramètre | Valeur | Description |
|---|------------------|---|
| Vérifier si les liens figurent dans la base des liens malveillants | Activé | L'analyse des liens pour déterminer s'ils sont inclus dans la base de données des adresses Internet malveillantes vous permet de suivre les sites Internet qui ont été ajoutés à la liste de refus. La base des adresses Internet malveillantes est créée par les experts de Kaspersky. Elle est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security. |
| Vérifiez l'URL par rapport à la base de données des URL de phishing | Activé | La base des adresses Internet de phishing comprend les URL connues actuellement qui sont utilisées lors des attaques de phishing. Les experts de Kaspersky ajoutent à la base des adresses Internet de phishing fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). La base des adresses Internet de phishing est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security. |
| Utiliser l'analyse heuristique (Protection contre les menaces Internet) | Analyse standard | Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu. Lorsque le trafic Internet est analysé à la recherche de virus et d'autres applications qui présentent une menace, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique. |
| Utiliser l'analyse heuristique (Anti-Phishing) | Activé | Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu. |
| Action en | Bloquer le | Si cette action est sélectionnée, en cas de détection d'un objet |

| | | |
|--------------------------------------|-----------------------|--|
| cas de détection d'une menace | téléchargement | infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche un message dans le navigateur. |
|--------------------------------------|-----------------------|--|

Modification de l'action à effectuer sur les objets malveillants du trafic Internet

Par défaut, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche sur l'écran une fenêtre de notification sur le blocage.

Pour modifier l'action sur les objets malveillants du trafic Internet, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces Internet**.
3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants du trafic Internet :
 - **Interdire le téléchargement**. Si cette action est sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche un message dans le navigateur.
 - **Notifier**. Si cette option est sélectionnée, Kaspersky Endpoint Security permet, en cas de détection d'un objet infecté dans le trafic Internet, de télécharger cet objet sur l'ordinateur et ajoute les informations sur l'objet infecté à la liste des menaces actives.
4. Enregistrez vos modifications.

Analyse des URL par rapport aux bases de données de phishing et d'adresses Internet malveillantes

La vérification des liens pour contrôler leur appartenance aux URL de phishing permet d'éviter les *attaques de phishing*. L'exemple type en est le message électronique prétendument envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel de la banque. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site Internet de phishing peut figurer non seulement dans un message électronique, mais également dans un message ICQ, le module Protection contre les menaces Internet contrôle les tentatives d'accès à un site de phishing au niveau de l'analyse du trafic Internet et bloque l'accès à ces sites Internet. La liste des adresses de phishing est reprise dans la distribution de Kaspersky Endpoint Security.

Pour configurer l'analyse des liens selon les bases des adresses Internet malveillantes ou de phishing à l'aide du module Protection contre les menaces Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces Internet**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Procédez comme suit :

- Cochez la case **Vérifiez l'URL par rapport à la base de données des URL malveillantes** dans groupe **Méthodes d'analyse** si vous souhaitez que le module Protection contre les menaces Internet analyse les liens selon la base des adresses Internet malveillantes. L'analyse des liens pour déterminer s'ils sont inclus dans la base de données des adresses Internet malveillantes vous permet de suivre les sites Internet qui ont été ajoutés à la liste de refus. La base des adresses Internet malveillantes est créée par les experts de Kaspersky. Elle est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security.

Kaspersky Endpoint analyse tous les liens pour déterminer s'ils sont présents dans des bases de données d'adresses Internet malveillantes. Les paramètres d'analyse de la connexion sécurisée de l'application n'ont aucune incidence sur la fonctionnalité d'analyse des liens. Autrement dit, si les [analyses de connexions chiffrées sont désactivées](#), Kaspersky Endpoint Security vérifie les liens par rapport aux bases de données d'adresses Internet malveillantes, même si le trafic réseau est transmis au moyen d'une connexion chiffrée.

- Si vous souhaitez que le module Protection contre les menaces Internet vérifie les liens en fonction des bases de données d'adresses Internet de phishing, cochez la case **Vérifiez l'URL par rapport à la base de données des URL de phishing** dans le groupe **Anti-Phishing**. La base des adresses Internet de phishing comprend les URL connues actuellement qui sont utilisées lors des attaques de phishing. Les experts de Kaspersky ajoutent à la base des adresses Internet de phishing fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). La base des adresses Internet de phishing est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security.

Pour analyser les liens, vous pouvez également utiliser les bases de données de réputation de [Kaspersky Security Network](#).

5. Enregistrez vos modifications.

Utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les menaces Internet

Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier les menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

Pour configurer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.


2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces Internet**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Méthodes d'analyse**, cochez la case **Utiliser l'analyse heuristique** si vous souhaitez que l'application utilise l'analyse heuristique pour analyser le trafic Internet à la recherche de virus et d'autres logiciels malveillants. Ensuite, définissez le niveau de l'analyse heuristique à l'aide du curseur : **niveau superficiel**, **niveau intermédiaire** ou **niveau minutieux**.
5. Dans le groupe **Anti-phishing**, cochez la case **Utiliser l'analyse heuristique** si vous souhaitez que l'application utilise l'analyse heuristique lorsqu'elle analyse les pages Internet à la recherche de liens de phishing.
6. Enregistrez vos modifications.

Constitution d'une liste des URL de confiance

Vous pouvez composer une liste des URL dont vous faites confiance au contenu. Le module Protection contre les menaces Internet ne recherche pas la présence éventuelle de virus et d'autres applications présentant une menace dans les informations en provenance des adresses Internet de confiance. Cette fonctionnalité peut être utilisée, par exemple, si le module Protection contre les menaces Internet empêche le téléchargement d'un fichier depuis un site Internet que vous connaissez.

Le terme URL signifie à la fois l'URL d'une page Internet et celle d'un site Internet.

Pour composer une liste d'URL de confiance, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces Internet**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Cochez la case **Ne pas analyser le trafic Internet en provenance des adresses URL de confiance**.
Si la case est cochée, le module Protection contre les menaces Internet n'analyse pas le contenu des pages Internet/des sites Internet dont les adresses figurent dans la liste des URL de confiance. Vous pouvez ajouter à la liste des URL de confiance une adresse particulière d'une page Internet/d'un site Internet ou le masque de l'adresse de la page Internet/du site Internet.
5. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable.
6. Enregistrez vos modifications.

Exportation et importation de la liste des adresses Internet de confiance

Vous pouvez exporter la liste des adresses Internet de confiance dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses Internet du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des adresses Internet de confiance ou pour procéder à la migration de la liste vers un autre serveur.

Comment exporter et importer une liste d'adresses Internet de confiance dans la Console d'administration (MMC)



1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Protection contre les menaces Internet**.
6. Cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **URL de confiance**.
8. Pour exporter une liste d'adresses Internet de confiance, procédez comme suit :
 - a. Sélectionnez les adresses Internet de confiance que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune adresse Internet de confiance, Kaspersky Endpoint Security exportera toutes les adresses Internet.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des adresses Internet de confiance et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des adresses Internet de confiance dans un fichier XML.
9. Pour importer une liste d'adresses de confiance, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des adresses de confiance.
 - b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'adresses de confiance, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
10. Enregistrez vos modifications.

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste d'adresses Internet de confiance.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection principale** → **Protection contre les menaces Internet**.
5. Pour exporter la liste des exclusions dans le groupe **URL de confiance**, procédez comme suit :
 - a. Sélectionnez les adresses Internet de confiance que vous souhaitez exporter.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des adresses Internet de confiance et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des adresses Internet de confiance dans un fichier XML.
6. Pour importer une liste d'exclusions dans le groupe **URL de confiance**, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des adresses de confiance.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'adresses de confiance, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
7. Enregistrez vos modifications.

Protection contre les menaces par emails

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le module Protection contre les menaces par emails analyse les pièces jointes des messages entrants et sortants à la recherche d'éventuels virus et d'autres programmes présentant une menace. Le module analyse également les messages à la recherche de liens malveillants et de phishing. Par défaut, le module Protection contre les menaces par emails se trouve en permanence dans la RAM de l'ordinateur et analyse tous les messages reçus ou envoyés à l'aide des protocoles POP3, SMTP, IMAP, NNTP ou dans le client de messagerie Microsoft Office Outlook (MAPI). Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.

Le module Protection contre les menaces par emails n'analyse pas les messages si le client de messagerie est ouvert dans un navigateur.


Lorsqu'un fichier malveillant est détecté dans une pièce jointe, Kaspersky Endpoint Security change l'objet du message comme suit : [Message infecté] <objet du message> ou [Objet infecté supprimé] <objet du message>.

Le module interagit avec les clients de messagerie installés sur l'ordinateur. Pour le client de messagerie Microsoft Office Outlook, il existe une [extension avec des paramètres complémentaires](#). L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

Activation et désactivation de la Protection contre les menaces par emails

Par défaut, le module Protection contre les menaces par emails est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les menaces par emails. Les ensembles de paramètres enregistrés dans l'application sont dénommés *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres **recommandés** du niveau de sécurité de messagerie sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky (cf. tableau ci-après). Vous pouvez sélectionner un des niveaux de protection prédéfinis pour le courrier ou personnaliser le niveau de sécurité du courrier. Après avoir modifié les paramètres du niveau de sécurité du courrier, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du courrier.

Pour activer ou désactiver le module Protection contre les menaces par emails, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces par emails**.
3. Utilisez le commutateur **Protection contre les menaces par emails** pour activer ou désactiver le module.
4. Si vous avez activé le module, réalisez l'une des opérations suivantes dans la section **Niveau de protection** :
 - Pour appliquer un des niveaux prédéfinis de sécurité, sélectionnez-le à l'aide du curseur :
 - **Élevé**. Niveau de sécurité du courrier auquel la Protection contre les menaces par emails garantit le contrôle maximal des messages. Le module Protection contre les menaces par emails analyse les messages électroniques entrants et sortants et effectue également une analyse heuristique minutieuse. Un niveau de sécurité **Élevé** est recommandé pour un travail en environnement dangereux. Parmi les environnements dangereux, citons la connexion à un service de messagerie en ligne gratuit depuis le réseau domestique dépourvu de protection centralisée du courrier.

- **Recommandé.** Le niveau de sécurité du courrier qui garantit l'équilibre optimum entre les performances de Kaspersky Endpoint Security et la sécurité du courrier. Le module Protection contre les menaces par emails analyse l'ensemble des messages électroniques entrants et sortants et réalise également une analyse heuristique au niveau moyen. Le niveau de sécurité du courrier recommandé par les experts de Kaspersky. Les valeurs des paramètres pour le niveau de sécurité recommandé sont fournies dans le tableau ci-dessous.
- **Faible.** Le niveau de sécurité du courrier auquel le module Protection contre les menaces par emails analyse uniquement les messages électroniques entrants et réalise également une analyse heuristique superficielle. Il n'analyse pas les archives jointes aux messages électroniques. À ce niveau de sécurité du courrier, le module Protection contre les menaces par emails réalise l'analyse la plus rapide des messages électroniques et utilise le minimum de ressources du système d'exploitation. Le niveau de sécurité **Faible** pour la protection du courrier est recommandé pour les environnements bien protégés. Exemple de cet environnement : réseau local d'entreprise avec un système centralisé de protection du courrier.
- Si vous souhaitez configurer un niveau de sécurité personnalisé, cliquez sur le bouton **Paramètres avancés** et définissez vos propres paramètres du module.

Vous pouvez restaurer les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut** dans la partie supérieure de la fenêtre.

5. Enregistrez vos modifications.

Paramètres recommandés par les experts de Kaspersky pour le module Protection contre les menaces par emails (niveau de sécurité recommandé)


| Paramètre | Valeur | Description |
|--|--|---|
| Zone de protection | Analyser les messages entrants et sortants | La <i>Zone d'analyse</i> comprend les objets que le module vérifie lorsqu'il est exécuté : Analyser les messages entrants et sortants ou Analyser uniquement les messages entrants . Afin de protéger vos ordinateurs, il vous suffit de scanner les messages entrants. Vous pouvez activer l'analyse des messages sortants pour empêcher l'envoi de fichiers infectés dans les archives. Vous pouvez également activer l'analyse des messages sortants si vous souhaitez empêcher l'envoi de fichiers dans des formats particuliers, tels que des fichiers audio et Vidéo, par exemple. |
| Connecter l'extension Microsoft Outlook | Activé | Si la case est activée, l'analyse des messages électroniques transmis via les protocoles POP3, SMTP, NNTP, IMAP est activée au niveau de l'extension intégrée à Microsoft Outlook. En cas d'analyse du courrier à l'aide d'une extension pour Microsoft Outlook, il est recommandé d'utiliser le mode de mise en cache Exchange (Cached Exchange Mode). Vous pouvez obtenir tous les détails sur le mode Exchange mis en cache et sur ses recommandations d'utilisation dans la base de connaissances de Microsoft . |
| Analyser les archives jointes | Activé | Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE. |
| Analyser les fichiers joints aux formats Office | Activé | Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. |
| Filtre des pièces jointes | Renommer les types de pièces jointes indiqués | Si vous sélectionnez cette option, le module Protection contre les menaces par emails remplacera le dernier caractère d'extension trouvé dans les fichiers joints des types spécifiés par le caractère de soulignement (par exemple, pièce jointe.doc_). Ainsi, dans l'ordre d'ouvrir le fichier, l'utilisateur doit renommer le fichier. |

| | | |
|--|---|---|
| Analyse heuristique | Analyse standard | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| Action en cas de détection d'une menace | Désinfecter, supprimer si impossible | <p>Si un objet infecté est détecté dans un message entrant ou sortant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. L'utilisateur pourra accéder à un message avec une pièce jointe qui ne présente aucun danger. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security le supprime. Kaspersky Endpoint Security ajoute des informations relatives à l'action réalisée dans l'objet du message : [Objet infecté supprimé] <objet du message>.</p> |

Modification de l'action exécutée sur les messages électroniques infectés

Par défaut, le module Protection contre les menaces par emails tente de désinfecter tous les messages électroniques infectés détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails supprime les messages électroniques infectés.

Pour modifier l'action à exécuter sur les messages électroniques infectés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces par emails**.
3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un message infecté :
 - **Désinfecter ; supprimer si la désinfection est impossible.** Si un objet infecté est détecté dans un message entrant ou sortant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. L'utilisateur pourra accéder à un message avec une pièce jointe qui ne présente aucun danger. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security le supprime. Kaspersky Endpoint Security ajoute des informations relatives à l'action réalisée dans l'objet du message : [Objet infecté supprimé] <objet du message>.
 - **Désinfecter ; bloquer si la désinfection est impossible.** Si un objet infecté est détecté dans un message entrant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. L'utilisateur pourra accéder à un message avec une pièce jointe qui ne présente aucun danger. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security ajoute un avertissement à l'objet du message : [Message infecté] <objet du message>. L'utilisateur pourra accéder au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security bloque l'envoi du message et le client de messagerie affiche une erreur.
 - **Interdire.** Si un objet infecté est détecté dans un message entrant, Kaspersky Endpoint Security ajoute un avertissement à l'objet du message : [Message infecté] <objet du message>. L'utilisateur pourra


accéder au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, Kaspersky Endpoint Security bloque l'envoi du message et le client de messagerie affiche une erreur.

4. Enregistrez vos modifications.

Composition de la zone de protection du module Protection contre les menaces par emails

La *zone de protection* désigne les objets analysés par le module lorsque celui-ci est actif. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection du module Protection contre les menaces par emails reprennent les paramètres de l'intégration du module Protection contre les menaces par emails, le type de messages électroniques et les protocoles de messagerie dont le trafic est analysé par la Protection contre les menaces par emails. Par défaut, Kaspersky Endpoint Security analyse les messages électroniques entrant et sortant, le trafic des protocoles de courrier électronique POP3, SMTP, NNTP et IMAP, et s'intègre au client de messagerie Microsoft Office Outlook.

Pour former la zone de protection du module Protection contre les menaces par emails, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces par emails**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Zone de protection**, sélectionnez les messages à analyser :
 - **Analyser les messages entrants et sortants.**
 - **Analyser uniquement les messages entrants.**

Afin de protéger vos ordinateurs, il vous suffit de scanner les messages entrants. Vous pouvez activer l'analyse des messages sortants pour empêcher l'envoi de fichiers infectés dans les archives. Vous pouvez également activer l'analyse des messages sortants si vous souhaitez empêcher l'envoi de fichiers dans des formats particuliers, tels que des fichiers audio et Vidéo, par exemple.

Si vous sélectionnez l'analyse des messages entrants uniquement, il est recommandé d'analyser une fois tous les messages sortants car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

5. Dans le groupe **Intégration au système** procédez comme suit :

- Cochez la case **Analyser le trafic POP3/SMTP/NNTP/IMAP** si vous souhaitez que le module Protection contre les menaces par emails analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur.

Décochez la case **Analyser le trafic POP3/SMTP/NNTP/IMAP** si vous ne souhaitez pas que le module Protection contre les menaces par emails analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur. Dans ce cas, les messages sont analysés par l'extension du module Protection contre les menaces par emails installée dans le client de messagerie Microsoft Office Outlook après réception sur l'ordinateur de l'utilisateur, si la case **Connecter l'extension Microsoft Outlook** est cochée.

Si vous utilisez un autre client de messagerie que Microsoft Office Outlook, si la case **Analyser le trafic POP3/SMTP/NNTP/IMAP** est décochée, le module Protection contre les menaces par emails n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP.

- Cochez la case **Connecter l'extension Microsoft Outlook** si vous souhaitez donner l'accès à la configuration du module Protection contre les menaces par emails depuis l'application Microsoft Office Outlook et activer l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur à l'aide de l'extension dans l'application Microsoft Office Outlook.

Décochez la case **Connecter l'extension Microsoft Outlook**, si vous souhaitez bloquer l'accès à la configuration des paramètres du module Protection contre les menaces par emails depuis l'application Microsoft Office Outlook et désactiver l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur à l'aide de l'extension dans l'application Microsoft Office Outlook.


L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

6. Enregistrez vos modifications.

Analyse des fichiers composés joints aux messages électroniques

Vous pouvez activer ou désactiver l'analyse des objets joints aux messages, limiter la taille maximale des objets à analyser joints aux messages et la durée maximale d'analyse des objets joints aux messages.

Pour configurer l'analyse des fichiers composés joints aux messages électroniques, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces par emails**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans la section **Analyse des fichiers composés**, configurez les paramètres d'analyse :
 - **Analyser les fichiers joints aux formats Microsoft Office**. Analysez les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE.
 - **Analyser les archives jointes**. Analysez les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE.

Si pendant l'analyse, Kaspersky Endpoint Security détecte un mot de passe pour une archive dans le texte du message, ce mot de passe sera utilisé pour analyser le contenu de l'archive à la recherche d'applications malveillantes. Dans ce cas, le mot de passe n'est pas enregistré. Une archive est décompressée pendant l'analyse. Si une erreur d'application se produit pendant le processus de décompression, vous pouvez supprimer manuellement les fichiers décompressés qui sont enregistrés dans le chemin suivant : %systemroot%\temp. Les fichiers ont le préfixe PR.

- **Ne pas analyser les archives de plus de X Mo.** Si la case est cochée, le module Protection contre les menaces par emails exclut de l'analyse les archives jointes aux messages électroniques dont la taille est supérieure à la valeur définie. Si la case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques.
- **Limiter le temps d'analyse des archives à X secondes.** Si la case est cochée, la durée d'analyse des archives jointes aux emails est limitée à la valeur définie.


5. Enregistrez vos modifications.

Filtrage des pièces jointes dans les messages électroniques

La fonction de filtrage des pièces jointes ne s'applique pas aux messages électroniques sortants.

Les programmes malveillants peuvent se propager sous la forme des pièces jointes dans des messages électroniques. Vous pouvez configurer le filtrage selon le type des pièces jointes dans les messages de telle sorte qu'il soit possible de renommer ou de supprimer automatiquement les fichiers des types indiqués. En renommant une pièce jointe d'un type en particulier, Kaspersky Endpoint Security peut protéger votre ordinateur contre l'exécution d'un programme malveillant.

Pour configurer le filtrage des pièces jointes, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection contre les menaces par emails**.
3. Cliquez sur le bouton **Paramètres avancés**.
4. Dans le groupe **Filtre des pièces jointes**, exécutez une des actions suivantes :
 - Sélectionnez l'option **Désactiver le filtre** si vous ne souhaitez pas que le module Protection contre les menaces par emails filtre les pièces jointes dans les messages.
 - Sélectionnez l'option **Renommer les types de pièces jointes indiqués** si vous souhaitez que le module Protection contre les menaces par emails change les noms des fichiers des [types indiqués](#) joints aux messages.
 - Sélectionnez l'option **Supprimer les types de pièces jointes indiqués** si vous souhaitez que le module Protection contre les menaces par emails supprime les pièces jointes des [types de fichiers indiqués](#).
5. Si à l'étape précédente des instructions vous avez choisi l'option **Renommer les types de pièces jointes indiqués** ou l'option **Supprimer les types de pièces jointes indiqués**, cochez les cases en regard des types de fichier requis.

6. Enregistrez vos modifications.

Exportation et importation d'extensions pour le filtrage des pièces jointes

Vous pouvez exporter la liste des extensions de filtres de pièces jointes dans un fichier XML. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des extensions ou pour procéder à la migration de la liste vers un autre serveur.

[Comment exporter et importer une liste d'extensions de filtres de pièces jointes dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Protection contre les menaces par emails**.
6. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Filtre des pièces jointes**.
8. Pour exporter la liste des extensions, procédez comme suit :
 - a. Sélectionnez les extensions que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des extensions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des extensions dans un fichier XML.
9. Pour importer la liste des extensions, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des extensions.
 - c. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'extensions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
10. Enregistrez vos modifications.

[Comment exporter et importer une liste d'extensions de filtres de pièces jointes dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste d'exclusions.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection principale** → **Protection contre les menaces par emails**.
5. Pour exporter la liste des extensions dans le groupe **Filtre des pièces jointes**, procédez comme suit :
 - a. Sélectionnez les extensions que vous souhaitez exporter.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des extensions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des extensions dans un fichier XML.
6. Pour importer une liste d'extensions dans le groupe **Filtre des pièces jointes**, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des extensions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'extensions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
7. Enregistrez vos modifications.

Analyse du courrier dans Microsoft Office Outlook

L'intégration de l'extension du module Protection contre les menaces par emails à l'application Microsoft Office Outlook (ci-après Outlook) s'opère lors de l'installation de Kaspersky Endpoint Security. Cette extension permet de passer à la configuration des paramètres du module Protection contre les menaces par emails depuis l'application Outlook et d'indiquer le moment auquel il convient de rechercher parmi les messages électroniques la présence de virus et d'autres applications présentant une menace. L'extension du module Protection contre les menaces par emails pour Outlook peut analyser les messages entrants et sortants transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI. Kaspersky Endpoint Security prend également en charge l'utilisation d'autres clients de messagerie (y compris Microsoft Outlook Express®, Windows Mail et Mozilla™ Thunderbird™).

L'extension du module Protection contre les menaces par emails prend en charge les opérations avec Outlook 2010, 2013, 2016 et 2019.

Lorsqu'il s'agit du client de messagerie Mozilla Thunderbird, le module Protection contre les menaces par emails ne recherche pas des virus et d'autres programmes présentant une menace dans les messages transmis via le protocole IMAP en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

Dans l'application Outlook, les messages entrants sont d'abord analysés par le module Protection contre les menaces par emails (si la case [Analyser le trafic POP3, SMTP, NNTP et IMAP](#) est cochée dans l'interface de Kaspersky Endpoint Security), puis ils sont analysés par l'extension du module Protection contre les menaces par emails pour Outlook. Lorsque le module Protection contre les menaces par emails détecte un objet malveillant dans un message, il vous en avertit.

La configuration du module Protection contre les menaces par emails est possible dans Outlook si l'[extension Microsoft Outlook est connectée](#) dans l'interface de Kaspersky Endpoint Security.

L'analyse des messages sortants est confiée d'abord à l'extension du module Protection contre les menaces par emails pour Outlook, puis au module Protection contre les menaces par emails.

En cas d'analyse du courrier à l'aide de l'extension du module Protection contre les menaces par emails pour Outlook, il est recommandé d'utiliser le Mode Exchange mis en cache (Use Cached Exchange Mode). Vous pouvez obtenir tous les détails sur le mode Exchange mis en cache et sur ses recommandations d'utilisation dans la [base de connaissances de Microsoft](#).

Pour configurer le mode de fonctionnement de l'extension du module Protection contre les menaces par emails pour Outlook via Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Protection contre les menaces par emails**.
6. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Paramètres**.
La fenêtre **Protection contre les menaces par emails** s'ouvre.
7. Cliquez sur le bouton **Paramètres** dans le groupe **Intégration au système**.
8. Dans la fenêtre **Protection du courrier** procédez comme suit :
 - Cochez la case **Analyser à la réception** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages entrants au moment de leur arrivée dans la boîte aux lettres.
 - Cochez la case **Analyser à la lecture** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages entrants quand l'utilisateur les ouvre pour les lire.
 - Cochez la case **Analyser à l'envoi** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages sortants au moment de leur envoi.
9. Enregistrez vos modifications.

Protection contre les menaces réseau


Le module Protection contre les menaces réseau (Intrusion Detection System en anglais) recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque la connexion réseau issue de l'ordinateur attaquant.

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Endpoint Security. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la [mise à jour des bases et des modules de l'application](#).

Activation et désactivation de la Protection contre les menaces réseau

Par défaut, la Protection contre les menaces réseau est activée et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver la Protection contre les menaces réseau.


Pour activer ou désactiver le module Protection contre les menaces réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection contre les menaces réseau**.
3. Utilisez le commutateur **Protection contre les menaces réseau** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si la Protection contre les menaces réseau est activée, Kaspersky Endpoint Security analyse le trafic réseau entrant à la recherche d'activités caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque la connexion réseau issue de l'ordinateur attaquant.

Blocage d'un ordinateur attaquant

Pour bloquer un ordinateur attaquant, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection contre les menaces réseau**.
3. Cochez la case **Bloquer l'ordinateur à l'origine de l'attaque pendant X minutes**.

Si la case est cochée, le module Prévention des intrusions ajoute l'ordinateur à l'origine de l'attaque à la liste des ordinateurs à bloquer. Cela signifie que le module Protection contre les menaces réseau bloque la connexion réseau avec l'ordinateur attaquant après la première tentative d'attaque réseau pendant la durée indiquée. Ce groupe protège automatiquement l'ordinateur de l'utilisateur contre d'éventuelles attaques réseau futures à partir de la même adresse.

Vous pouvez consulter la liste des groupes dans la fenêtre de l'[outil Surveillance du réseau](#).

Kaspersky Endpoint Security efface la liste du groupe lorsque l'application est redémarrée et lorsque les paramètres de la Protection contre les menaces réseau sont modifiés.


4. Pour modifier la durée du blocage de l'ordinateur attaquant, dans le champ qui se trouve à côté de la case **Bloquer l'ordinateur à l'origine de l'attaque pendant X minutes**.
5. Enregistrez vos modifications.

Par conséquent, lorsque Kaspersky Endpoint Security détecte une tentative d'attaque réseau lancée contre l'ordinateur de l'utilisateur, il bloque toutes les connexions issues de l'ordinateur attaquant.

Configuration des adresses des exclusions du blocage

Kaspersky Endpoint Security peut reconnaître une attaque réseau et bloquer une connexion réseau non sécurisée qui transmet un grand nombre de paquets (par exemple, provenant de caméras de surveillance). Pour travailler avec des appareils de confiance, vous pouvez ajouter les adresses IP de ces appareils à la liste des exclusions.

Pour configurer les adresses des exclusions du blocage, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection contre les menaces réseau**.
3. Cliquez sur le lien **Configurer les exclusions**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Saisissez l'adresse IP de l'ordinateur à l'origine des attaques réseaux qui ne devront pas être bloquées.
6. Enregistrez vos modifications.

Par conséquent, Kaspersky Endpoint Security n'effectue aucun suivi de l'activité des appareils figurant dans la liste des exclusions.

Exportation et importation de la liste des exclusions de blocage

Vous pouvez exporter la liste des exclusions dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions ou pour procéder à la migration de la liste vers un autre serveur.

[Comment exporter et importer une liste d'exclusions dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Protection contre les menaces réseau**.
6. Dans le groupe **Paramètres de la Protection contre les menaces réseau**, cliquez sur le bouton **Exclusions**.
7. Pour exporter la liste des règles, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune exclusion, Kaspersky Endpoint Security exportera toutes les exclusions.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
8. Pour importer la liste des exclusions, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
9. Enregistrez vos modifications.

[Comment exporter et importer une liste d'exclusions dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste d'exclusions.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection principale** → **Protection contre les menaces réseau**.
5. Dans le groupe **Paramètres de la Protection contre les menaces réseau**, cliquez sur le lien **Exclusions**.
La liste des exclusions s'ouvre.
6. Pour exporter la liste des règles, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.
 - d. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - e. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
7. Pour importer la liste des exclusions, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

Configuration de la protection contre les attaques réseau par type

Kaspersky Endpoint Security vous permet de gérer la protection contre les types d'attaques réseau suivants :


- *L'inondation des réseaux* est une attaque contre les ressources réseau d'une organisation (comme les serveurs Internet). Cette attaque consiste à envoyer un grand nombre de requêtes pour surcharger la bande passante des ressources réseau. Lorsque cela se produit, les utilisateurs ne peuvent pas accéder aux ressources réseau de l'organisation.

- Une attaque par *analyse des ports* consiste à analyser les ports UDP, les ports TCP et les services réseau de l'ordinateur. Cette attaque permet à l'attaquant d'identifier le degré de vulnérabilité de l'ordinateur avant de mener des types d'attaques réseau plus dangereux. L'analyse des ports permet également au pirate informatique d'identifier le système d'exploitation de l'ordinateur et de sélectionner les attaques réseau appropriées pour ce système d'exploitation.
- Une *attaque MAC spoofing* consiste à substituer l'adresses MAC de l'appareil réseau (adaptateur réseau). Par conséquent, un individu malintentionné peut rediriger les données envoyées vers un appareil vers un autre et accéder à ces données. Kaspersky Endpoint Security permet de bloquer les attaques de type MAC Spoofing et de recevoir les notifications relatives aux attaques.

Vous pouvez désactiver la détection de ces types d'attaques au cas où certaines de vos applications autorisées effectueraient des opérations typiques de ces types d'attaques. Cela permettra d'éviter les fausses alertes.

Par défaut, Kaspersky Endpoint Security ne surveille pas les attaques par inondation des réseaux, analyse des ports et MAC spoofing.

Pour configurer la protection contre les attaques réseau par type, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection contre les menaces réseau**.
3. Utilisez le commutateur **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection de ces attaques.
4. Utilisez le commutateur **Protection contre les attaques MAC Spoofing**.
5. Dans le groupe **En cas de détection d'une attaque de type MAC spoofing**, sélectionnez l'une des options suivantes :
 - **Signaler uniquement.**
 - **Signaler et bloquer.**
6. Enregistrez vos modifications.

Firewall

Le pare-feu bloque les connexions non autorisées à l'ordinateur lorsque vous travaillez sur Internet ou sur un réseau local. De plus, le pare-feu contrôle l'activité des applications de l'ordinateur sur le réseau. Cela permet de protéger le réseau local de l'organisation contre le vol de données personnelles et d'autres attaques. Le module assure la protection de l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et de *règles réseau* prédéfinies.

L'Agent d'administration est utilisé dans le cadre de l'interaction avec Kaspersky Security Center. Le pare-feu crée automatiquement les règles réseau nécessaires au fonctionnement de l'application et de l'Agent d'administration. En conséquence, le pare-feu ouvre plusieurs ports sur l'ordinateur. Les ports qui sont ouverts dépendent du rôle de l'ordinateur (par exemple, le point de distribution). Pour en savoir plus à propos des ports qui seront ouverts sur l'ordinateur, consultez la rubrique [Aide de Kaspersky Security Center](#).

Règles réseau

Vous pouvez configurer les règles réseau aux niveaux suivants :

- *Règles pour les paquets réseau.* Elles sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Kaspersky Endpoint Security possède des règles de paquets réseau prédéfinies avec les autorisations recommandées par les experts de Kaspersky.
- *Règles réseau des applications* Elles sont utilisées pour limiter l'activité réseau d'une application spécifique. Elles tiennent compte non seulement des caractéristiques du paquet réseau, mais aussi de l'application spécifique destinataire ou expéditeur de ce paquet réseau.

Le contrôle de l'accès des applications aux ressources du système d'exploitation, aux processus et aux données personnelles est assuré par le [module Prévention des intrusions](#) avec l'aide des *autorisations de l'application*.

Lors du premier lancement de l'application, le pare-feu exécute les actions suivantes :

1. Il vérifie la sécurité de l'application à l'aide des bases antivirus chargées.
2. Il vérifie la sécurité de l'application dans Kaspersky Security Network.

Pour garantir le fonctionnement le plus efficace du Pare-feu, il est conseillé de [participer au Kaspersky Security Network](#).

3. Il place l'application dans un des *groupes de confiance* : de confiance, restrictions faibles, restrictions élevées, douteuses.

Le [groupe de confiance définit les privilèges](#) que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications. Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction du niveau de danger que cette application peut représenter pour l'ordinateur.

Kaspersky Endpoint Security place l'application dans un groupe de confiance pour les modules Pare-feu et Prévention des intrusions. Vous ne pouvez pas modifier le groupe de confiance uniquement pour le Pare-feu ou la Prévention des intrusions.

Si vous avez refusé de participer au KSN ou s'il n'y a pas de réseau, Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction des [paramètres du module Prévention des intrusions](#). Après la récupération des données sur la réputation de l'application dans KSN, le groupe de confiance peut être modifié automatiquement.

4. Il bloque l'activité réseau de l'application en fonction du groupe de confiance. Par exemple, les applications du groupe de confiance Restrictions élevées ne peuvent établir aucune connexion réseau.

Lors du prochain démarrage de l'application, Kaspersky Endpoint Security vérifie l'intégrité de l'application. Si l'application n'a pas été modifiée, le module lui applique les règles réseau en vigueur. En cas de modification de l'application, Kaspersky Endpoint Security l'analyse comme s'il s'agissait de sa première exécution.

Priorités des règles réseau

Chaque règle a une priorité. Plus haut se situe une règle dans la liste, plus haute est sa priorité. Si l'activité réseau est ajoutée à plusieurs règles, le Pare-feu réglemente l'activité réseau selon la règle affichant la priorité la plus élevée.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau pour les applications. Si des règles pour les paquets réseau et des règles réseau pour les applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Les règles réseau des applications fonctionnent comme suit : une règle réseau des applications comprend les règles d'accès selon l'état du réseau : *public*, *local* ou *fiable*. Par exemple, pour le groupe de confiance Restrictions élevées, toute activité réseau de l'application dans les réseaux de n'importe quel état est interdite. Si une règle réseau est définie pour une application individuelle (application parent), les processus enfants d'autres applications seront exécutés conformément à la règle réseau de l'application parent. S'il n'y a pas de règle réseau pour l'application, les processus enfant seront exécutés conformément à la règle d'accès aux réseaux du groupe de confiance.

Par exemple, vous avez interdit toute activité réseau de toutes les applications quel que soit l'état du réseau, sauf pour le navigateur X. Si vous lancez l'installation du navigateur Y (processus enfant) dans le navigateur X (processus parent), le programme d'installation du navigateur Y aura accès au réseau et téléchargera les fichiers requis. Après l'installation, le navigateur Y se verra refuser toutes les connexions réseau conformément aux paramètres du pare-feu. Pour interdire l'activité réseau au programme d'installation du navigateur Y en tant que processus enfant, vous devez ajouter une règle réseau pour le programme d'installation du navigateur Y.

États des connexions réseau.

Le Pare-feu permet de surveiller l'activité du réseau en fonction de l'état de la connexion réseau. Kaspersky Endpoint Security obtient l'état de la connexion réseau via le système d'exploitation de l'ordinateur. L'état de la connexion réseau dans le système d'exploitation est défini par l'utilisateur lors de la configuration de la connexion. Vous pouvez [modifier l'état de la connexion réseau dans les paramètres de Kaspersky Endpoint Security](#). Le Pare-feu contrôle l'activité réseau en fonction de l'état du réseau dans les paramètres de Kaspersky Endpoint Security, et non pas du système d'exploitation.

Il existe les états suivant de la connexion réseau :

- **Réseau public.** Le réseau n'est pas protégé par des logiciels antivirus, des pare-feu, des filtres (par exemple, le Wi-Fi dans un café). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur d'accéder aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur. Le Pare-feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.


Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.

- **Réseau local.** Réseau pour les utilisateurs dont l'accès est limité aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).
- **Réseau de confiance.** Réseau sûr dont l'utilisation n'expose pas l'ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état n'importe quelle activité réseau dans le cadre de ce réseau.

Activation et désactivation du Pare-feu

Par défaut, le Pare-feu est activé et fonctionne en mode optimal.


Pour activer ou désactiver le Pare-feu, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Utilisez le commutateur **Pare-feu** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Modification de l'état de la connexion réseau

Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.

Pour modifier l'état d'une connexion réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Réseaux disponibles**.
4. Sélectionnez la connexion réseau dont vous souhaitez modifier l'état.
5. Dans la colonne **Type de réseau**, sélectionnez l'état de la connexion réseau :
 - **Réseau public**. Le réseau n'est pas protégé par des logiciels antivirus, des pare-feu, des filtres (par exemple, le Wi-Fi dans un café). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur d'accéder aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur. Le Pare-feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.
 - **Réseau local**. Réseau pour les utilisateurs dont l'accès est limité aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).
 - **Réseau de confiance**. Réseau sûr dont l'utilisation n'expose pas l'ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état n'importe quelle activité réseau dans le cadre de ce réseau.
6. Enregistrez vos modifications.

Application des règles pour les paquets réseau

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles pour les paquets réseau :

- Créer une nouvelle règle pour les paquets réseau.

Vous pouvez créer une nouvelle règle pour les paquets réseau en sélectionnant un ensemble des conditions et des actions relatives aux paquets réseau et aux flux de données.

- Activer et désactiver la règle pour les paquets réseau.

Toutes les règles pour les paquets réseau créés par défaut par le Pare-feu possèdent l'état *Activé*. Si la règle pour les paquets réseau est activée, le Pare-feu applique cette règle.

Vous pouvez activer toute règle pour les paquets réseau, sélectionnée dans la liste des règles pour les paquets réseau. Si la règle pour les paquets réseau est désactivée, le Pare-feu suspend temporairement l'application de la règle.

La nouvelle règle pour les paquets réseau créée par l'utilisateur est par défaut ajoutée à la liste des règles pour les paquets réseau avec l'état *Activé*.

- Modifier les paramètres de la règle pour les paquets réseau.

Après avoir créé une nouvelle règle pour les paquets réseau, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle pour les paquets réseau.

Dans la liste des règles pour les paquets réseau, vous pouvez modifier l'action que le Pare-feu exécute en cas de détection d'une activité réseau de la règle pour les paquets réseau indiquée.

- Modifier la priorité de la règle pour les paquets réseau.

Vous pouvez augmenter ou diminuer la priorité de la règle pour les paquets réseau sélectionnée dans la liste.

- Supprimer la règle pour les paquets réseau.

Vous pouvez supprimer la règle pour les paquets réseau si vous ne souhaitez pas que le Pare-feu applique cette règle en cas de détection d'une activité réseau et qu'elle soit affichée dans la liste des règles pour les paquets réseau avec l'état *Désactivé*.

Création d'une règle pour les paquets réseau

Vous pouvez créer une règle pour les paquets réseau des façons suivantes :

- Utilisez l'[outil Surveillance du réseau](#).

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de l'ordinateur d'un utilisateur en temps réel. C'est pratique, car vous n'avez pas besoin de configurer tous les paramètres des règles. Certains paramètres du pare-feu seront insérés automatiquement à partir des données de l'outil Surveillance du réseau. L'outil Surveillance du réseau n'est accessible que dans l'interface de l'application.

- Configurez les paramètres du pare-feu.

Cela vous permet de régler avec précision les paramètres du pare-feu. Vous pouvez créer des règles pour toute activité réseau, même s'il n'y a aucune activité réseau à l'heure actuelle.

Au moment de créer des règles pour les paquets réseau, il ne faut pas oublier qu'elles ont priorité sur les règles réseau pour les applications.

[Utilisation de l'outil Surveillance du réseau pour créer une règle pour les paquets réseau dans l'interface de l'application](#) 

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Surveillance du réseau**.

2. Sélectionnez l'onglet **Activité réseau**.

L'onglet **Activité réseau** affiche toutes les connexions réseau à l'ordinateur de l'utilisateur qui sont actuellement actives. Il affiche non seulement les connexions réseau ouvertes par l'ordinateur de l'utilisateur, mais aussi les connexions réseau entrantes.

3. Dans le menu contextuel d'une connexion réseau, sélectionnez **Créer une règle de paquet**.

Cette action permet d'ouvrir les propriétés des règles réseau.

4. Définissez l'état **Actif** pour la règle des paquets.

5. Saisissez manuellement le nom du service réseau dans le champ **Nom**.

6. Configurez les paramètres des règles réseau (cf. tableau ci-après).

Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Modèle de règle réseau**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.

Tous les paramètres de règles réseau seront remplis automatiquement.

7. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).


8. Cliquez sur le bouton **Enregistrer**.

La nouvelle règle réseau sera ajoutée à la liste.


9. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.

10. Enregistrez vos modifications.

[Utilisation des paramètres du pare-feu pour créer une règle pour les paquets réseau dans l'interface de l'application](#) ²

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles pour les paquets**.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
4. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles réseau.
5. Définissez l'état **Actif** pour la règle des paquets.
6. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
7. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Modèle de règle réseau**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.
8. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).
9. Cliquez sur le bouton **Enregistrer**.
La nouvelle règle réseau sera ajoutée à la liste.
10. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.
11. Enregistrez vos modifications.

[Procédure de création d'une règle pour les paquets réseau dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.
6. Dans le groupe **Paramètres du pare-feu**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la liste des règles pour les paquets réseau et la liste des règles réseau des applications.
7. Sélectionnez l'onglet **Règles pour les paquets réseau**.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
8. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles pour les paquets.
9. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
10. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le bouton . Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.
11. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).
12. Cliquez sur le bouton **Enregistrer**.
La nouvelle règle réseau sera ajoutée à la liste.
13. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.
14. Enregistrez vos modifications.

Le pare-feu contrôlera les paquets réseau conformément à la règle. Vous pouvez désactiver une règle pour les paquets du fonctionnement du pare-feu sans la supprimer de la liste. Pour ce faire, décochez la case à côté de l'objet.

[Procédure de création d'une règle pour les paquets réseau dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection principale** → **Pare-feu**.
5. Dans le groupe **Paramètres du pare-feu**, cliquez sur le lien **Règles pour les paquets réseau**.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
6. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles pour les paquets.
7. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
8. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Sélectionner le modèle**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.
9. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).
10. Cliquez sur le bouton **Enregistrer**.
La nouvelle règle réseau sera ajoutée à la liste.
11. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.
12. Enregistrez vos modifications.

Le pare-feu contrôlera les paquets réseau conformément à la règle. Vous pouvez désactiver une règle pour les paquets du fonctionnement du pare-feu sans la supprimer de la liste. Utilisez le commutateur dans la colonne **État** pour activer ou désactiver la règle pour les paquets.


Paramètres des règles pour les paquets réseau

| Paramètre | Description |
|------------------|---|
| Action | <p>Autoriser.</p> <p>Bloquer.</p> <p>Par règles de l'application. Si cette option est sélectionnée, le pare-feu applique les règles réseau des applications à la connexion réseau.</p> |
| Protocole | <p>Contrôlez l'activité du réseau sur le protocole sélectionné : TCP, UDP, ICMP, ICMPv6, IGMP et GRE.</p> <p>Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP.</p> <p>Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les numéros des ports (séparés par une virgule) de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée.</p> |

| | |
|---------------------------|---|
| Direction | <p>Entrant (paquet). Le pare-feu applique la règle réseau à tous les paquets réseau entrants.</p> <p>Entrant. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par un ordinateur distant.</p> <p>Entrant/Sortant. Le pare-feu applique la règle réseau aux paquets réseau entrants et sortants, quel que soit l'ordinateur (l'ordinateur de l'utilisateur ou l'ordinateur distant) qui a amorcé la connexion réseau.</p> <p>Sortant (paquet). Le pare-feu applique la règle réseau à tous les paquets réseau sortants.</p> <p>Sortant. Le pare-feu applique la règle réseau à tous les paquets réseau envoyés via une connexion qui a été amorcée par l'ordinateur de l'utilisateur.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Le protocole TCP établit une connexion. Utilisez les directions Entrant, Sortant et Entrant/Sortant pour le protocole TCP. Tous les autres protocoles n'établissent aucune connexion, mais ils envoient des paquets. Pour tous les autres protocoles, utilisez les directions Entrant (paquet), Sortant (paquets) ou Entrant/Sortant.</p> </div> |
| Adaptateurs réseau | <p>Adaptateurs réseau qui peuvent envoyer et/ou recevoir des paquets réseau. L'indication des paramètres réseaux permet de distinguer les paquets envoyés ou reçus par les adaptateurs réseaux dotés d'adresses IP identiques.</p> |
| Durée de vie (TTL) | <p>Limitez le contrôle des paquets réseau en fonction de leur durée de vie (TTL).</p> |
| Adresses distantes | <p>Adresses réseau des ordinateurs distants qui peuvent envoyer et recevoir des paquets réseau. Le pare-feu applique la règle réseau à la plage définie d'adresses réseau distantes. Vous pouvez inclure toutes les adresses IP dans une règle réseau, créer une liste séparée d'adresses IP ou sélectionner un sous-réseau (Réseaux de confiance, Réseaux locaux, Réseaux publics).</p> |
| Adresses locales | <p>Adresses réseau des ordinateurs qui peuvent envoyer et recevoir des paquets réseau. Le Pare-feu applique la règle réseau à la plage définie d'adresses réseau locales. Vous pouvez inclure toutes les adresses IP dans une règle de réseau ou créer une liste séparée d'adresses IP.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Les applications ne peuvent pas toujours obtenir une adresse locale. Si c'est le cas, ce paramètre est ignoré.</p> </div> |

Activation et désactivation de la règle pour les paquets réseau

Pour activer ou désactiver la règle pour les paquets réseau, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles pour les paquets**.
 Cette action permet d'ouvrir la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.
4. Choisissez dans la liste la règle pour les paquets réseau requise.

5. Utilisez le commutateur dans la colonne **État** pour activer ou désactiver la règle.

6. Enregistrez vos modifications.

Modification de l'action du Pare-feu pour la règle pour les paquets réseau

Pour modifier l'action du Pare-feu pour la règle pour les paquets réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles pour les paquets**.
Cette action permet d'ouvrir la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.
4. Sélectionnez-la dans la liste des règles pour les paquets réseau et cliquez sur le bouton **Modifier**.
5. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
 - **Autoriser.**
 - **Bloquer.**
 - **Par règles de l'application.**
6. Enregistrez vos modifications.


Modification de la priorité de la règle pour les paquets réseau

La priorité d'exécution de la règle pour les paquets réseau est définie par l'emplacement de la règle dans la liste des règles pour les paquets réseau. La première règle pour les paquets réseau dans la liste des règles pour les paquets réseau possède la priorité la plus élevée.

Chaque règle pour les paquets réseau que vous avez créée est ajoutée à la fin de la liste des règles pour les paquets réseau et possède la priorité la plus faible.

Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles pour les paquets réseau haut/bas. Suivant chacune des règles pour les paquets réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Pour modifier la priorité de la règle pour les paquets réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles pour les paquets**.

Cette action permet d'ouvrir la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.

4. Choisissez dans la liste la règle pour les paquets réseau pour laquelle vous souhaitez modifier la priorité.
5. À l'aide des boutons **Haut** et **Bas**, déplacez la règle pour les paquets réseau vers la position requise dans la liste des règles pour les paquets réseau.
6. Enregistrez vos modifications.

Règles d'exportation et d'importation des paquets réseau

Vous pouvez exporter la liste des règles de paquets réseau dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre de règles du même type. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles de paquets réseau ou pour procéder à la migration de la liste vers un autre serveur.

[Comment exporter et importer une liste de règles de paquets réseau dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.
6. Pour exporter une liste de règles de paquets réseau, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune règle, Kaspersky Endpoint Security exportera toutes les règles.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des règles et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.
7. Pour importer une liste de règles de paquets réseau, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

[Comment exporter et importer une liste de règles de paquets réseau dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer la liste des règles.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection principale** → **Pare-feu**.
5. Cliquez sur le lien **Règles pour les paquets réseau**.
6. Pour exporter une liste de règles de paquets réseau, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les règles sélectionnées ou exporter la liste complète.
 - d. Cliquez sur le bouton **Exporter**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML dans le dossier des téléchargements par défaut.
7. Pour importer une liste de règles de paquets réseau, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

Application des règles réseau pour les applications

Kaspersky Endpoint Security regroupe par défaut toutes les applications installées selon le nom de l'éditeur de l'application dont il contrôle l'activité de réseau ou de fichiers. Les groupes d'applications sont à leur tour regroupés en [groupes de confiance](#). Toutes les applications et tous les groupes d'applications héritent des propriétés de leur groupe parent : règles du contrôle des applications, règles réseau de l'application, ainsi que la priorité de leur exécution.

À l'instar du module [Prévention des intrusions](#), le module Pare-feu applique par défaut les règles réseau du groupe d'applications afin de filtrer l'activité réseau de toutes les applications appartenant à ce groupe. Les règles réseau du groupe d'applications définissent les droits d'accès aux différentes connexions réseau attribués aux applications qui font partie du groupe.

Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Endpoint Security a identifié sur l'ordinateur. Vous avez deux options pour modifier l'action du Pare-feu pour les règles réseau du groupe d'applications créées par défaut. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau du groupe d'applications créées par défaut, ni modifier leur priorité.

Vous pouvez également créer une règle réseau pour une application distincte. La priorité de cette règle sera plus élevée que celle de la règle réseau du groupe auquel appartient cette application.

Création d'une règle réseau d'applications

Par défaut le contrôle de l'application est assuré par les règles réseau définies pour le [groupe de confiance](#) auquel Kaspersky Endpoint Security a attribué l'application lors de son premier démarrage. Le cas échéant, vous pouvez créer des règles réseau pour tout le groupe de confiance, pour une application spécifique ou pour un groupe d'applications qui font partie du groupe de confiance.

Les règles réseau définies manuellement ont une priorité plus élevée que les règles réseau qui ont été déterminées pour un groupe de confiance. Autrement dit, si les règles d'application définies manuellement diffèrent des règles d'application déterminées pour un groupe de confiance, le pare-feu contrôle l'activité des applications selon les règles d'application définies manuellement.

Par défaut, le pare-feu crée les règles réseau suivantes pour chaque application :

- Toute activité réseau dans les réseaux de confiance.
- Toute activité réseau dans les réseaux locaux.
- Toute activité réseau dans les réseaux publics.

Kaspersky Endpoint Security contrôle l'activité réseau des applications selon des règles réseau prédéfinies comme suit :

- De confiance, Restrictions faibles : toute activité réseau est autorisée.
- Restrictions élevées et Douteux : toute activité réseau est bloquée.

Les règles d'application prédéfinies ne peuvent être ni modifiées ni supprimées.

Vous pouvez créer une règle réseau des applications des façons suivantes :

- Utilisez l'[outil Surveillance du réseau](#).

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de l'ordinateur d'un utilisateur en temps réel. C'est pratique, car vous n'avez pas besoin de configurer tous les paramètres des règles. Certains paramètres du pare-feu seront insérés automatiquement à partir des données de l'outil Surveillance du réseau. L'outil Surveillance du réseau n'est accessible que dans l'interface de l'application.

- Configurez les paramètres du pare-feu.

Cela vous permet de régler avec précision les paramètres du pare-feu. Vous pouvez créer des règles pour toute activité réseau, même s'il n'y a aucune activité réseau à l'heure actuelle.

Lorsque vous créez des règles réseau pour des applications, n'oubliez pas que les règles pour les paquets réseau ont la priorité sur les règles réseau des applications.

Utilisation de l'outil Surveillance du réseau pour créer une règle réseau d'applications dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Surveillance du réseau**.

2. Sélectionnez l'onglet **Activité réseau** ou **Ouvrir les ports**.

L'onglet **Activité réseau** affiche toutes les connexions réseau à l'ordinateur de l'utilisateur qui sont actuellement actives. Il affiche non seulement les connexions réseau ouvertes par l'ordinateur de l'utilisateur, mais aussi les connexions réseau entrantes.

L'onglet **Ports ouverts** reprend tous les ports réseau ouverts sur l'ordinateur de l'utilisateur.

3. Dans le menu contextuel d'une connexion réseau, sélectionnez **Créer une règle pour l'application**.

La fenêtre des règles et des propriétés de l'application s'ouvre.

4. Sélectionnez l'onglet **Règles réseau**.

Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.

5. Cliquez sur le bouton **Ajouter**.

Cette action permet d'ouvrir les propriétés des règles réseau.

6. Saisissez manuellement le nom du service réseau dans le champ **Nom**.

7. Configurez les paramètres des règles réseau (cf. tableau ci-après).

Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Modèle de règle réseau**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.

Tous les paramètres de règles réseau seront remplis automatiquement.

8. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).

9. Cliquez sur le bouton **Enregistrer**.


La nouvelle règle réseau sera ajoutée à la liste.

10. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.


11. Enregistrez vos modifications.

Utilisation des paramètres du pare-feu pour créer une règle réseau d'applications dans l'interface de l'application



1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles de l'application**.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
4. Dans la liste des applications, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez créer une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Détails et règles**.
La fenêtre des règles et des propriétés de l'application s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles réseau.
8. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
9. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Modèle de règle réseau**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.
10. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).
11. Cliquez sur le bouton **Enregistrer**.
La nouvelle règle réseau sera ajoutée à la liste.
12. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.
13. Enregistrez vos modifications.

[Procédure de création d'une règle réseau d'applications dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.
6. Dans le groupe **Paramètres du pare-feu**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la liste des règles pour les paquets réseau et la liste des règles réseau des applications.
7. Sélectionnez l'onglet **Règles réseau des applications**.
8. Cliquez sur le bouton **Ajouter**.
9. Dans la fenêtre ouverte, entrez les critères de recherche de l'application pour laquelle vous souhaitez créer une règle réseau.
Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères * et ? lors de la saisie d'un masque.
10. Cliquez sur le bouton **Actualiser**.
Kaspersky Endpoint Security recherchera l'application dans la liste consolidée des applications installées sur les ordinateurs administrés. Kaspersky Endpoint Security affichera une liste d'applications qui répondent à vos critères de recherche.
11. Sélectionnez l'application requise.
12. Dans la liste déroulante **Ajouter les applications sélectionnées au groupe <groupe de confiance>**, sélectionnez **Groupes par défaut**, puis cliquez sur **OK**.
L'application sera ajoutée au groupe par défaut.
13. Sélectionnez l'application concernée, puis sélectionnez **Privilèges des applications** dans le menu contextuel de l'application.
La fenêtre des règles et des propriétés de l'application s'ouvre.
14. Sélectionnez l'onglet **Règles réseau**.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
15. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles réseau.
16. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
17. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le bouton . Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.

18. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).
19. Cliquez sur le bouton **Enregistrer**.
La nouvelle règle réseau sera ajoutée à la liste.
20. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.
21. Enregistrez vos modifications.

[Procédure de création d'une règle réseau d'applications dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection principale** → **Pare-feu**.
5. Dans le groupe **Paramètres du pare-feu**, cliquez sur le lien **Règles réseau des applications**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
6. Choisissez l'onglet **Privilèges des applications**.
Vous verrez une liste des groupes de confiance sur le côté gauche de la fenêtre et leurs propriétés sur le côté droit.
7. Cliquez sur le bouton **Ajouter**.
Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.
8. Cliquez sur le lien **Groupe cible sélectionné** pour sélectionner le groupe de confiance approprié pour l'application.
9. Sélectionnez le type d'**application**. Cliquez sur le bouton **Suivant**.
Si vous souhaitez créer une règle réseau pour plusieurs applications, sélectionnez le type de **groupe** et définissez un nom pour le groupe d'application.
10. Dans la liste ouverte des applications, sélectionnez les applications pour lesquelles vous souhaitez créer une règle réseau.
Utilisez un filtre. Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères * et ? lors de la saisie d'un masque.
11. Quittez l'Assistant en cliquant sur **OK**.
L'application sera ajoutée au groupe de confiance.
12. Dans la partie gauche de la fenêtre, sélectionnez l'application concernée.
13. Dans la partie droite de la fenêtre, sélectionnez **Règles réseau** dans la liste déroulante.
Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.
14. Cliquez sur le bouton **Ajouter**.
Cette action permet d'ouvrir les propriétés des règles d'application.
15. Saisissez manuellement le nom du service réseau dans le champ **Nom**.
16. Configurez les paramètres des règles réseau (cf. tableau ci-après).
Vous pouvez sélectionner un modèle de règle prédéfini en cliquant sur le lien **Sélectionner le modèle**. Les modèles de règles décrivent les connexions réseau les plus fréquemment utilisées.
Tous les paramètres de règles réseau seront remplis automatiquement.

17. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le [rapport](#).

18. Cliquez sur le bouton **Enregistrer**.

La nouvelle règle réseau sera ajoutée à la liste.

19. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle réseau.


20. Enregistrez vos modifications.

Paramètres des règles réseau des applications

| Paramètre | Description |
|---------------------------|---|
| Action | Autoriser. Bloquer. |
| Protocole | Contrôlez l'activité du réseau sur le protocole sélectionné : TCP, UDP, ICMP, ICMPv6, IGMP et GRE. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les numéros des ports (séparés par une virgule) de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée. |
| Direction | Entrant. Entrant/Sortant. Sortant. |
| Adresses distantes | Adresses réseau des ordinateurs distants qui peuvent envoyer et recevoir des paquets réseau. Le pare-feu applique la règle réseau à la plage définie d'adresses réseau distantes. Vous pouvez inclure toutes les adresses IP dans une règle réseau, créer une liste séparée d'adresses IP ou sélectionner un sous-réseau (Réseaux de confiance, Réseaux locaux, Réseaux publics). |
| Adresses locales | Adresses réseau des ordinateurs qui peuvent envoyer et recevoir des paquets réseau. Le Pare-feu applique la règle réseau à la plage définie d'adresses réseau locales. Vous pouvez inclure toutes les adresses IP dans une règle de réseau ou créer une liste séparée d'adresses IP. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">Les applications ne peuvent pas toujours obtenir une adresse locale. Si c'est le cas, ce paramètre est ignoré.</div> |

Activation et désactivation de la règle réseau des applications

Pour activer ou désactiver la règle réseau des applications, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles de l'application**.
Cette action permet d'ouvrir la liste des règles de l'application.

4. Dans la liste des applications, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez créer ou modifier une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Détails et règles**.
La fenêtre des règles et des propriétés de l'application s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau du groupe d'applications la règle réseau requise.
La fenêtre des propriétés des règles réseau s'ouvre.
8. Définissez l'état **Actif** ou **Inactif** pour la règle réseau.
Vous ne pouvez pas désactiver la règle réseau du groupe d'applications si elle a été créée par le Pare-feu par défaut.
9. Enregistrez vos modifications.

Modification de l'action du Pare-feu pour la règle réseau des applications

Vous pouvez modifier l'action du Pare-feu pour toutes les règles réseau d'application ou de groupe d'applications qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle réseau d'une application ou d'un groupe d'applications qui a été créée manuellement.

Pour modifier l'action du Pare-feu pour toutes les règles réseau d'application ou de groupe des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles de l'application**.
Cette action permet d'ouvrir la liste des règles de l'application.
4. Sélectionnez dans la liste l'application ou le groupe d'applications si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau créées par défaut. Les règles réseau définies manuellement resteront inchangées.
5. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel, sélectionnez **Règles réseau**, puis choisissez l'action que vous souhaitez définir :
 - **Hériter**.
 - **Autoriser**.
 - **Bloquer**.
6. Enregistrez vos modifications.

Pour modifier l'action du Pare-feu pour une règle réseau d'une application ou d'un groupe d'applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles de l'application**.
Cette action permet d'ouvrir la liste des règles de l'application.
4. Dans la liste, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez modifier l'action d'une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Détails et règles**.
La fenêtre des règles et des propriétés de l'application s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Choisissez la règle réseau pour laquelle vous voulez modifier l'action du Pare-feu.
8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :
 - **Hériter.**
 - **Autoriser.**
 - **Bloquer.**
 - **Consigner dans le rapport.**
9. Enregistrez vos modifications.


Modification de la priorité de la règle réseau des applications

La priorité d'exécution de la règle réseau est définie par l'emplacement de la règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Suivant chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau créées manuellement ont une priorité plus élevée que les règles réseau créées par défaut.

Vous ne pouvez pas modifier la priorité des règles réseau d'un groupe d'applications créées par défaut.

Pour modifier la priorité d'une règle réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Pare-feu**.
3. Cliquez sur le bouton **Règles de l'application**.
Cette action permet d'ouvrir la liste des règles de l'application.

4. Dans la liste des applications, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez modifier la priorité de la règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Détails et règles**.
La fenêtre des règles et des propriétés de l'application s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez la règle réseau dont vous souhaitez modifier la priorité.
8. À l'aide des boutons **Haut** et **Bas**, déplacez la règle réseau vers la position requise dans la liste des règles réseau.
9. Enregistrez vos modifications.

Surveillance du réseau

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de l'ordinateur d'un utilisateur en temps réel.

Pour lancer la Surveillance du réseau, procédez comme suit :

Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Surveillance du réseau**.

La fenêtre **Surveillance du réseau** s'ouvre. Cette fenêtre affiche les informations sur l'activité réseau de l'ordinateur de l'utilisateur sur quatre onglets :

- L'onglet **Activité réseau** affiche toutes les connexions réseau à l'ordinateur de l'utilisateur qui sont actuellement actives. Il affiche non seulement les connexions réseau ouvertes par l'ordinateur de l'utilisateur, mais aussi les connexions réseau entrantes. Sous cet onglet, vous pouvez également [créer des règles pour les paquets réseau](#) pour le fonctionnement du pare-feu.
- L'onglet **Ports ouverts** reprend tous les ports réseau ouverts sur l'ordinateur de l'utilisateur. Sous cet onglet, vous pouvez également [créer des règles pour les paquets réseau](#) et [des règles d'applications](#) pour le fonctionnement du pare-feu.
- L'onglet **Trafic réseau** affiche le volume du trafic réseau entrant et sortant entre l'ordinateur de l'utilisateur et les autres ordinateurs du réseau auquel l'utilisateur est connecté actuellement.
- L'onglet **Ordinateurs bloqués** affiche la liste des adresses IP des ordinateurs distants dont l'activité réseau a été bloquée par le module Protection contre les menaces réseau après une tentative d'attaque réseau effectuée depuis cette adresse IP.

Protection BadUSB

Certains virus modifient l'application interne des appareils USB afin que le système d'exploitation considère l'appareil USB comme un clavier. Par conséquent, le virus peut exécuter des commandes sous votre compte d'utilisateur, par exemple, pour télécharger des logiciels malveillants.

Le module Protection BadUSB permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier.

Quand un appareil USB est connecté à l'ordinateur et que le système d'exploitation le reconnaît comme étant un clavier, l'application génère un code numérique et invite l'utilisateur à le saisir à partir de ce clavier ou à l'aide d'[un clavier numérique, si ce dernier est disponible](#) (cf. ill. ci-après). C'est ce qu'on appelle l'autorisation du clavier.

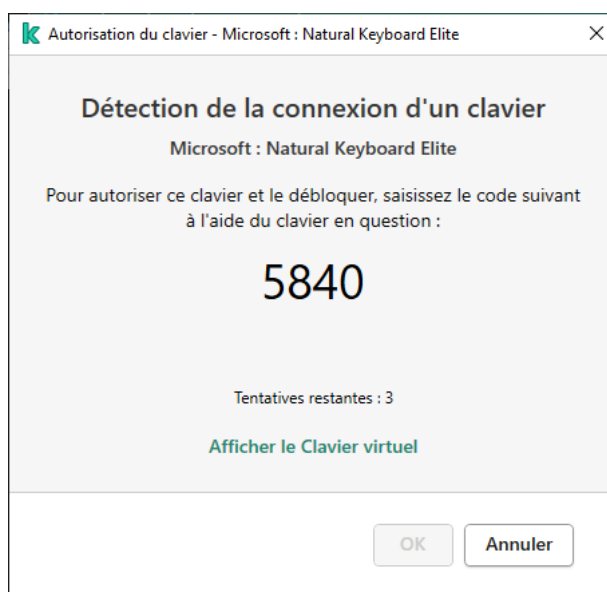
Si le code est saisi correctement, l'application enregistre les paramètres d'identification VID/PID du clavier et le numéro de port utilisé pour la connexion dans la liste des claviers autorisés. Il ne sera pas nécessaire d'autoriser à nouveau le clavier lors de la prochaine connexion ou suite au redémarrage du système d'exploitation.

Par contre, si vous connectez un clavier autorisé à un autre port USB, l'application sollicitera à nouveau l'autorisation.

Si le code numérique n'est pas saisi correctement, l'application crée un autre code. Le nombre maximum de tentatives de saisie est limité à trois. Après trois tentatives infructueuses ou si la fenêtre **Autorisation de clavier** <nom du clavier> est fermée, l'application bloque la saisie à l'aide de ce clavier. Si le clavier est reconnecté ou si le système d'exploitation redémarre, l'application proposera à nouveau d'autoriser le clavier.

L'application autorise l'utilisation du clavier autorisé et bloque tout clavier qui n'a pas réussi l'autorisation.

Le module Protection BadUSB n'est pas installé par défaut. Si vous avez besoin du module Protection BadUSB, vous pouvez l'ajouter dans les propriétés du [paquet d'installation](#) avant d'installer l'application ou [modifier la sélection des modules de l'application](#) après avoir installé l'application.



Autorisation de clavier

Activation et désactivation de la Protection BadUSB

Les appareils USB définis par le système d'exploitation comme des claviers et connectés à l'ordinateur avant l'installation du module Protection BadUSB sont considérés comme autorisés après son installation.

Pour activer ou désactiver le module Protection BadUSB, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale contre les menaces** → **Protection BadUSB**.

3. Utilisez le commutateur **Protection BadUSB** pour activer ou désactiver le module.


4. Enregistrez vos modifications.

Par conséquent, si la protection BadUSB est activée, Kaspersky Endpoint Security exige l'autorisation d'un appareil USB connecté identifié comme un clavier par le système d'exploitation. L'utilisateur ne peut pas utiliser un clavier que si ce dernier a été autorisé.

Utilisation d'un clavier virtuel pour l'autorisation des appareils USB

La possibilité d'utiliser le clavier virtuel existe uniquement pour l'autorisation des appareils USB qui ne prennent pas en charge la saisie de caractères (par exemple, un lecteur de code-barres). Il est déconseillé d'utiliser le clavier virtuel pour autoriser des appareils USB que vous ne connaissez pas.

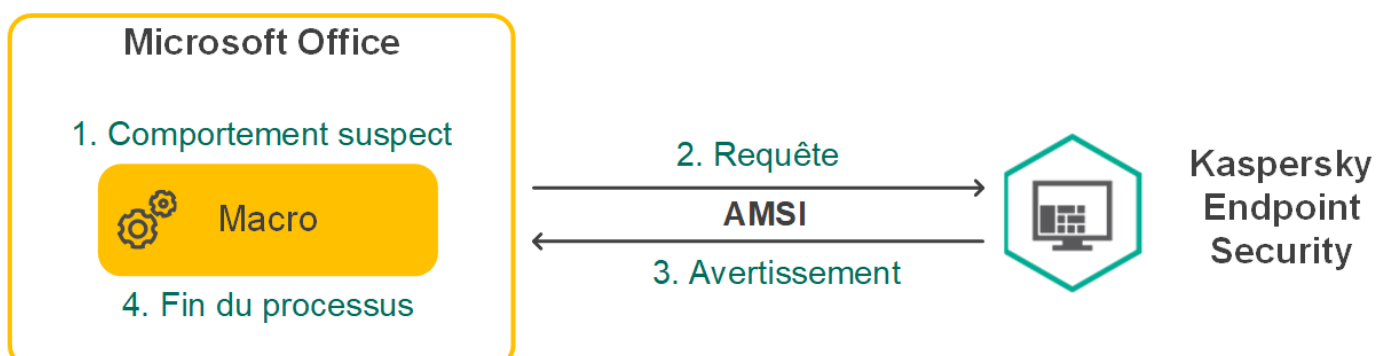
Pour autoriser ou interdire l'utilisation du clavier virtuel pour l'autorisation, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale contre les menaces** → **Protection BadUSB**.
3. Utilisez la case **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB** pour interdire ou autoriser l'utilisation du clavier virtuel pour l'autorisation.
4. Enregistrez vos modifications.

Protection AMSI

Le module de la protection AMSI est prévu pour la prise en charge de l'interface Antimalware Scan Interface de Microsoft. L'interface AMSI (*Antimalware Scan Interface*) permet aux applications tierces compatibles avec AMSI d'envoyer des objets (par exemple, des scripts PowerShell) à Kaspersky Endpoint Security pour une analyse supplémentaire et de recevoir les résultats de l'analyse de ces objets. Les applications tierces peuvent être, par exemple, des applications Microsoft Office (cf. ill. ci-dessous). Pour en savoir plus sur l'interface AMSI, consultez la [documentation de Microsoft](#).

La protection AMSI peut uniquement détecter une menace et la signaler à une application tierce. Après la réception de la notification sur la menace, l'application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt le fonctionnement).



Le module de la protection AMSI peut rejeter la demande d'une application tierce, par exemple, si cette application a dépassé le nombre maximum de demandes pour l'intervalle défini. Kaspersky Endpoint Security envoie les informations relatives au rejet de la demande de l'application tierce au Serveur d'administration. Le module de la protection AMSI ne rejette pas les demandes des applications tierces pour lesquelles la [case Ne pas bloquer l'interaction avec le fournisseur de protection AMSI](#) a été cochée


La protection AMSI est disponible pour les systèmes d'exploitation suivants pour postes de travail et serveurs :

- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise ;
- Windows Server 2016 Essentials/Standard/Datacenter ;
- Windows Server 2019 Essentials/Standard/Datacenter.

Activation et désactivation de la protection AMSI

La protection AMSI est activée par défaut.


Pour activer ou désactiver la protection AMSI, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection AMSI**.
3. Utilisez le commutateur **Protection AMSI** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Utilisation de la protection AMSI pour analyser les fichiers composés

L'insertion de virus dans des fichiers composés tels que des archives est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulée de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter la sélection de types de fichiers composés à analyser pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés par la protection AMSI, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection principale** → **Protection AMSI**.
3. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets de distribution ou fichiers au format Office.
4. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

- Pour empêcher que le module de la protection AMSI ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**. Le module de la protection AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.
- Pour autoriser le module de la protection AMSI à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

Le module de la protection AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

5. Enregistrez vos modifications.

Protection contre les Exploits


Le module Protection contre les Exploits surveille le code qui exploite les vulnérabilités d'un ordinateur pour obtenir des privilèges d'administrateur ou effectuer des actions malveillantes de la part de l'exploit. Les exploits, par exemple, utilisent l'attaque par débordement de tampon. Dans ce cas, l'exploit envoie un gros volume de données à l'application vulnérable. Lors du traitement de ces données, l'application vulnérable exécute un code malveillant. Suite à cette attaque, un exploit pourrait lancer l'installation non autorisée d'une application malveillante.

S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier ou le signale à l'utilisateur.

Activation et désactivation de la Protection contre les Exploits

Par défaut, la Protection contre les Exploits est activée et fonctionne dans le mode recommandé par les experts de Kaspersky. Vous pouvez désactiver la Protection contre les Exploits le cas échéant.

Pour activer ou désactiver la Protection contre les exploits, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Protection contre les Exploits**.
3. Utilisez le commutateur **Protection contre les Exploits** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si la protection contre les exploits est activée, Kaspersky Endpoint Security surveillera les fichiers exécutables qui sont exécutés par des applications vulnérables. Si Kaspersky Endpoint Security détecte qu'un fichier exécutable d'une application vulnérable n'a pas été lancé par l'utilisateur, il exécute l'action sélectionnée (par exemple, il interdit l'opération).

Sélection de l'action à exécuter en cas de détection d'un exploit

Par défaut, quand Kaspersky Endpoint Security détecte un exploit, il en bloque les opérations.


Pour choisir l'action à exécuter en cas de détection d'un exploit, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Protection contre les Exploits**.
3. Sélectionnez l'action appropriée dans le groupe **En cas de détection d'un exploit** :
 - **Bloquer l'opération**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après la détection d'un exploit, bloque l'opération de ce code d'exploitation et crée dans le journal une entrée qui reprend des informations relatives à ce code d'exploitation.
 - **Notifier**. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert un exploit, crée une entrée dans le journal qui reprend les informations relatives à l'exploit et ajoute les informations relatives à l'exploit dans la liste des menaces actives.
4. Enregistrez vos modifications.

Protection de la mémoire des processus système

La protection de la mémoire des processus système est activée par défaut.

Pour activer ou désactiver la protection de la mémoire des processus système, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Protection contre les Exploits**.
3. Utilisez le commutateur **Activer la protection de la mémoire des processus système** pour activer ou désactiver cette fonctionnalité.
4. Enregistrez vos modifications.

Par conséquent, Kaspersky Endpoint Security interdira les processus externes qui tentent d'accéder aux processus système.

Détection comportementale

Le module Détection comportementale récupère des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent intervenir avec plus d'efficacité.


Le module Détection comportementale utilise des modèles de comportement d'applications dangereux. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Endpoint Security exécute la réaction choisie. La fonction de Kaspersky Endpoint Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

Activation et désactivation de la Détection comportementale

Par défaut, la Détection comportementale est activée et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver la Détection comportementale.

Il est déconseillé de désactiver la Détection comportementale sans nécessité car cela réduit l'efficacité des modules de la protection. Les modules de la protection peuvent solliciter des informations récupérées par la Détection comportementale pour détecter les menaces.


Pour activer ou désactiver la Détection comportementale, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Détection comportementale**.
3. Utilisez le commutateur **Détection comportementale** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si la détection de comportement est activée, Kaspersky Endpoint Security utilisera les modèles de comportement dangereux pour analyser l'activité des applications dans le système d'exploitation.

Sélection de l'action à exécuter en cas de détection d'une activité malveillante d'une application

Pour choisir l'action à exécuter en cas de détection de l'activité malveillante d'une application, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Détection comportementale**.
3. Sélectionnez l'action appropriée dans le groupe **En cas de détection de l'activité d'une application malveillante** :
 - **Supprimer le fichier.** Si cet élément est sélectionné, Kaspersky Endpoint Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application.
 - **Interrompre l'application.** Si cet élément est sélectionné, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.
 - **Notifier.** Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.
4. Enregistrez vos modifications.

Protection des dossiers partagés contre le chiffrement externe

Le module assure le suivi des opérations uniquement pour les fichiers qui se trouvent sur des appareils de stockage de masse avec système de fichiers NTFS et qui ne sont pas chiffrés par le système EFS.

La fonction de protection des dossiers partagés contre le chiffrement externe garantit l'analyse de l'activité dans les dossiers partagés. Si l'activité correspond à un modèle de comportement dangereux caractéristique du chiffrement externe, Kaspersky Endpoint Security exécute l'action choisie.


La protection des dossiers partagés contre le chiffrement externe est désactivée par défaut.

Après l'installation de Kaspersky Endpoint Security, la fonction de protection des dossiers partagés contre le chiffrement externe est limitée avant le redémarrage de l'ordinateur.

Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe


Après l'installation de Kaspersky Endpoint Security, la fonction de protection des dossiers partagés contre le chiffrement externe est limitée avant le redémarrage de l'ordinateur.

Pour activer ou désactiver la protection des dossiers partagés contre le chiffrement externe, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Détection comportementale**.
3. Utilisez le commutateur **Activer la protection des dossiers partagés contre le chiffrement externe** pour activer ou désactiver la détection d'une activité caractéristique du chiffrement externe.
4. Enregistrez vos modifications.

Sélection de l'action à exécuter en cas de détection du chiffrement externe de dossiers partagés

Pour choisir l'action à exécuter en cas de détection du chiffrement externe de dossiers partagés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Détection comportementale**.
3. Sélectionnez l'action appropriée dans le groupe **Protection des dossiers partagés contre le chiffrement externe** :

- **Bloquer la connexion pendant X minutes.** Si cette option est sélectionnée, Kaspersky Endpoint Security réalise les opérations suivantes en cas de détection d'une tentative de modification de fichiers dans des dossiers partagés :
 - bloque l'activité réseau de l'ordinateur à l'origine de la modification ;
 - crée des copies de sauvegarde des fichiers modifiés ;
 - ajoute un enregistrement aux [rapports de l'interface locale de l'application](#) ;
 - envoie des informations sur la détection d'une 'activité malveillante à Kaspersky Security Center.

Si le module Réparation des actions malicieuses est activé, l'application restaure les fichiers modifiés au départ des copies de sauvegarde.

- **Notifier.** Si cette option est sélectionnée, Kaspersky Endpoint Security réalise les opérations suivantes en cas de détection d'une tentative de modification de fichiers dans des dossiers partagés :
 - ajoute un enregistrement aux [rapports de l'interface locale de l'application](#) ;
 - ajoute une entrée à la liste des menaces actives ;
 - envoie des informations sur la détection d'une 'activité malveillante à Kaspersky Security Center.

4. Enregistrez vos modifications.

Création d'une exclusion pour la protection des dossiers partagés contre le chiffrement externe

L'exclusion d'un dossier peut réduire le nombre de faux positifs si votre entreprise utilise le chiffrement des données lors de l'échange de fichiers à l'aide de dossiers partagés. Par exemple, la Détection comportementale peut générer des faux positifs lorsque l'utilisateur traite des fichiers portant l'extension ENC dans un dossier partagé. Une telle activité correspond à un modèle comportemental typique de chiffrement externe. Si vous avez chiffré des fichiers dans un dossier partagé pour protéger des données, ajoutez ce dossier aux exclusions.

[Comment créer une exclusion pour la protection des dossiers partagés à l'aide de la Console d'administration \(MMC\) ?](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions**.
6. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Exclusions de l'analyse**.
Une fenêtre reprenant la liste des exclusions s'ouvre.
8. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.
9. Cochez la case **Autoriser l'utilisation des applications de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les fichiers figurant dans la liste.
10. Cliquez sur le bouton **Ajouter**.
11. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.
12. Le lien **sélectionnez le fichier ou le dossier** situé dans le groupe **Description de l'exclusion de l'analyse (cliquez sur les éléments soulignés pour les modifier)** permet d'ouvrir la fenêtre **Nom du fichier ou du dossier**.
13. Cliquez sur **Parcourir** et sélectionnez le dossier partagé.

Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les caractères * et ? lors de la saisie d'un masque :

- Le caractère ***** remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque **C:**.txt** inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
- Deux caractères ***** qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque **C:\Dossier***.txt** inclura tous les chemins d'accès aux fichiers avec l'extension TXT

situés dans le dossier joint nommé **Dossier**, sauf pour le **Dossier** lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:***.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé **Dossier** qui ont l'extension TXT et un nom composé de trois caractères.

14. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

15. Cliquez sur le lien **quelconque** situé dans le groupe **Description de l'exclusion de l'analyse (cliquez sur les éléments soulignés pour les modifier)** pour activer le lien **sélectionnez les modules**.

16. Cliquez sur le lien **sélectionnez les modules** pour ouvrir la fenêtre **Modules de la protection**.

17. Cochez la case située à côté du module **Détection comportementale**.

18. Enregistrez vos modifications.

[Comment créer une exclusion pour la protection des dossiers partagés à l'aide de Web Console et de Cloud Console ?](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez **Paramètres généraux** → **Exclusions**.
5. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le lien **Exclusions de l'analyse**.
6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.
7. Cochez la case **Autoriser l'utilisation des applications de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les fichiers figurant dans la liste.


8. Cliquez sur le bouton **Ajouter**.
9. Sélectionnez la manière dont vous souhaitez ajouter l'exclusion : **Fichier ou dossier**.
10. Cliquez sur **Parcourir** et sélectionnez le dossier partagé.

Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les caractères * et ? lors de la saisie d'un masque :

- Le caractère * remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:**.txt inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
- Deux caractères * qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier***.txt inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé Dossier, sauf pour le Dossier lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque C:***.txt n'est pas un masque valide.
- Le caractère ? remplace n'importe quel caractère unique, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier\???.txt inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé Dossier qui ont l'extension TXT et un nom composé de trois caractères.

11. Dans le groupe **Modules de la protection**, sélectionnez le module **Détection comportementale**.
12. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.
13. Sélectionnez l'état **Actif** pour l'exclusion.
Vous pouvez utiliser le commutateur pour [mettre fin à une exclusion](#) à tout moment.
14. Enregistrez vos modifications.

[Comment créer une exclusion pour la protection des dossiers partagés dans l'interface de l'application ?](#)


1. Dans la fenêtre principale de l'application, cliquez sur le bouton .
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Menaces et exclusions**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.
4. Cliquez sur le bouton **Ajouter**.
5. Cliquez sur **Parcourir** et sélectionnez le dossier partagé.
Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les caractères * et ? lors de la saisie d'un masque :
 - Le caractère * remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:**.txt inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
 - Deux caractères * qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier***.txt inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé Dossier, sauf pour le Dossier lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque C:***.txt n'est pas un masque valide.
 - Le caractère ? remplace n'importe quel caractère unique, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier\???.txt inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé Dossier qui ont l'extension TXT et un nom composé de trois caractères.
6. Dans le groupe **Modules de la protection**, sélectionnez le module **Détection comportementale**.
7. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.
8. Sélectionnez l'état **Actif** pour l'exclusion.
Vous pouvez utiliser le commutateur pour [mettre fin à une exclusion](#) à tout moment.
9. Enregistrez vos modifications.

Configuration des adresses des exclusions de la protection des dossiers partagés contre le chiffrement externe

Pour pouvoir profiter de la fonction d'exclusion des adresses de la protection des dossiers partagés contre le chiffrement externe, il faut activer le service d'Audit de l'accès au système. Ce service est désactivé par défaut (pour en savoir plus sur l'activation du service d'audit de l'accès au système, consultez le site de Microsoft).

La fonction des exclusions des adresses de la protection des dossiers partagés n'est pas disponible sur un ordinateur distant si celui-ci a été allumé avant le lancement de Kaspersky Endpoint Security. Vous pouvez redémarrer cet ordinateur distant après le lancement de Kaspersky Endpoint Security pour garantir le fonctionnement de l'exclusion des adresses de la protection des dossiers partagés sur cet ordinateur distant.

Pour exclure de la protection des ordinateurs distants qui réalisent le chiffrement externe des dossiers partagés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Détection comportementale**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Configuration des adresses d'exclusions**.
4. Si vous voulez ajouter l'adresse IP ou le nom de l'ordinateur à la liste des exclusions, cliquez sur le bouton **Ajouter**.
5. Saisissez l'adresse IP ou le nom de l'ordinateur pour lequel les tentatives de chiffrement externe ne doivent pas être traitées.
6. Enregistrez vos modifications.

Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe

Vous pouvez exporter la liste des exclusions dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions ou pour procéder à la migration de la liste vers un autre serveur.

[Comment exporter et importer une liste d'exclusions dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Détection comportementale**.
6. Dans le groupe **Protection des dossiers partagés contre le chiffrement externe**, cliquez sur le bouton **Exclusions**.
7. Pour exporter la liste des règles, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune exclusion, Kaspersky Endpoint Security exportera toutes les exclusions.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
8. Pour importer la liste des exclusions, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
9. Enregistrez vos modifications.

[Comment exporter et importer une liste d'exclusions dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste d'exclusions.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection avancée** → **Détection comportementale**.
5. Pour exporter la liste des exclusions dans le groupe **Exclusions**, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.
 - d. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - e. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
6. Pour importer la liste des exclusions dans le groupe **Exclusions**, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
7. Enregistrez vos modifications.

Prévention des intrusions

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le module Prévention des intrusions (en anglais, HIPS – Host Intrusion Prevention System) empêche l'exécution des actions dangereuses pour le système et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles. Le module assure la protection de l'ordinateur à l'aide de bases antivirus et du service cloud Kaspersky Security Network.

Le module contrôle le fonctionnement des applications à l'aide des *privileges des applications*. Les privileges des applications incluent les paramètres d'accès suivants :

- l'accès aux ressources du système d'exploitation (par exemple, les options de démarrage automatique, les clés de registre) ;
- l'accès aux données personnelles (par exemple, les fichiers, les applications).

L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.

Lors du premier lancement de l'application, le module Prévention des intrusions exécute les actions suivantes :

1. Il vérifie la sécurité de l'application à l'aide des bases antivirus chargées.
2. Il vérifie la sécurité de l'application dans Kaspersky Security Network.

Pour contribuer au fonctionnement plus efficace du module Prévention des intrusions, il est conseillé de [participer au Kaspersky Security Network](#).

3. Il place l'application dans un des *groupes de confiance* : de confiance, restrictions faibles, restrictions élevées, douteuses.

Le [groupe de confiance définit les privileges](#) que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications. Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction du niveau de danger que cette application peut représenter pour l'ordinateur.

Kaspersky Endpoint Security place l'application dans un groupe de confiance pour les modules Pare-feu et Prévention des intrusions. Vous ne pouvez pas modifier le groupe de confiance uniquement pour le Pare-feu ou la Prévention des intrusions.

Si vous avez refusé de participer au KSN ou s'il n'y a pas de réseau, Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction des [paramètres du module Prévention des intrusions](#). Après la récupération des données sur la réputation de l'application dans KSN, le groupe de confiance peut être modifié automatiquement.

4. Il bloque les actions de l'application en fonction du groupe de confiance. Par exemple, les applications du groupe de confiance Restrictions élevées n'ont pas accès aux modules du système d'exploitation.

Lors du prochain démarrage de l'application, Kaspersky Endpoint Security vérifie l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les privileges des applications existants. En cas de modification de l'application, Kaspersky Endpoint Security l'analyse comme s'il s'agissait de sa première exécution.

Activation et désactivation de la Prévention des intrusions

Par défaut, le module Prévention des intrusions est activé et fonctionne dans le mode recommandé par les experts de Kaspersky.


[Procédure d'activation ou de désactivation du module Prévention des intrusions dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Utilisez la case **Prévention des intrusions** pour activer ou désactiver le module.
7. Enregistrez vos modifications.

[Procédure d'activation ou de désactivation du module Prévention des intrusions dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Utilisez le commutateur **Prévention des intrusions** pour activer ou désactiver le module.
6. Enregistrez vos modifications.

[Procédure d'activation ou de désactivation du module Prévention des intrusions dans l'interface de l'application](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Utilisez le commutateur **Prévention des intrusions** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Si le module Prévention des intrusions est activé, Kaspersky Endpoint Security placera l'application dans un [groupe de confiance](#) en fonction du niveau de danger que cette application peut représenter pour l'ordinateur. Kaspersky Endpoint Security bloquera alors les actions de l'application en fonction du groupe de confiance.

Utilisation des groupes de confiance d'applications

Au premier lancement de chaque l'application, le module Prévention des intrusions vérifie le niveau de danger de l'application et la place dans un des [groupes de confiance](#).

À la première étape de l'analyse de l'application, Kaspersky Endpoint Security cherche l'enregistrement sur l'application dans la base interne des applications connues et envoie simultanément une demande à la base de Kaspersky Security Network (s'il existe une connexion à Internet). L'application est placée dans un groupe de confiance sur la base des résultats de l'analyse selon la base interne et selon la base de Kaspersky Security Network. À chaque lancement de l'application, Kaspersky Endpoint Security envoie une nouvelle demande à la base KSN et déplace l'application dans un autre groupe de confiance si la réputation de l'application dans la base KSN a changé.

Vous pouvez choisir un groupe de confiance dans lequel Kaspersky Endpoint Security doit [placer automatiquement les applications inconnues](#). Les applications, lancées avant Kaspersky Endpoint Security, sont placées automatiquement dans le groupe de confiance défini dans la fenêtre [Paramètres du module Prévention des intrusions](#).

S'agissant des applications lancées avant Kaspersky Endpoint Security, le contrôle porte uniquement sur leur activité réseau. Le contrôle s'opère selon les règles réseau [définies dans les paramètres du pare-feu](#).

Modifier le groupe de confiance d'une application

Au premier lancement de chaque l'application, le module Prévention des intrusions vérifie le niveau de danger de l'application et la place dans un des [groupes de confiance](#).

Les experts de Kaspersky déconseillent de déplacer les applications du groupe de confiance défini automatiquement dans un autre groupe de confiance. Au lieu de cela, modifiez le cas échéant les [privilèges de l'application en question](#).


[Procédure de modification du groupe de confiance d'une application dans la Console d'administration \(MMC\)](#) 


1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Privilèges des applications**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
7. Choisissez l'onglet **Privilèges des applications**.
8. Cliquez sur le bouton **Ajouter**.
9. Dans la fenêtre qui s'ouvre, entrez les critères de recherche de l'application dont vous souhaitez modifier le groupe de confiance.
Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères ***** et **?** lors de la saisie d'un masque.
10. Cliquez sur le bouton **Actualiser**.
Kaspersky Endpoint Security recherchera l'application dans la liste consolidée des applications installées sur les ordinateurs administrés. Kaspersky Endpoint Security affichera une liste d'applications qui répondent à vos critères de recherche.
11. Sélectionnez l'application requise.
12. Dans la liste déroulante **Ajouter les applications sélectionnées au groupe <groupe de confiance>**, sélectionnez le groupe de confiance nécessaire pour l'application.
13. Enregistrez vos modifications.

[Procédure de modification du groupe de confiance d'une application dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Droits des applications et ressources protégées**, cliquez sur le lien **Droits des applications et ressources protégées**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
6. Choisissez l'onglet **Privilèges des applications**.
Vous verrez une liste des groupes de confiance sur le côté gauche de la fenêtre et leurs propriétés sur le côté droit.
7. Cliquez sur le bouton **Ajouter**.
Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.
8. Cliquez sur le lien **Groupe cible sélectionné** pour sélectionner le groupe de confiance approprié pour l'application.
9. Sélectionnez le type d'**application**. Cliquez sur le bouton **Suivant**.
Si vous souhaitez modifier le groupe de confiance pour plusieurs applications, sélectionnez le type de **groupe** et définissez un nom pour le groupe d'application.
10. Dans la liste ouverte des applications, sélectionnez les applications dont vous souhaitez modifier le groupe de confiance.
Utilisez un filtre. Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères ***** et **?** lors de la saisie d'un masque.
11. Quittez l'Assistant en cliquant sur **OK**.
L'application sera ajoutée au groupe de confiance.
12. Enregistrez vos modifications.

[Procédure de modification du groupe de confiance d'une application dans l'interface de l'application](#) 

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Cliquez sur le bouton **Gestion des applications**.
Cette action permet d'ouvrir la liste des applications installées.
4. Sélectionnez l'application requise.
5. Dans le menu contextuel de l'application, sélectionnez l'option **Restrictions** → <γρουπε δε χονφιανχε>.
6. Enregistrez vos modifications.

Par conséquent, l'application sera placée dans l'autre groupe de confiance. Kaspersky Endpoint Security bloquera alors les actions de l'application en fonction du groupe de confiance. L'état  (*user-defined*) sera attribué à l'application. Si la réputation de l'application est modifiée dans Kaspersky Security Network, le module Prévention des intrusions laissera le groupe de confiance de cette application inchangé.

Configuration des privilèges des groupes de confiance

Les [privilèges d'application optimaux](#) sont créés par défaut pour différents groupes de confiance. Les paramètres des privilèges de groupes d'applications qui font partie du groupe de confiance héritent des valeurs des paramètres des privilèges des groupes de confiance.


[Modification des privilèges des groupes de confiance dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
 2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
 3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
 4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
 5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
 6. Dans le groupe **Privilèges des applications**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
 7. Choisissez l'onglet **Privilèges des applications**.
 8. Sélectionnez le groupe de confiance requis.
 9. Sélectionnez l'option **Privilèges des groupes** dans le menu contextuel du groupe de confiance.
Cette action ouvre les propriétés du groupe de confiance.
 10. Exécutez une des actions suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez l'onglet **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez l'onglet **Privilèges**.
- L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.
11. Pour la ressource concernée, dans la colonne de l'action correspondante, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (✓) ou **Interdire** (⊘).
 12. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (✓ / ⊘).
Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.
 13. Enregistrez vos modifications.

[Modification des privilèges des groupes de confiance dans Web Console et Cloud Console](#)


1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
 2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
 3. Choisissez l'onglet **Paramètres des applications**.
 4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
 5. Dans le groupe **Droits des applications et ressources protégées**, cliquez sur le lien **Droits des applications et ressources protégées**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
 6. Choisissez l'onglet **Privilèges des applications**.
Vous verrez une liste des groupes de confiance sur le côté gauche de la fenêtre et leurs propriétés sur le côté droit.
 7. Dans la partie gauche de la fenêtre, sélectionnez le groupe de confiance concerné.
 8. Dans la partie droite de la fenêtre, dans la liste déroulante, réalisez une des opérations suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez **Privilèges**.
- L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.
9. Pour la ressource concernée, dans la colonne de l'action correspondante, sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (✓) ou **Interdire** (✗).
 10. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (✓/✗).
Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.
 11. Enregistrez vos modifications.

[Modification des privilèges des groupes de confiance dans l'interface de l'application](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Cliquez sur le bouton **Gestion des applications**.
Cette action permet d'ouvrir la liste des applications installées.
4. Sélectionnez le groupe de confiance requis.
5. Dans le menu contextuel du groupe de confiance, sélectionnez l'option **Détails et règles**.
Cette action ouvre les propriétés du groupe de confiance.
6. Exécutez une des actions suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez l'onglet **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez l'onglet **Privilèges**.

L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.

7. Pour la ressource concernée, dans la colonne de l'action correspondante, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (🔒) ou **Interdire** (🚫).
8. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (📄).
Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.
9. Enregistrez vos modifications.

Les privilèges du groupe de confiance seront modifiés. Kaspersky Endpoint Security bloquera alors les actions de l'application en fonction du groupe de confiance. L'état  (*Paramètres utilisateur*) sera attribué au groupe de confiance.

Sélection du groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security

S'agissant des applications lancées avant Kaspersky Endpoint Security, le contrôle porte uniquement sur leur activité réseau. Le contrôle s'opère selon les [règles réseau](#) définies dans les paramètres du pare-feu. Pour désigner les règles réseau qui doivent régir le contrôle de l'activité réseau de ces applications, il faut choisir un groupe de confiance.


Sélection d'un groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Privilèges des applications**, cliquez sur le bouton **Modifier**.
7. Sélectionnez le [groupe de confiance](#) nécessaire pour le paramètre **Les applications lancées avant Kaspersky Endpoint Security for Windows sont automatiquement placées dans le groupe de confiance <groupe de confiance>**.
8. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Sélectionnez le [groupe de confiance](#) nécessaire pour le paramètre **Les applications lancées avant Kaspersky Endpoint Security for Windows sont automatiquement placées dans le groupe de confiance <groupe de confiance>**.
6. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security dans l'interface de l'application

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Sélectionnez le [groupe de confiance](#) nécessaire dans le groupe **Les applications lancées avant Kaspersky Endpoint Security for Windows sont automatiquement placées dans le groupe de confiance <groupe de confiance>**.
4. Enregistrez vos modifications.

Par conséquent, une application qui est lancée avant Kaspersky Endpoint Security sera placée dans l'autre groupe de confiance. Kaspersky Endpoint Security bloquera alors les actions de l'application en fonction du groupe de confiance.

Sélection d'un groupe de confiance pour les applications inconnues

Lors du premier démarrage d'une application, le module Prévention des intrusions détermine le [groupe de confiance](#) pour l'application. Si vous n'avez pas accès Internet ou si Kaspersky Security Network ne dispose d'aucune information à propos de cette application, Kaspersky Endpoint Security placera l'application dans le groupe Restrictions faibles par défaut. Lorsque des informations à propos d'une application précédemment inconnue sont détectées dans KSN, Kaspersky Endpoint Security met à jour les privilèges de cette application. Ensuite, vous pourrez [modifier manuellement les privilèges de l'application](#).

[Sélection d'un groupe de confiance pour des applications inconnues dans la Console d'administration \(MMC\)](#)


1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Règles de traitement des applications**, utilisez la liste déroulante **Groupe de confiance pour les applications qui n'ont pas pu être attribuées à d'autres groupes** pour sélectionner le groupe de confiance souhaité.

Si la participation à [Kaspersky Security Network est activée](#), Kaspersky Endpoint Security envoie une demande à propos de la réputation de l'application à KSN à chaque lancement de l'application. En fonction de la réponse reçue, l'application peut être déplacée dans un groupe de confiance différent de celui désigné dans les paramètres du module Prévention des intrusions.
7. Utilisez la case **Mettre à jour les droits pour les applications précédemment inconnues de la base de données KSN** pour configurer la mise à jour automatique des privilèges des applications inconnues.
8. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour des applications inconnues dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Règles de traitement des applications**, utilisez la liste déroulante **Groupe de confiance pour les applications qui n'ont pas pu être attribuées à d'autres groupes** pour sélectionner le groupe de confiance souhaité.
Si la participation à [Kaspersky Security Network est activée](#), Kaspersky Endpoint Security envoie une demande à propos de la réputation de l'application à KSN à chaque lancement de l'application. En fonction de la réponse reçue, l'application peut être déplacée dans un groupe de confiance différent de celui désigné dans les paramètres du module Prévention des intrusions.
6. Utilisez la case **Mettre à jour les droits pour les applications précédemment inconnues de la base de données KSN** pour configurer la mise à jour automatique des privilèges des applications inconnues.
7. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour des applications inconnues dans l'interface de l'application

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Dans le groupe **Groupe de confiance pour les applications inconnues**, sélectionnez le groupe de confiance approprié.
Si la participation à [Kaspersky Security Network est activée](#), Kaspersky Endpoint Security envoie une demande à propos de la réputation de l'application à KSN à chaque lancement de l'application. En fonction de la réponse reçue, l'application peut être déplacée dans un groupe de confiance différent de celui désigné dans les paramètres du module Prévention des intrusions.
4. Utilisez la case **Mettre à jour les droits pour les applications précédemment inconnues de la base de données KSN** pour configurer la mise à jour automatique des privilèges des applications inconnues.
5. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour les applications dotées d'une signature numérique

Kaspersky Endpoint Security place toujours les applications signées par des certificats Microsoft ou des certificats Kaspersky dans le groupe "De confiance".

Comment sélectionner un groupe de confiance pour les applications dotées d'une signature numérique dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Règles de traitement des applications**, cochez la case **Faire confiance aux applications dotées d'une signature numérique** pour activer ou désactiver l'attribution automatique au groupe de confiance pour les applications contenant la signature numérique d'un éditeur de confiance.

Les *éditeurs de confiance* sont les éditeurs d'applications qui sont inclus par Kaspersky dans le groupe de confiance. Vous pouvez également [ajouter manuellement le certificat de l'éditeur au stockage système sécurisé des certificats](#).

Si la case est décochée, le module Prévention des intrusions ne considère pas les applications dotées d'une signature numérique comme des applications de confiance et détermine leur [groupe de confiance](#) sur la base d'autres paramètres.
7. Enregistrez vos modifications.


Sélection d'un groupe de confiance pour les applications dotées d'une signature numérique dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Règles de traitement des applications**, cochez la case **Faire confiance aux applications dotées d'une signature numérique** pour activer ou désactiver l'attribution automatique au groupe de confiance pour les applications contenant la signature numérique d'un éditeur de confiance.

Les *éditeurs de confiance* sont les éditeurs d'applications qui sont inclus par Kaspersky dans le groupe de confiance. Vous pouvez également [ajouter manuellement le certificat de l'éditeur au stockage système sécurisé des certificats](#).

Si la case est décochée, le module Prévention des intrusions ne considère pas les applications dotées d'une signature numérique comme des applications de confiance et détermine leur [groupe de confiance](#) sur la base d'autres paramètres.
6. Enregistrez vos modifications.

Sélection d'un groupe de confiance pour les applications dotées d'une signature numérique dans l'interface de l'application

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.

3. Dans le groupe **Règles de traitement des applications**, cochez la case **Faire confiance aux applications dotées d'une signature numérique** pour activer ou désactiver l'attribution automatique au groupe de confiance pour les applications contenant la signature numérique d'un éditeur de confiance.

Les *éditeurs de confiance* sont les éditeurs d'applications qui sont inclus par Kaspersky dans le groupe de confiance. Vous pouvez également [ajouter manuellement le certificat de l'éditeur au stockage système sécurisé des certificats](#).

Si la case est décochée, le module Prévention des intrusions ne considère pas les applications dotées d'une signature numérique comme des applications de confiance et détermine leur [groupe de confiance](#) sur la base d'autres paramètres.

4. Enregistrez vos modifications.

Utilisation des privilèges des applications

Par défaut le contrôle de l'application est assuré par les privilèges des applications définis pour le [groupe de confiance](#) en particulier que Kaspersky Endpoint Security a attribué à l'application lors de son premier démarrage. Le cas échéant, vous pouvez [modifier les privilèges des applications pour tout le groupe de confiance](#), pour une application en particulier ou pour un groupe d'applications qui font partie du groupe de confiance.

Les privilèges des applications définis manuellement ont une priorité plus élevée que les privilèges des applications qui ont été définis pour un groupe de confiance. Autrement dit, si les privilèges des applications définis manuellement diffèrent des privilèges des applications définis pour un groupe de confiance, le module Prévention des intrusions contrôle l'activité des applications en fonction des privilèges des applications définis manuellement.

Les règles que vous créez pour les applications sont héritées par des applications enfants. Par exemple, si vous avez interdit toute activité réseau au programme cmd.exe, cette interdiction s'appliquera au programme notepad.exe s'il a été exécuté avec cmd.exe. Si une application est lancée indirectement par une autre application, mais n'est pas un enfant de l'application dont elle est issue, les règles ne sont pas héritées.

Modification des privilèges des applications dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Privilèges des applications**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
7. Choisissez l'onglet **Privilèges des applications**.
8. Cliquez sur le bouton **Ajouter**.
9. Dans la fenêtre qui s'ouvre, entrez les critères de recherche de l'application dont vous souhaitez modifier les privilèges.
Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères * et ? lors de la saisie d'un masque.
10. Cliquez sur le bouton **Actualiser**.
Kaspersky Endpoint Security recherchera l'application dans la liste consolidée des applications installées sur les ordinateurs administrés. Kaspersky Endpoint Security affichera une liste d'applications qui répondent à vos critères de recherche.
11. Sélectionnez l'application requise.
12. Dans la liste déroulante **Ajouter les applications sélectionnées au groupe <groupe de confiance>**, sélectionnez **Groupes par défaut**, puis cliquez sur **OK**.
L'application sera ajoutée au groupe par défaut.
13. Sélectionnez l'application concernée, puis sélectionnez **Privilèges des applications** dans le menu contextuel de l'application.
Les propriétés de l'application s'ouvrent.
14. Exécutez une des actions suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez l'onglet **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez l'onglet **Privilèges**.

L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.

15. Pour la ressource concernée, dans la colonne de l'action correspondante, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (✓) ou

Interdire (🚫).

16. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (✓ / 🚫).

Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.

17. Enregistrez vos modifications.

[Modification des privilèges des applications dans Web Console et Cloud Console](#) ?

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Droits des applications et ressources protégées**, cliquez sur le lien **Droits des applications et ressources protégées**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
6. Choisissez l'onglet **Privilèges des applications**.
Vous verrez une liste des groupes de confiance sur le côté gauche de la fenêtre et leurs propriétés sur le côté droit.
7. Cliquez sur le bouton **Ajouter**.
Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.
8. Cliquez sur le lien **Groupe cible sélectionné** pour sélectionner le groupe de confiance approprié pour l'application.
9. Sélectionnez le type d'**application**. Cliquez sur le bouton **Suivant**.
Si vous souhaitez modifier le groupe de confiance pour plusieurs applications, sélectionnez le type de **groupe** et définissez un nom pour le groupe d'application.
10. Dans la liste ouverte des applications, sélectionnez les applications dont vous souhaitez modifier les privilèges.
Utilisez un filtre. Vous pouvez saisir le nom de l'application ou le nom du fournisseur. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
11. Quittez l'Assistant en cliquant sur **OK**.
L'application sera ajoutée au groupe de confiance.
12. Dans la partie gauche de la fenêtre, sélectionnez l'application concernée.
13. Dans la partie droite de la fenêtre, dans la liste déroulante, réalisez une des opérations suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez **Privilèges**.

L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.


14. Pour la ressource concernée, dans la colonne de l'action correspondante, sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (✔) ou **Interdire** (✘).

15. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (✔ / ✘).

Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.

16. Enregistrez vos modifications.

[Modification des privilèges des applications dans l'interface de l'application](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Cliquez sur le bouton **Gestion des applications**.
Cette action permet d'ouvrir la liste des applications installées.
4. Sélectionnez l'application requise.
5. Dans le menu contextuel de l'application, sélectionnez l'option **Détails et règles**.
Les propriétés de l'application s'ouvrent.
6. Exécutez une des actions suivantes :
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent les opérations avec le registre du système d'exploitation, les fichiers des utilisateurs et les paramètres des applications, sélectionnez l'onglet **Fichiers et base de registre**.
 - Si vous souhaitez modifier les privilèges des groupes de confiance qui réglementent l'accès aux processus et aux objets du système d'exploitation, sélectionnez l'onglet **Privilèges**.
7. Pour la ressource concernée, dans la colonne de l'action correspondante, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'option nécessaire : **Hériter**, **Autoriser** (🔓) ou **Interdire** (🔒).
8. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Écrire dans le rapport** (📄).
Kaspersky Endpoint Security enregistrera des informations concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.
9. Sélectionnez l'onglet **Exclusions** et configurez les paramètres avancés de l'application (cf. tableau ci-après).
10. Enregistrez vos modifications.

Paramètres avancés de l'application

| Paramètre | Description |
|--|---|
| Ne pas analyser les fichiers ouverts | Tous les fichiers qui sont ouverts par l'application sont exclus des analyses par Kaspersky Endpoint Security. Par exemple, si vous utilisez des applications pour effectuer des sauvegardes de fichiers, cette fonctionnalité permet de réduire la consommation de ressources par Kaspersky Endpoint Security. |
| Ne pas surveiller l'activité de l'application | Kaspersky Endpoint Security ne surveille pas l'activité des fichiers et du réseau de l'application dans le système d'exploitation. L'activité de l'application est contrôlée par les modules suivants : Détection comportementale , Protection contre les Exploits , Prévention des intrusions , Réparation des actions malicieuses et Pare-feu . |
| Ne pas hériter les restrictions du processus | Les restrictions configurées pour le processus parent ne seront pas appliquées par Kaspersky Endpoint Security à un processus enfant. Le processus parent est lancé par une application pour laquelle des droits d'application (Prévention des intrusions) et des règles réseau d'application (Pare-feu) sont configurés. |

| | |
|---|---|
| parent (application) | |
| Ne pas surveiller l'activité des applications enfants | Kaspersky Endpoint Security ne surveille pas l'activité des fichiers ni du réseau des applications qui sont lancées par cette application. |
| Autoriser l'interaction avec l'interface de Kaspersky Endpoint Security | Kaspersky Endpoint Security Self-Defense bloque toute tentative de gestion des services d'application à partir d'un ordinateur distant. Si la case est cochée, l'application d'accès à distance à l'ordinateur peut gérer les paramètres de Kaspersky Endpoint Security via l'interface de Kaspersky Endpoint Security. |
| Ne pas analyser le trafic chiffré/Ne pas analyser tout le trafic | Le trafic réseau amorcé par l'application sera exclu des analyses par Kaspersky Endpoint Security. Vous pouvez exclure des analyses l'ensemble du trafic ou seulement le trafic chiffré. Vous pouvez également exclure des analyses des adresses IP et des numéros de port individuels. |

Protection des ressources du système d'exploitation et des données personnelles

Le module Prévention des intrusions gère les privilèges des applications relatifs aux opérations sur différentes catégories de ressources du système d'exploitation et de données personnelles. Les experts de Kaspersky ont sélectionné des catégories de ressources à protéger. Par exemple, la catégorie *Système d'exploitation* comporte une sous-catégorie *Paramètres de démarrage* qui répertorie toutes les clés de registre associées à l'exécution automatique des applications. Vous ne pouvez pas modifier ou supprimer les catégories préinstallées de ressources à protéger et des ressources protégées connexes.



[Procédure d'ajout d'une ressource protégée dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Privilèges des applications**, cliquez sur le bouton **Paramètres**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
7. Sélectionnez l'onglet **Ressources protégées**.
Vous verrez une liste des ressources protégées dans la partie gauche de la fenêtre ainsi que les privilèges d'accès correspondants à ces ressources en fonction du groupe de confiance particulier.
8. Sélectionnez la catégorie de ressources protégées à laquelle vous souhaitez ajouter une nouvelle ressource protégée.
Si vous souhaitez ajouter une sous-catégorie, cliquez sur **Ajouter** → **Catégorie**.
9. Cliquez sur le bouton **Ajouter**. Dans la liste déroulante, sélectionnez le type de ressource que vous souhaitez ajouter : **Fichier ou dossier**, ou **Clé de registre**.
10. Dans la fenêtre qui s'ouvre, sélectionnez un fichier, un dossier ou une clé de registre.
Vous pouvez consulter les privilèges des applications pour accéder aux ressources ajoutées. Pour ce faire, sélectionnez une ressource ajoutée dans la partie gauche de la fenêtre, et Kaspersky Endpoint Security affichera les privilèges d'accès pour chaque groupe de confiance. Vous pouvez également désactiver le contrôle de l'activité des applications avec les ressources à l'aide de la case située à côté d'une nouvelle ressource.
11. Enregistrez vos modifications.

[Procédure d'ajout d'une ressource protégée dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Droits des applications et ressources protégées**, cliquez sur le lien **Droits des applications et ressources protégées**.
Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
6. Sélectionnez l'onglet **Ressources protégées**.
Vous verrez une liste des ressources protégées dans la partie gauche de la fenêtre ainsi que les privilèges d'accès correspondants à ces ressources en fonction du groupe de confiance particulier.
7. Cliquez sur le bouton **Ajouter**.
L'Assistant de nouvelles ressources démarre.
8. Cliquez sur le lien **Nom du groupe** pour sélectionner la catégorie de ressources protégées à laquelle vous souhaitez ajouter une nouvelle ressource protégée.
Si vous souhaitez ajouter une sous-catégorie, sélectionnez l'option **Catégorie de ressources protégées**.
9. Sélectionnez le type de ressource que vous souhaitez ajouter : **Fichier ou dossier**, ou **Clé de registre**.
10. Sélectionnez un fichier, un dossier ou une clé de registre.
11. Quittez l'Assistant en cliquant sur **OK**.
Vous pouvez consulter les privilèges des applications pour accéder aux ressources ajoutées. Pour ce faire, sélectionnez une ressource ajoutée dans la partie gauche de la fenêtre, et Kaspersky Endpoint Security affichera les privilèges d'accès pour chaque groupe de confiance. Vous pouvez également utiliser la case dans la colonne **État** pour désactiver le contrôle de l'activité des applications avec les ressources.
12. Enregistrez vos modifications.

[Procédure d'ajout d'une ressource protégée dans l'interface de l'application](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Cliquez sur le bouton **Administrer les ressources**.
La liste des ressources protégées s'ouvre.
4. Sélectionnez la catégorie de ressources protégées à laquelle vous souhaitez ajouter une nouvelle ressource protégée.
Si vous souhaitez ajouter une sous-catégorie, cliquez sur **Ajouter** → **Catégorie**.
5. Cliquez sur le bouton **Ajouter**. Dans la liste déroulante, sélectionnez le type de ressource que vous souhaitez ajouter : **Fichier ou dossier**, ou **Clé de registre**.
6. Dans la fenêtre qui s'ouvre, sélectionnez un fichier, un dossier ou une clé de registre.
Vous pouvez consulter les privilèges des applications pour accéder aux ressources ajoutées. Pour ce faire, sélectionnez une ressource ajoutée dans la partie gauche de la fenêtre, et Kaspersky Endpoint Security affichera une liste d'applications ainsi que les privilèges d'accès pour chaque application. Vous pouvez également désactiver le contrôle de l'activité des applications avec les ressources à l'aide du bouton  **Désactiver le contrôle** dans la colonne **État**.
7. Enregistrez vos modifications.

Kaspersky Endpoint Security contrôlera l'accès aux données à caractère personnel ainsi qu'aux ressources ajoutées au système d'exploitation. Kaspersky Endpoint Security contrôle l'accès d'une application aux ressources en fonction du groupe de confiance attribué à l'application. Vous pouvez également [modifier le groupe de confiance d'une application](#).

Suppression des informations sur les applications inutilisées

Kaspersky Endpoint Security surveille le fonctionnement des applications à l'aide des privilèges d'application. Les privilèges d'une application sont déterminés par un groupe de confiance. Kaspersky Endpoint Security place une application dans un [groupe de confiance](#) lorsque l'application est lancée pour la première fois. Vous pouvez [modifier manuellement le groupe de confiance de l'application](#). Vous pouvez également [configurer manuellement les privilèges d'une application distincte](#). Ainsi, Kaspersky Endpoint Security stocke les informations suivantes sur l'application : groupe de confiance et privilèges de l'application.

Kaspersky Endpoint Security supprime automatiquement les informations sur les applications non utilisées afin d'économiser les ressources de l'ordinateur. Kaspersky Endpoint Security supprime les informations relatives aux applications conformément aux règles suivantes :

- Si le groupe de confiance et les privilèges sont déterminés automatiquement, Kaspersky Endpoint Security supprime les informations relatives à cette application après 30 jours. Il n'est pas possible de modifier la durée de conservation des informations relatives à l'application ou de désactiver la suppression automatique.
- Si vous avez placé manuellement l'application dans un groupe de confiance ou configuré les droits d'accès, Kaspersky Endpoint Security supprime les informations relatives à cette application au bout de 60 jours (valeur par défaut). Vous pouvez modifier la durée de conservation des informations relatives à l'application ou désactiver la suppression automatique (cf. les instructions ci-dessous).

Lorsque vous lancez une application dont les informations ont été supprimées, Kaspersky Endpoint Security examine l'application comme au premier lancement.


[Configuration de la suppression automatique des informations relatives aux applications non utilisées dans la Console d'administration \(MMC\)](#) ²

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
6. Dans le groupe **Règles de traitement des applications**, exécutez une des actions suivantes :
 - Si vous souhaitez configurer la suppression automatique, cochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours** et indiquez le nombre de jours requis.
Kaspersky Endpoint Security supprimera à l'issue d'un délai défini les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime également au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
 - Si vous souhaitez désactiver la suppression automatique, décochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours**.
Kaspersky Endpoint Security conservera pendant une durée indéterminée les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime uniquement au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
7. Enregistrez vos modifications.

[Configuration de la suppression automatique des informations relatives aux applications non utilisées dans Web Console et Cloud Console](#) ²

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Prévention des intrusions**.
5. Dans le groupe **Règles de traitement des applications**, exécutez une des actions suivantes :
 - Si vous souhaitez configurer la suppression automatique, cochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours** et indiquez le nombre de jours requis.
Kaspersky Endpoint Security supprimera à l'issue d'un délai défini les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime également au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
 - Si vous souhaitez désactiver la suppression automatique, décochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours**.
Kaspersky Endpoint Security conservera pendant une durée indéterminée les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime uniquement au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
6. Enregistrez vos modifications.

[Configuration de la suppression automatique des informations relatives aux applications non utilisées dans l'interface de l'application](#) 

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Prévention des intrusions**.
3. Dans le groupe **Règles de traitement des applications**, exécutez une des actions suivantes :
 - Si vous souhaitez configurer la suppression automatique, cochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours** et indiquez le nombre de jours requis.

Kaspersky Endpoint Security supprimera à l'issue d'un délai défini les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime également au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
 - Si vous souhaitez désactiver la suppression automatique, décochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours**.

Kaspersky Endpoint Security conservera pendant une durée indéterminée les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime uniquement au bout de 30 jours les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.
4. Enregistrez vos modifications.

Surveillance du module Prévention des intrusions

Vous pouvez recevoir des rapports concernant le fonctionnement du module Prévention des intrusions. Les rapports contiennent des informations relatives aux opérations effectuées par l'application avec des ressources informatiques (autorisées ou interdites). Les rapports contiennent également des informations concernant les applications qui utilisent chaque ressource.

Pour surveiller le fonctionnement du module Prévention des intrusions, vous devez activer l'écriture dans les rapports. Par exemple, vous pouvez [activer la transmission de rapports pour des applications individuelles dans les paramètres du module Prévention des intrusions](#).

Lorsque vous configurez la surveillance du module Prévention des intrusions, tenez compte de la charge potentielle sur le réseau lorsque vous transmettez des événements à Kaspersky Security Center. Vous pouvez également activer l'enregistrement des rapports uniquement dans le journal local de Kaspersky Endpoint Security.

Protection de l'accès au flux audio et vidéo

Les cybercriminels peuvent utiliser des programmes spéciaux pour essayer d'accéder à des appareils qui enregistrent du son et de la vidéo (comme des microphones ou des webcams). Kaspersky Endpoint Security contrôle le moment où les applications reçoivent un flux audio ou un flux vidéo et protège les données contre toute interception non autorisée.

Par défaut, Kaspersky Endpoint Security contrôle l'accès des applications au flux audio et au flux vidéo en fonction de la catégorie de l'application :

- Les applications appartenant au groupe De confiance et Restrictions faibles sont autorisées par défaut à recevoir le flux audio et le flux vidéo des appareils.
- Les applications appartenant au groupe Restrictions élevées et Douteux ne sont pas autorisées par défaut à recevoir le flux audio et le flux vidéo des appareils.

Vous pouvez [autoriser manuellement des applications à recevoir le flux audio et le flux vidéo](#).

Les fonctionnalités particulières de la protection des flux audio

La fonction de protection du signal audio présente les caractéristiques spéciales suivantes :

- Pour que la fonction soit opérationnelle, le [module Prévention des intrusions doit être activé](#).
- Si l'application a commencé à recevoir le signal audio avant le lancement de la Prévention des intrusions, Kaspersky Endpoint Security permet à l'application de recevoir le signal audio et n'affiche aucune notification.
- Si vous avez placé l'application dans le groupe Douteux ou Restrictions élevées après que l'application a commencé à recevoir le signal audio, Kaspersky Endpoint Security permet à l'application de recevoir le signal audio et n'affiche aucune notification.
- En cas de modification des paramètres d'accès de l'application aux dispositifs d'enregistrement (par exemple, [la réception du signal audio par l'application a été interdite](#)), il faut relancer l'application afin qu'elle arrête de recevoir le signal audio.
- Le contrôle de la réception du signal audio depuis le dispositif d'enregistrement ne dépend pas des paramètres de l'accès des applications à la webcam.
- Kaspersky Endpoint Security protège uniquement l'accès aux microphones intégrés et externes. Les autres dispositifs de transmission du son ne sont pas pris en charge.
- Kaspersky Endpoint Security ne garantit pas la protection du signal audio transmis par des appareils comme les appareils photo reflex numériques, les caméras vidéo portables ou les caméras sportives.
- Au premier lancement de l'application Kaspersky Endpoint Security après son installation, la reproduction ou l'enregistrement audio ou vidéo peuvent être interrompus dans les applications de d'enregistrement ou de lecture audio et vidéo. Ceci est nécessaire pour activer la fonction du contrôle de l'accès des applications aux dispositifs d'enregistrement audio. Le service système d'administration des outils de manipulation du son sera redémarré au premier lancement de l'application Kaspersky Endpoint Security.

Les fonctionnalités particulières de la protection de l'accès aux webcams des applications

La fonction de protection de l'accès à la webcam possède les particularités et les restrictions suivantes :

- L'application contrôle les images dynamiques et statiques reçues à la suite du traitement des données de la webcam.
- L'application contrôle le signal audio afin de déterminer s'il appartient au flux vidéo de la webcam.
- L'application contrôle uniquement les webcams connectées via l'interface USB ou IEEE1394 et affichées dans le Gestionnaire d'appareils Windows comme **Appareil d'acquisition d'image** (Imaging Device).

- Kaspersky Endpoint Security est compatible avec les webcams suivantes :
 - Logitech HD Webcam C270 ;
 - Logitech HD Webcam C310 ;
 - Logitech Webcam C210 ;
 - Logitech Webcam Pro 9000 ;
 - Logitech HD Webcam C525 ;
 - Microsoft LifeCam VX-1000 ;
 - Microsoft LifeCam VX-2000 ;
 - Microsoft LifeCam VX-3000 ;
 - Microsoft LifeCam VX-800 ;
 - Microsoft LifeCam Cinema.

Kaspersky ne garantit pas la prise en charge des webcams qui ne figurent pas dans cette liste.

Réparation des actions malicieuses

Le module Réparation des actions malicieuses permet à Kaspersky Endpoint Security d'exécuter le retour à l'état antérieur aux actions des applications malveillantes dans le système d'exploitation.

Lors de la restauration des actions du programme malveillant dans le système d'exploitation, Kaspersky Endpoint Security traite les types suivants d'activité de programme malveillant :

- **Activité de fichiers**

Kaspersky Endpoint Security réalise les opérations suivantes :

- suppression des fichiers exécutables créés par l'application malveillante (sur tous les supports, sauf les disques réseau) ;
- suppression des fichiers exécutables créés par les applications dans lesquelles une application malveillante s'est introduite ;
- restauration des fichiers modifiés ou supprimés par l'application malveillante.

La fonction de restauration est soumise à une [série de restrictions](#).

- **Activité sur la base de registre**

Kaspersky Endpoint Security réalise les opérations suivantes :

- suppression des sections et des clés de registre créées par l'application malveillante ;
- non-restauration des sections et clés de registre modifiées ou supprimées par l'application malveillante.

- **Activité système**

Kaspersky Endpoint Security réalise les opérations suivantes :

- arrêt des processus lancés par l'application malveillante ;
 - arrêt des processus dans lesquels l'application malveillante s'est introduite ;
 - non-rétablissement des processus arrêtés par l'application malveillante.
- **Activité réseau**

Kaspersky Endpoint Security réalise les opérations suivantes :

- interdiction de l'activité réseau de l'application malveillante ;
- interdiction de l'activité réseau des processus dans lesquels l'application malveillante s'est introduite.

L'annulation des actions de l'application malveillante peut être lancée par le module [Protection contre les fichiers malicieux](#), [Détection comportementale](#) ou lors de la [recherche de virus](#).

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cela n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.


[Procédure d'activation ou de désactivation du module Réparation des actions malicieuses dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Protection avancée** → **Réparation des actions malicieuses**.
6. Utilisez la case **Réparation des actions malicieuses** pour activer ou désactiver le module.
7. Enregistrez vos modifications.

[Procédure d'activation ou de désactivation du module Réparation des actions malicieuses dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez la section **Protection avancée** → **Réparation des actions malicieuses**.
5. Utilisez le commutateur **Réparation des actions malicieuses** pour activer ou désactiver le module.
6. Enregistrez vos modifications.

Procédure d'activation ou de désactivation du module Réparation des actions malicieuses dans l'interface de l'application [?](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Réparation des actions malicieuses**.
3. Utilisez le commutateur **Réparation des actions malicieuses** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si la réparation des actions malicieuses est activée, Kaspersky Endpoint Security annulera les actions entreprises par les applications malveillantes dans le système d'exploitation.

Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau Kaspersky Security Network permet de récupérer ces données.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite. Si vous participez au Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la catégorie et la réputation des fichiers analysés, ainsi que sur la réputation des adresses Internet analysées.

L'utilisation de Kaspersky Security Network est volontaire. L'application propose d'utiliser le KSN pendant la configuration initiale de l'application. Vous pouvez commencer à utiliser le KSN ou arrêter de l'utiliser à n'importe quel moment.

Vous pouvez lire des informations plus détaillées sur l'envoi à Kaspersky, le stockage et la destruction des informations statistiques obtenues lors de l'utilisation de KSN dans la Déclaration de Kaspersky Security Network et sur le [site Internet de Kaspersky](#). Le fichier ksn_<ID de la langue>.txt qui contient la Déclaration de Kaspersky Security Network figure dans le [kit de distribution](#).

Pour réduire la charge sur les serveurs de KSN, les spécialistes de Kaspersky peuvent lancer des mises à jour de l'application qui désactivent temporairement ou limitent en partie la communication dans Kaspersky Security Network. Dans ce cas, l'état de la connexion à KSN dans l'interface de programme locale est *Inclus avec des restrictions*.

Infrastructure du KSN

Kaspersky Endpoint Security prend en charge les infrastructures KSN suivantes :

- Le *KSN global* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky Security Network et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques de Kaspersky.
- Le *KSN privé* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Endpoint Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KSN privé a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :
 - absence de connexion des postes de travail locaux à Internet ;
 - interdiction législative ou restriction imposée par la sécurité de l'entreprise sur l'envoi de données hors du pays ou hors du réseau local de l'organisation.

Par défaut, Kaspersky Security Center utilise le KSN global. Vous pouvez configurer l'utilisation du KSN privé dans la Console d'administration (MMC), dans Kaspersky Security Center 12 Web Console et dans la [ligne de commande](#). Il n'est pas possible de configurer l'utilisation du KSN privé dans Kaspersky Security Center Cloud Console.

Pour en savoir plus sur le fonctionnement du KSN local, reportez-vous à la *documentation de Kaspersky Private Security Network*.

KSN Proxy

Les ordinateurs des utilisateurs qui sont administrés par le Serveur d'administration de Kaspersky Security Center peuvent interagir avec KSN à l'aide du service KSN Proxy.


Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur de l'utilisateur peut interroger KSN et transmettre à KSN des informations, même s'il n'a pas d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication avec le réseau externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Pour en savoir plus sur le service KSN Proxy consultez l'[aide de Kaspersky Security Center](#).

Activation et désactivation de l'utilisation de Kaspersky Security Network

Pour activer ou désactiver l'utilisation de Kaspersky Security Network, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Kaspersky Security Network**.
3. Utilisez le commutateur **Kaspersky Security Network** pour activer ou désactiver le module.
Si vous avez activé l'utilisation de KSN, Kaspersky Endpoint Security affichera la déclaration de Kaspersky Security Network. Si vous êtes d'accord avec le contenu, acceptez les conditions d'utilisation de KSN.
Par défaut, Kaspersky Endpoint Security utilise le mode étendu du KSN. Le *mode étendu du KSN* est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Endpoint Security envoie [des données supplémentaires](#) à Kaspersky.
4. Si nécessaire, désactivez le commutateur **Activer le mode étendu de KSN**.
5. Enregistrez vos modifications.

Par conséquent, si l'utilisation de KSN est activée, Kaspersky Endpoint Security utilise les informations sur la réputation des fichiers, des ressources Internet et des applications reçues de Kaspersky Security Network.

Restrictions de KSN privé

KSN privé (ci-après également dénommé KPSN) vous permet d'utiliser votre propre base de données de réputation locale pour vérifier la réputation des objets (fichiers ou adresses Internet). La réputation d'un objet ajouté à la base de données de réputation locale a une priorité plus élevée que celle d'un objet ajouté à KSN/KPSN. Par exemple, imaginez que Kaspersky Endpoint Security analyse un ordinateur et demande la réputation d'un fichier dans KSN/KPSN. Si le fichier a une réputation "non fiable" dans la base de données de réputation locale, mais a une réputation "fiable" dans KSN/KPSN, Kaspersky Endpoint Security détectera le fichier comme "non fiable" et prendra les mesures définies concernant les menaces détectées.

Cependant, dans certains cas, il se peut que Kaspersky Endpoint Security ne demande pas la réputation d'un objet dans KSN/KPSN. Si tel est le cas, Kaspersky Endpoint Security ne recevra pas les données de la base de données de réputation locale de KPSN. Il se peut que Kaspersky Endpoint Security ne demande pas la réputation d'un objet dans KSN/KPSN pour les raisons suivantes :

- Les applications de Kaspersky utilisent des bases de données de réputation hors ligne. Les bases de données de réputation hors ligne sont conçues pour optimiser les ressources pendant le fonctionnement des applications Kaspersky et pour protéger les objets d'importance critique sur l'ordinateur. Les bases de données de réputation hors ligne sont créées par les experts de Kaspersky à partir des données de Kaspersky Security Network. Les applications Kaspersky mettent à jour les bases de données de réputation hors ligne avec les bases antivirus de l'application en question. Si les bases de données de réputation hors ligne contiennent des informations sur un objet en cours d'analyse, l'application ne demande pas la réputation de cet objet à KSN/KPSN.
- Les exclusions d'analyse ([zone de confiance](#)) sont configurées dans les paramètres de l'application. Si tel est le cas, l'application ne tient pas compte de la réputation de l'objet dans la base de données de réputation locale.
- L'application utilise des technologies d'optimisation de l'analyse, comme iSwift ou iChecker, ou met en cache les demandes de réputation dans KSN/KPSN. Si tel est le cas, il se peut que l'application ne demande pas la réputation des objets précédemment analysés.


- Pour optimiser sa charge de travail, l'application analyse les fichiers d'un certain format et d'une certaine taille. La liste des formats et des limites de taille pertinents est déterminée par les experts de Kaspersky. Cette liste est mise à jour avec les bases antivirus de l'application. Vous pouvez également configurer les paramètres d'optimisation de l'analyse dans l'interface de l'application, par exemple pour le [module Protection contre les fichiers malicieux](#).

Activation et désactivation du mode Cloud pour les modules de la protection

Le *mode Cloud* est un mode de fonctionnement de l'application dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données antivirus. L'utilisation avec les bases antivirus allégées est garantie par Kaspersky Security Network. La version allégée des bases de données antivirus peut réduire de moitié la charge sur la mémoire vive de l'ordinateur. Si vous ne participez pas à Kaspersky Security Network ou si le mode cloud est désactivé, Kaspersky Endpoint Security télécharge la version complète des bases de données antivirus depuis les serveurs de Kaspersky.

Lors de l'utilisation de Kaspersky Private Security Network, la fonction du mode Cloud est accessible à partir de la version Kaspersky Private Security Network 3.0.

Pour activer ou désactiver le mode cloud pour les modules de la protection, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection** → **Protection avancée** → **Kaspersky Security Network**.
3. Utilisez le commutateur **Activer le mode Cloud** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, Kaspersky Endpoint Security télécharge une version allégée ou une version complète des bases antivirus lors de la prochaine mise à jour.

Si la version simplifiée des bases antivirus ne peut être utilisée, Kaspersky Endpoint Security passe automatiquement à l'utilisation de la version complète des bases antivirus.

Vérification de la connexion à Kaspersky Security Network

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- Vous ne participez pas à Kaspersky Security Network.
- Votre ordinateur n'est pas connecté à Internet.
- L'état actuel de la clé ne permet pas d'effectuer la connexion à Kaspersky Security Network. Par exemple, une connexion à KSN peut être indisponible pour les raisons suivantes :

- L'application n'est pas activée.
- La licence ou l'abonnement a expiré.
- Des problèmes de clé de licence ont été identifiés (par exemple, la clé a été ajoutée à la liste des clés interdites).

Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :

Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Kaspersky Security Network**.

Cette action ouvre la fenêtre **Kaspersky Security Network**, qui affiche des informations sur l'activité de Kaspersky Security Network. L'application obtient les données statistiques sur l'utilisation de KSN à l'ouverture de la fenêtre **Kaspersky Security Network**. La mise à jour en temps réel des statistiques globales de l'infrastructure des services cloud Kaspersky Security Network et de l'heure de synchronisation n'a pas lieu.

La partie gauche de la fenêtre **Kaspersky Security Network** affiche l'un des états suivants concernant la connexion entre l'ordinateur et Kaspersky Security Network :

- *Activé.*

Cet état signifie que Kaspersky Security Network intervient dans le fonctionnement de Kaspersky Endpoint Security et les serveurs KSN sont accessibles.

- *Activé. Disponible avec des restrictions.*

Cet état signifie que Kaspersky Security Network intervient dans le fonctionnement de Kaspersky Endpoint Security et les serveurs KSN ne sont pas accessibles.

Il se peut que les serveurs KSN soient inaccessibles pour les raisons suivantes :

- Le service KSN Proxy (ksnproxy) est en cours d'exécution sur l'ordinateur.
- Le pare-feu bloque le port 13111.

Si le temps écoulé depuis la dernière synchronisation avec les serveurs KSN est supérieur à 15 minutes ou si l'état *Inconnu* est affiché, l'état de la connexion de Kaspersky Endpoint Security à Kaspersky Security Network prend la *valeur Activé. Indisponible*.

- *Désactivé.*

Cet état signifie que Kaspersky Security Network n'intervient pas dans le fonctionnement de Kaspersky Endpoint Security.

En cas d'échec du rétablissement de la connexion aux serveurs de Kaspersky Security Network, il est conseillé de contacter le Support Technique ou le prestataire de services.

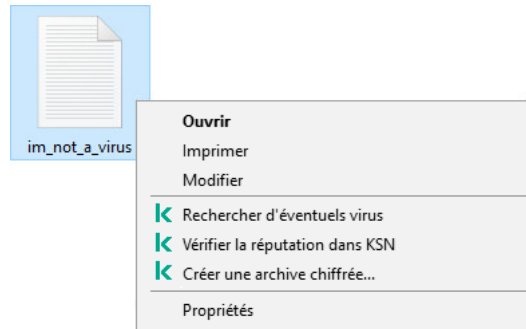
Vérification de la réputation d'un fichier dans Kaspersky Security Network

Si vous doutez de la sécurité d'un fichier, vous pouvez vérifier sa réputation dans Kaspersky Security Network.

La vérification de la réputation d'un fichier est accessible si vous avez accepté les conditions de la [Déclaration de Kaspersky Security Network](#).


Pour vérifier la réputation d'un fichier dans Kaspersky Security Network,


ouvrez le menu contextuel du fichier et sélectionnez l'option **Consulter la réputation dans le KSN** (cf. ill. ci-dessous).




Menu contextuel du fichier

Kaspersky Endpoint Security affiche la réputation du fichier :

 **De confiance.** La plupart des utilisateurs de Kaspersky Security Network ont confirmé que le fichier est de confiance.

 **Programme légitime pouvant être exploité afin de nuire à l'ordinateur ou aux données** Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être exploitées par des individus malintentionnés. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'[Encyclopédie de virus de Kaspersky](#). Vous pouvez [ajouter ces applications à la liste des applications de confiance](#).

 **Douteuses.** Un virus ou un autre programme [présentant une menace](#).

 **Inconnu.** Kaspersky Security Network ne dispose pas d'informations sur le fichier. Vous pouvez analyser un fichier à l'aide de bases antivirus (option du menu contextuel **Rechercher d'éventuels virus**).

Kaspersky Endpoint Security affiche la solution KSN utilisée pour déterminer la réputation du fichier : *KSN global* ou *KSN privé*.

Kaspersky Endpoint Security affiche également des informations supplémentaires sur le fichier (cf. ill. ci-dessous).

| | |
|------------------------|---------------------|
| Application : | Cool Application |
| Éditeur : | Mr. Vendor |
| Chemin d'accès : | c:\temp\file.exe |
| Version : | 1.0.0.4 |
| Taille : | 7,00 Mo |
| Date de création : | 01/05/2018 13:11:12 |
| Date de modification : | 08/05/2018 20:24:40 |



Douteux (Kaspersky Security Network)

KSN privé

| | |
|-----------------------|------------------|
| Première apparition : | Il y a 2 ans |
| Diffusion : | Russie (90 %) |
| Signature numérique : | Mr. Vendor |
| Date de signature : | 17/02/2018 15:37 |

Réputation d'un fichier dans Kaspersky Security Network

Analyse des connexions chiffrées

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.


Après l'installation, Kaspersky Endpoint Security ajoute un certificat Kaspersky au système de stockage des certificats de confiance (liste de certificats Windows). Kaspersky Endpoint Security prévoit également l'utilisation du système de stockage des certificats de confiance dans Firefox et Thunderbird pour analyser le trafic de ces applications.

Les modules [Contrôle Internet](#), [Protection contre les menaces par emails](#) et [Protection contre les menaces Internet](#) sont en mesure de déchiffrer et d'analyser le trafic réseau transmis via des connexions chiffrées selon les protocoles suivants :

- SSL 3.0 ;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Configuration des paramètres d'analyse des connexions chiffrées

Pour configurer les paramètres d'analyse des connexions chiffrées, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans la section Analyse des connexions chiffrées, sélectionnez le mode d'analyse des connexions chiffrées :

- **Ne pas analyser les connexions chiffrées** Kaspersky Endpoint Security n'aura pas accès au contenu des sites Internet dont l'adresse commence par <https://>.
- **Analyser les connexions chiffrées à la demande des modules de la protection.** Kaspersky Endpoint Security analysera le trafic chiffré uniquement à la demande des modules Protection contre les fichiers malicieux, Protection contre les menaces par emails et Contrôle Internet.
- **Toujours analyser les connexions chiffrées** Kaspersky Endpoint Security analysera le trafic réseau chiffré même si les modules de la protection sont désactivés.

Kaspersky Endpoint Security n'analyse pas les connexions chiffrées qui ont été établies par des [applications de confiance pour lesquelles l'analyse du trafic est désactivée](#). Kaspersky Endpoint Security n'analyse pas les connexions chiffrées provenant de la liste prédéfinie de sites Internet de confiance. La liste prédéfinie des sites Internet de confiance est créée par les experts de Kaspersky. Cette liste est mise à jour avec les bases antivirus de l'application. Vous pouvez consulter la liste prédéfinie des sites Internet de confiance uniquement dans l'interface de Kaspersky Endpoint Security. Il est impossible de consulter la liste dans Kaspersky Security Center Console.

4. Si nécessaire, [ajoutez des exclusions à l'analyse : adresses et applications de confiance](#).
5. Cliquez sur le bouton **Paramètres avancés**.
6. Configurez les paramètres d'analyse des connexions chiffrées (cf. tableau ci-après).
7. Enregistrez vos modifications.

Paramètres d'analyse des connexions chiffrées

| Paramètre | Description |
|---|---|
| Lors de l'accès à un domaine avec un certificat douteux | <ul style="list-style-type: none"> • Autoriser. Si vous choisissez cette option, Kaspersky Endpoint Security autorise l'établissement d'une connexions réseau lors de l'accès à un domaine avec un certificat douteux. <p>Si vous accédez à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui reprend un avertissement et la raison pour laquelle il est déconseillé de visiter ce domaine. Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé. Après que vous avez cliqué sur le lien, Kaspersky Endpoint Security n'affiche plus d'avertissements sur le certificat douteux pendant une heure quand vous accédez à d'autres ressources dans le même domaine.</p> <ul style="list-style-type: none"> • Bloquer la connexion. Si vous choisissez cette option, Kaspersky Endpoint Security bloque l'établissement d'une connexions réseau lors de l'accès à un domaine avec un certificat douteux. <p>Lors de l'accès à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui indique la raison pour laquelle l'accès à ce domaine est bloqué.</p> |
| En cas d'erreur lors de l'analyse des connexions sécurisées | <ul style="list-style-type: none"> • Bloquer la connexion. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée. • Ajouter un domaine aux exclusions. Si vous choisissez cette option, en cas d'erreur lors de l'analyse d'une connexion sécurisée, Kaspersky Endpoint Security ajoute le domaine dont l'accès est à l'origine de l'erreur à la liste des domaines avec erreurs |

| | |
|---|--|
| | d'analyse et il n'analyse pas le trafic réseau chiffré lors de l'accès à ce domaine. Vous pouvez consulter la liste des domaines contenant des erreurs d'analyse des connexions chiffrées uniquement dans l'interface locale de l'application. Pour réinitialiser le contenu de la liste, sélectionnez l'élément Bloquer la connexion . |
| Bloquer la connexions selon le protocole SSL 2.0 | <p>Si cette case est cochée, Kaspersky Endpoint Security bloque les connexions réseau établies via le protocole SSL 2.0.</p> <p>Si cette case est désactivée, Kaspersky Endpoint Security ne bloque pas les connexions réseau établies via le protocole SSL 2.0 et ne surveille pas le trafic réseau transmis via ces connexions.</p> |
| Déchiffrer les connexions chiffrées avec un site à l'aide d'un certificat EV | <p>Les certificats EV (Extended Validation Certificates) confirment l'authenticité des sites Internet et améliorent la sécurité de la connexion. Les navigateurs signalent la présence du certificat EV sur le site à l'aide de l'icône du cadenas dans la ligne d'adresse du navigateur. Les navigateurs peuvent aussi colorer en vert la ligne d'adresse entièrement ou partiellement.</p> <p>Si cette case est cochée, Kaspersky Endpoint Security déchiffre et surveille les connexions chiffrées avec les sites Internet qui utilisent un certificat EV.</p> <p>Si la case est décochée, Kaspersky Endpoint Security n'a pas accès au contenu du trafic HTTPS. Pour cette raison, l'application surveille le trafic HTTPS uniquement en fonction de l'adresse du site Internet, par exemple, <code>https://facebook.com</code>.</p> <p>Si vous ouvrez le site avec le certificat EV pour la première fois, la connexion sécurisée sera déchiffrée peu importe le statut de la case.</p> |

Analyse de connexions chiffrées dans Firefox et Thunderbird


Après l'installation, Kaspersky Endpoint Security ajoute un certificat Kaspersky au système de stockage des certificats de confiance (liste de certificats Windows). Par défaut, Firefox et Thunderbird utilisent leur propre liste de certificats de Mozilla au lieu de la liste de certificats Windows. Si Kaspersky Security Center est déployé dans votre organisation et qu'une stratégie est appliquée à un ordinateur, Kaspersky Endpoint Security permet automatiquement d'utiliser la liste de certificats Windows dans Firefox et Thunderbird pour analyser le trafic de ces applications. Si aucune stratégie n'est appliquée à l'ordinateur, vous pouvez choisir le stockage de certificats qui sera utilisé par les applications Mozilla. Si vous avez sélectionné la liste de certificats de Mozilla, ajoutez-y manuellement un certificat Kaspersky. Cela permettra d'éviter les erreurs lors de l'utilisation du protocole HTTPS.

Pour analyser le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird, vous devez [activer l'analyse des connexions chiffrées](#). Si l'Analyse des connexions chiffrées est désactivée, Kaspersky Endpoint Security n'analyse pas le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird.

Avant d'ajouter un certificat à la liste de Mozilla, exportez le certificat Kaspersky à partir du panneau de configuration de Windows (propriétés du navigateur). Pour en savoir plus à propos de l'exportation du certificat de Kaspersky, veuillez consulter la [base des connaissances du Support Technique](#). Pour en savoir plus sur l'ajout d'un certificat au stockage, consultez le [site Internet de l'assistance technique de Mozilla](#).

Vous pouvez choisir la liste de certificats uniquement dans l'interface locale de l'application.


Pour choisir une liste de certificats permettant d'analyser des connexions chiffrées dans Firefox et Thunderbird, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres réseau**.
3. Dans le groupe **Mozilla Firefox et Thunderbird**, cochez la case **Vérifier le trafic sécurisé dans les applications Mozilla**.
4. Sélectionnez une liste de certificats :
 - **Utiliser la boutique des certificats Windows**. Le certificat racine de Kaspersky est ajouté à cette boutique lors de l'installation de Kaspersky Endpoint Security.
 - **Utiliser la liste de certificats Mozilla**. Mozilla Firefox et Thunderbird utilisent leurs propres boutiques de certificats. Si la boutique de certificats Mozilla est sélectionnée, vous devez ajouter manuellement le certificat racine de Kaspersky à cette boutique via les propriétés du navigateur.
5. Enregistrez vos modifications.

Exclusion des connexions chiffrées de l'analyse

La majorité des ressources Web utilise une connexion chiffrée. Les experts de Kaspersky conseillent d'[activer l'analyse des connexions chiffrées](#). Si l'analyse des connexions chiffrées interfère avec votre travail, vous pouvez ajouter le site Internet aux exceptions en tant qu'*adresse de confiance*. Si une application de confiance utilise une connexion chiffrée, vous pouvez [désactiver l'analyse de la connexion chiffrée pour cette application](#). Par exemple, vous pouvez désactiver l'analyse des connexions chiffrées pour les applications de stockage dans le cloud, car celles-ci utilisent une authentification à deux facteurs avec leur propre certificat.

Pour exclure une adresse Internet de l'analyse des connexions chiffrées, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Cliquez sur le bouton **Adresses de confiance** dans le groupe **Analyse des connexions chiffrées**.
4. Cliquez sur le bouton **Ajouter**.
5. Saisissez le nom de domaine ou l'adresse IP si vous ne souhaitez pas que Kaspersky Endpoint Security analyse les connexions chiffrées établies lors de l'accès à cette page Internet.

Kaspersky Endpoint Security prend en charge le caractère  dans la saisie d'un masque d'identifiant de l'appareil.

Kaspersky Endpoint Security ne prend pas en charge les masques des adresses IP.

Exemples :

- `domain.com` : cette entrée comprend les adresses suivantes : `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Cette entrée exclut des sous-domaines

(par exemple, `subdomain.domain.com`).

- `subdomain.domain.com` : cette entrée comprend les adresses suivantes : `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Cette entrée exclut le domaine `domain.com`.
- `*.domain.com` : cette entrée comprend les adresses suivantes : `https://movies.domain.com`, `https://images.domain.com/page123`. Cette entrée exclut le domaine `domain.com`.


6. Enregistrez vos modifications.

Par défaut, Kaspersky Endpoint Security n'analyse pas les connexions chiffrées en cas d'erreur et ajoute le site Internet à une liste spéciale intitulée *Domaines avec erreurs d'analyse*. Kaspersky Endpoint Security compile une liste distincte pour chaque utilisateur ne transfère pas les données vers Kaspersky Security Center. Vous pouvez [activer le blocage de la connexion en cas d'erreur](#). Vous pouvez consulter la liste des domaines contenant des erreurs d'analyse des connexions chiffrées uniquement dans l'interface locale de l'application.

- Enregistrez vos modifications.

Par défaut, Kaspersky Endpoint Security n'analyse pas les connexions chiffrées en cas d'erreur et ajoute le site Internet à une liste spéciale intitulée *Domaines avec erreurs d'analyse*. Kaspersky Endpoint Security compile une liste distincte pour chaque utilisateur ne transfère pas les données vers Kaspersky Security Center. Vous pouvez [activer le blocage de la connexion en cas d'erreur](#). Vous pouvez consulter la liste des domaines contenant des erreurs d'analyse des connexions chiffrées uniquement dans l'interface locale de l'application.


Pour afficher une liste de domaines avec des erreurs d'analyse, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Analyse des connexions chiffrées**, cliquez sur le bouton **Domaines avec des erreurs d'analyse**.

Une liste de domaines avec des erreurs d'analyse s'ouvre. Pour réinitialiser la liste, vous devez activer le blocage de la connexion lorsqu'une erreur se produit dans la stratégie, appliquer la stratégie, rétablir le paramètre sur son état d'origine et appliquer à nouveau la stratégie.

Les experts de Kaspersky dressent une liste de sites Internet de confiance que Kaspersky Endpoint Security n'analyse pas, quels que soient les paramètres de l'application. Ce sont les *exclusions globales*.

Pour consulter les exclusions globales de l'analyse du trafic chiffré, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Analyse des connexions chiffrées**, cliquez sur le lien **Sites Internet**.

Cette action permet d'ouvrir une liste des sites Internet compilés par les experts de Kaspersky. Kaspersky Endpoint Security n'analyse pas les connexions protégées à la recherche de sites Internet figurant dans la liste. La liste peut être actualisée suite à la mise à jour des bases et des modules de Kaspersky Endpoint Security.

Contrôle de l'ordinateur

Contrôle Internet

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le Contrôle Internet contrôle l'accès des utilisateurs aux ressources Internet. Il permet de réduire la consommation de données et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur essaie d'ouvrir un site Internet dont l'accès est limité par Contrôle Internet, Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement (cf. illustration ci-dessous).

Kaspersky Endpoint Security contrôle uniquement le trafic HTTP et HTTPS.

Pour contrôler le trafic HTTPS, vous devez [activer l'analyse des connexions sécurisées](#).

Outils d'administration de l'accès aux sites Internet

Contrôle Internet permet de configurer l'accès aux sites Internet des manières suivantes :

- **Catégorie du site Internet** La catégorisation des sites Internet est assurée par le service cloud Kaspersky Security Network, l'analyse heuristique ainsi qu'à l'aide d'une base de données de sites Internet connus (incluse dans les bases de données d'application). Par exemple, vous pouvez restreindre l'accès des utilisateurs à la catégorie "Réseaux sociaux" ou à d'[autres catégories](#) ².
- **Types de données** Vous pouvez restreindre l'accès des utilisateurs aux données d'un site Internet et, par exemple, masquer les images. Kaspersky Endpoint Security détermine le type de données selon le format du fichier et non pas selon son extension.

Kaspersky Endpoint Security n'analyse pas les fichiers de tous les types au sein des archives. Par exemple, si des fichiers image figurent dans l'archive, Kaspersky Endpoint Security optera pour le type de données "Archives" au lieu de "Fichiers image".

- **Adresse distincte.** Vous pouvez saisir une adresse Internet ou [utiliser des masques](#).

Vous pouvez utiliser plusieurs modes de contrôle de l'accès aux sites Internet en même temps. Par exemple, vous pouvez limiter l'accès au type de données "Fichiers Office" uniquement pour la catégorie de sites Internet "Emails en ligne".

Règles d'accès aux ressources Internet

Le Contrôle Internet contrôle l'accès des utilisateurs aux sites Internet à l'aide de *règles d'accès*. Vous pouvez configurer les paramètres complémentaires suivants pour une règle d'accès à un site Internet :

- Utilisateurs qui seront soumis à la règle.

Par exemple, vous pouvez limiter l'accès à Internet via un navigateur pour tous les utilisateurs de l'entreprise, à l'exception du service informatique.

- Planification de l'application de la règle.

Par exemple, vous pouvez limiter l'accès à Internet via un navigateur uniquement pendant les heures ouvrables.

Priorités de règle d'accès

Chaque règle a une priorité. Plus haut se situe une règle dans la liste, plus haute est sa priorité. Si un site Internet est ajouté à plusieurs règles, Contrôle Internet utilise la règle dont la priorité est la plus élevée. Par exemple, Kaspersky Endpoint Security peut définir le portail de l'entreprise en tant que réseau social. Pour limiter l'accès aux réseaux sociaux et octroyer un accès au portail de l'entreprise, créez deux règles : une règle d'interdiction pour la catégorie de sites Internet "Réseaux sociaux" et une règle d'autorisation pour le portail de l'entreprise. La priorité de la règle d'accès au portail de l'entreprise doit être supérieure à celle de la règle d'accès aux réseaux sociaux.



Impossible d'ouvrir la page Internet demandée.

Adresse : <http://kaspersky.ru/>.

La page Internet est bloquée par la règle "kasp".

Raison : le site Internet appartient à la catégorie (aux catégories) de contenu "Contenu inconnu" et à la catégorie (aux catégories) de type de données "Données inconnues".

Ce site Internet est interdit dans l'entreprise. En cas de blocage par erreur et/ou s'il est nécessaire d'accéder au site Internet, contacter l'administrateur du réseau local de l'entreprise ([Demander l'accès](#)).

Date de création du message : 10/14/2020 1:07:28 AM



La page Internet sollicitée peut être dangereuse ou l'accès à celle-ci est interdit par la stratégie de l'entreprise.

Adresse : <http://kaspersky.ru/>.

La page Internet est bloquée par la règle "kasp".

Raison : le site Internet appartient à la catégorie (aux catégories) de contenu "Contenu inconnu" et à la catégorie (aux catégories) de type de données "Données inconnues".

Cliquez sur le lien <http://kaspersky.ru/> pour ouvrir la page Internet demandée.

Cliquez sur le lien <http://kaspersky.ru/> pour accéder à tout le contenu du site Internet avec la page Internet demandée.

Cliquez sur le lien [*/*/kaspersky.ru/](http://kaspersky.ru/) pour accéder à tous les domaines existants du niveau marqué (inférieur ou égal au niveau par un **).

L'accès aux sites Internet énumérés sera autorisé lors de la session en cours de l'application.


Si cet avertissement vous parvient par erreur, contactez l'administrateur du réseau local de l'entreprise ([Demander l'accès](#)).

Date de création du message : 10/14/2020 1:08:04 AM

Activation et désactivation du Contrôle Internet

Le Contrôle Internet est activé par défaut.

Pour activer ou désactiver le Contrôle Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Utilisez le commutateur **Contrôle Internet** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Actions avec les règles d'accès aux sites Internet

Il est déconseillé de créer plus de 1 000 règles d'accès aux ressources Web car cela peut provoquer l'instabilité du système.

La règle d'accès aux ressources Internet est un ensemble de filtres et d'actions que Kaspersky Endpoint Security exécute lorsque les utilisateurs consultent les ressources Internet définies dans la règle à l'heure planifiée indiquée du fonctionnement de la règle. Les filtres permettent de préciser les sites Internet dont l'accès est contrôlé par le Contrôle Internet.

Les filtres suivants sont accessibles :

- **Filtrage selon le contenu.** Le Contrôle Internet organise les [ressources Internet par catégories de contenu](#) et par catégories de type de données. Vous pouvez contrôler l'accès des utilisateurs aux données hébergées sur les ressources Web qui sont liées aux données déterminées par ces catégories. Lorsque les utilisateurs consultent les sites Internet qui appartiennent à la catégorie de contenu sélectionnée et/ou à la catégorie de type de données sélectionnée, Kaspersky Endpoint Security exécute l'action indiquée dans la règle.
- **Filtrage selon les URL des ressources Internet.** Vous pouvez contrôler l'accès des utilisateurs à toutes les adresses des sites Internet ou à certaines adresses des sites Internet/ou à certains groupes d'adresses des sites Internet.

Si le filtrage selon le contenu et le filtrage selon les URL des ressources Internet sont activés et les adresses des sites Internet définies et/ou les groupes d'adresses des sites Internet définis appartiennent aux catégories de contenu ou aux catégories de types de données sélectionnées, Kaspersky Endpoint Security ne contrôle pas l'accès à tous les sites Internet des catégories de contenu sélectionnées et/ou des catégories de types de données sélectionnées. Au lieu de cela, l'application contrôle uniquement l'accès aux adresses de ressources Internet et/ou à des groupes d'adresses de ressources Internet définis.



- **Filtrer par nom d'utilisateur et de groupe d'utilisateurs.** Vous pouvez définir les utilisateurs et/ou les groupes d'utilisateurs pour lesquels l'accès aux sites Internet est contrôlé conformément à la règle.
- **Planification de l'application de la règle.** Vous pouvez planifier l'application de la règle. La planification de l'application de la règle définit le moment où Kaspersky Endpoint Security contrôle l'accès aux ressources Internet indiquées dans la règle.

Après l'installation de l'application Kaspersky Endpoint Security la liste des règles du module Contrôle Internet n'est pas vide. Deux règles sont prédéfinies :

- La règle "Scripts et tables de styles" qui autorise tous les utilisateurs à accéder à tout moment à tous les sites dont l'URL contient des fichiers portant l'extension CSS, JS, VBS. Par exemple, <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- Règle par défaut. Cette règle, en fonction de l'action choisie, autorise ou interdit l'accès pour tous les utilisateurs à toutes les ressources Internet qui ne sont pas soumises à l'action d'autres règles.

Ajout d'une règle d'accès aux ressources Internet

Pour ajouter ou modifier la règle d'accès aux sites Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès aux sites Internet**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
5. Dans le champ **Nom de la règle**, saisissez le nom de la règle.
6. Sélectionnez l'état **Actif** pour la règle d'accès à la ressource Internet.
Vous pouvez utiliser le commutateur pour [désactiver la règle d'accès aux ressources Internet](#) à tout moment.
7. Dans le groupe **Action**, sélectionnez l'option appropriée :
 - **Autoriser**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security autorise l'accès aux ressources Internet conformes aux paramètres de la règle.
 - **Interdire**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security interdit l'accès aux ressources Internet conformes aux paramètres de la règle.
 - **Avertir**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security affiche un message d'avertissement qui indique que la visite de la ressource Internet est déconseillée lorsque l'utilisateur tente d'accéder à une ressource qui satisfait à la règle. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.
8. Dans le groupe **Type de filtre**, sélectionnez le filtre de contenu approprié :
 - **Par catégorie**. Vous pouvez contrôler l'accès des utilisateurs aux ressources Internet par [catégorie](#)  (par exemple, la catégorie *Réseaux sociaux*).
 - **Par types de données**. Vous pouvez contrôler l'accès des utilisateurs aux ressources Internet en fonction du type de données particulières qui y sont publiées (par exemple, des *illustrations*).

Pour configurer le filtre de contenu, procédez comme suit :

- a. Cliquez sur le lien **Configurer**.

b. Cochez les cases en regard des catégories de contenu et/ou des catégories de type de données souhaitées.

Si la case en regard du nom de la catégorie de contenu et/ou de la catégorie de type de données est cochée, Kaspersky Endpoint Security, conformément à la règle, contrôle l'accès aux sites Internet qui appartiennent aux catégories de contenu et/ou aux catégories de type de données sélectionnées.

c. Revenez à la fenêtre de configuration de la règle d'accès aux ressources Internet.

9. Dans le groupe **Adresses**, sélectionnez le filtre d'adresse approprié de la ressource Internet :

- **À toutes les adresses.** Le Contrôle Internet ne filtrera pas les ressources Internet par adresse.
- **À certaines adresses.** Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. Pour composer une liste d'adresses de ressources Internet, procédez comme suit :

a. Cliquez sur le bouton **Ajouter une adresse** ou **Ajouter un groupe d'adresses**.

b. Dans la fenêtre qui s'ouvre, créez une liste d'adresses de ressources Internet. Vous pouvez saisir une adresse Internet ou [utiliser des masques](#). Vous pouvez également [exporter une liste d'adresses de ressources Internet à partir d'un fichier TXT](#).

c. Revenez à la fenêtre de configuration de la règle d'accès aux ressources Internet.

Si l'[Analyse des connexions chiffrées est désactivée](#), seul le filtrage selon le nom du serveur est accessible pour le protocole HTTPS.

10. Dans le groupe **Utilisateurs**, sélectionnez le filtre approprié pour les utilisateurs :

- **À tous les utilisateurs.** Le Contrôle Internet ne filtrera pas les ressources Internet pour les utilisateurs en particulier.
- **À certains utilisateurs et/ou groupes.** Le Contrôle Internet ne filtrera les ressources Internet que pour des utilisateurs particuliers. Pour créer une liste d'utilisateurs auxquels vous souhaitez appliquer la règle, procédez comme suit :

a. Cliquez sur le bouton **Ajouter**.

b. Dans la fenêtre qui s'ouvre, sélectionnez les utilisateurs ou le groupe d'utilisateurs auxquels vous souhaitez appliquer la règle d'accès aux ressources Internet.

c. Revenez à la fenêtre de configuration de la règle d'accès aux ressources Internet.

11. Dans la liste déroulante **Planification de l'application de la règle**, sélectionnez le nom de la planification requise ou composez une nouvelle planification sur la base de la planification sélectionnée de fonctionnement de la règle. Pour ce faire, procédez comme suit :

a. Cliquez sur le bouton **Administration des planifications**.

b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

c. Dans la fenêtre qui s'ouvre, saisissez le nom de la planification de la règle.

d. Configurez le programme d'accès aux ressources Internet pour les utilisateurs.


e. Revenez à la fenêtre de configuration de la règle d'accès aux ressources Internet.

12. Enregistrez vos modifications.

Définition de la priorité des règles d'accès aux sites Internet


Vous pouvez définir la priorité de chaque règle dans la liste des règles en les structurant dans l'ordre spécifique.

Pour définir la priorité des règles d'accès aux sites Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès aux sites Internet**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la règle dont vous souhaitez modifier la priorité.
5. Déplacez la règle à la position appropriée dans la liste des règles d'accès aux ressources Internet à l'aide des boutons **Haut** et **Bas**.
6. Enregistrez vos modifications.

Activation et désactivation de la règle d'accès aux sites Internet

Pour activer ou désactiver la règle d'accès aux sites Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès aux sites Internet**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la règle que vous souhaitez activer ou désactiver.
5. Dans la colonne **Condition**, procédez comme suit :
 - Pour activer l'utilisation de la règle, sélectionnez la valeur **Actif**.
 - Pour désactiver l'utilisation de la règle, sélectionnez la valeur **Inactif**.
6. Enregistrez vos modifications.

Exportation et importation de la liste des adresses Internet de confiance

Vous pouvez exporter la liste des règles du Contrôle Internet dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses du même type. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles du Contrôle Internet ou pour procéder à la migration de la liste vers un autre serveur.

[Comment exporter et importer une liste de règles du Contrôle Internet dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Contrôles de sécurité** → **Contrôle Internet**.
6. Pour exporter la liste des règles du Contrôle Internet :
 - a. Sélectionnez les règles que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune règle, Kaspersky Endpoint Security exportera toutes les règles.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des règles et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.
7. Pour importer la liste des règles du Contrôle Internet :
 - a. Cliquez sur le lien **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.


[Comment exporter et importer une liste de règles du Contrôle Internet dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer la liste des règles.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Contrôles de sécurité** → **Contrôle Internet**.
5. Pour exporter la liste des règles dans le groupe **Liste des règles**, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les règles sélectionnées ou exporter la liste complète.
 - d. Cliquez sur le bouton **Exporter**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML dans le dossier des téléchargements par défaut.
6. Pour importer la liste des règles dans le groupe **Liste des règles**, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
7. Enregistrez vos modifications.

Vérification du fonctionnement des règles d'accès aux sites Internet

Pour évaluer la coordination des règles du Contrôle Internet, vous pouvez vérifier leur fonctionnement. Pour ce faire, le module Contrôle Internet prévoit la fonction "Diagnostic des règles".

Pour vérifier le fonctionnement des règles d'accès aux sites Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Paramètres**, cliquez sur le lien **Diagnostic des règles**.
La fenêtre **Diagnostic des règles** s'ouvre.


4. Cochez la case **Indiquez l'adresse** pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à un site Internet spécifique. Saisissez l'adresse de la ressource Internet dans le champ ci-dessous.
5. Définissez la liste des utilisateurs et/ou des groupes d'utilisateurs si vous voulez vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet pour des utilisateurs et / ou des groupes d'utilisateurs spécifiques.
6. Cochez la case **Filtrer le contenu** et sélectionnez l'option requise dans la liste déroulante (**Par catégorie, Par types de données** ou **Par catégories et types de données**) pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet avec des catégories de contenu et/ou des catégories de type de données.
7. Cochez la case **Tenir compte de l'heure de la tentative d'accès** si vous voulez vérifier le fonctionnement des règles en tenant compte du jour de la semaine et de l'heure des tentatives d'accès aux sites Internet indiqués dans les conditions du diagnostic des règles. Indiquez ensuite le jour de la semaine et l'heure.
8. Cliquez sur le bouton **Tester**.

À l'issue de l'analyse, un message sur l'action de Kaspersky Endpoint Security conformément à la première règle appliquée au moment de l'accès au site Internet défini (autorisation, interdiction, avertissement) sera affiché. La première règle appliquée est celle qui se trouve dans la liste des règles de Contrôle Internet au-dessus des autres règles conformes aux conditions du diagnostic. Le message est affiché à droite du bouton **Tester**. Le tableau en dessous affiche la liste des autres règles qui se sont déclenchées et le nom de l'action exécutée par Kaspersky Endpoint Security. Les règles sont classées par ordre de priorité décroissante.

Exportation et importation de la liste des adresses de sites Internet

Si vous avez créé dans la règle d'accès aux sites Internet une liste des adresses des sites Internet, vous pouvez l'exporter dans un fichier au format TXT. Vous pouvez ensuite importer la liste depuis ce fichier pour ne pas créer manuellement la liste des adresses des sites Internet lors de la configuration de la règle. La fonction de l'exportation et de l'importation de la liste des adresses des sites Internet peut vous être utile si vous créez par exemple les règles aux paramètres similaires.

Pour importer ou exporter la liste des adresses des sites Internet dans un fichier, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès aux sites Internet**.
4. Sélectionnez la règle dont vous souhaitez exporter ou importer la liste des adresses de ressources Internet.
5. Pour exporter la liste des adresses Internet de confiance, procédez comme suit dans le groupe **Adresses** :
 - a. Sélectionnez les adresses que vous souhaitez exporter.
Si vous n'avez sélectionné aucune adresse, Kaspersky Endpoint Security exportera toutes les adresses.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format TXT dans lequel vous voulez exporter la liste des adresses de ressources Internet et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste des adresses de ressources Internet dans un fichier TXT.

6. Pour importer la liste des ressources Internet, procédez comme suit dans le groupe **Adresses** :

a. Cliquez sur le bouton **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier TXT à partir duquel vous souhaitez importer la liste des ressources Internet.

b. Cliquez sur le bouton **Ouvrir**.




Si l'ordinateur dispose déjà d'une liste d'adresses, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier TXT.

7. Enregistrez vos modifications.

Surveillance de l'activité des utilisateurs sur Internet

Kaspersky Endpoint Security vous permet d'enregistrer des données relatives aux visites des utilisateurs tous les sites Internet, y compris ceux autorisés. Ainsi, vous pouvez obtenir l'historique complet de l'utilisation du navigateur. Kaspersky Endpoint Security envoie les événements liés à l'activité de l'utilisateur vers Kaspersky Security Center, dans le journal [local de Kaspersky Endpoint Security](#), et dans le journal des événements Windows. Pour recevoir les événements dans Kaspersky Security Center, il faut configurer les paramètres d'événement dans la stratégie de la Console d'administration ou de Web Console. Vous pouvez également configurer l'envoi d'événements de Contrôle Internet par email ou l'affichage de notification sur l'écran de l'ordinateur de l'utilisateur.


Kaspersky Endpoint Security génère les événements suivants liés à l'activité de l'utilisateur sur Internet :

- blocage de sites Internet (statut *Événements critiques* );
- visite sur un site Internet déconseillé (statut *Avertissement* );
- visites sur des sites Internet autorisés (statut  des *Messages d'information*).

Avant d'activer la surveillance de l'activité des utilisateurs sur Internet, vous devez procéder comme suit :


- Injectez un script d'interaction avec les pages Internet dans le trafic Internet (cf. instructions ci-après). Le script permet l'enregistrement des événements du Contrôle Internet.
- Pour contrôler le trafic HTTPS, vous devez [activer l'analyse des connexions sécurisées](#).

Pour injecter un script d'interaction avec les pages Internet dans le trafic Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Traitement du trafic**, cochez la case **Injecter un script d'interaction dans le trafic**.
4. Enregistrez vos modifications.

En conséquence, Kaspersky Endpoint Security injectera un script d'interaction avec les pages Internet dans le trafic Internet. Ce script permet d'enregistrer les événements du Contrôle Internet pour le journal des événements de l'application, le journal des événements du système d'exploitation et les [rapports](#).

Pour configurer l'enregistrement des événements de Contrôle Internet sur l'ordinateur de l'utilisateur, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
3. Dans le groupe **Notifications**, cliquez sur le bouton **Règles des notifications**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la section **Contrôle Internet**.

Le tableau des événements de Contrôle Internet et des méthodes de notification s'ouvre.

5. Pour chacun des événements, configurez le mode de notification : **Enregistrer dans le rapport local** et **Enregistrer dans le journal d'événements Windows**.

Pour enregistrer les événements relatifs aux visites sur des sites Internet autorisés, vous devez également configurer Contrôle Internet (cf. les instructions ci-dessous).

Le tableau des événements permet également d'activer la notification à l'écran et la notification par email. Pour envoyer les notifications par email, vous devez configurer les paramètres du serveur SMTP. Pour en savoir plus sur l'envoi d'événements, consultez l'[aide de Kaspersky Security Center](#).


6. Enregistrez vos modifications.

Kaspersky Endpoint Security commence alors à enregistrer les événements liés à l'activité des utilisateurs sur Internet.

Le Contrôle Internet envoie les événements d'activité des utilisateurs à Kaspersky Security Center de la manière suivante :

- Si vous utilisez Kaspersky Security Center, Contrôle Internet envoie des événements pour tous les objets qui composent la page Internet. Par conséquent, le blocage d'une page Internet peut générer plusieurs événements. Par exemple, lors du blocage de la page Internet <http://www.example.com>, Kaspersky Endpoint Security peut générer des événements pour les objets suivants : <http://www.example.com>, <http://www.example.com/icon.ico>, <http://www.example.com/file.js> et ainsi de suite.
- Si vous utilisez Kaspersky Security Center Cloud Console, le Contrôle Internet regroupe les événements et envoie uniquement le protocole et le domaine du site Internet. Par exemple, si un utilisateur visite les pages Internet déconseillées <http://www.example.com/main>, <http://www.example.com/contact> et <http://www.example.com/gallery>, Kaspersky Endpoint Security envoie un seul événement avec l'objet <http://www.example.com>.

Pour activer l'enregistrement des événements liés aux visites sur des sites Internet autorisés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Avancé**, cliquez sur le bouton **Paramètres avancés**.
4. Dans la fenêtre qui s'ouvre, cochez la case **Enregistrer les données relatives aux visites des pages autorisées dans le journal**.
5. Enregistrez vos modifications.

Vous aurez ainsi accès à l'historique complet de l'utilisation du navigateur.

Modification des modèles de messages du Contrôle Internet

En fonction de l'action définie dans les propriétés des règles du Contrôle Internet, lorsque les utilisateurs essaient d'accéder aux sites Internet, Kaspersky Endpoint Security affiche un message (en remplaçant la réponse du serveur HTTP par une page HTML avec le message) de l'un des types suivants :

- **Message d'avertissement.** Ce message avertit l'utilisateur que la visite de la ressource Internet est déconseillée et/ou ne correspond pas à la stratégie de sécurité de l'entreprise. Kaspersky Endpoint Security affiche le message d'avertissement si dans les paramètres de la règle qui décrit ce site Internet, l'option **Avertir** a été sélectionnée dans la liste déroulante **Action**.


Si l'utilisateur pense recevoir ce message d'avertissement par erreur, il peut cliquer sur le lien dans le corps du message d'avertissement pour envoyer un message prérédigé destiné à l'administrateur du réseau local d'entreprise.

- **Message de blocage du site Internet.** Kaspersky Endpoint Security affiche le message de blocage du site Internet si l'option **Interdire** a été sélectionnée dans la liste déroulante **Action** des propriétés de la règle qui décrit ce site Internet.

Si l'utilisateur considère que l'accès à la ressource Internet a été bloqué par erreur, il peut cliquer sur le lien dans le corps du message de blocage du site Internet pour envoyer un message prérédigé destiné à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message d'avertissement, de message sur le blocage de l'accès à un site Internet et de message destiné à l'administrateur du réseau local d'entreprise. Vous pouvez modifier leur contenu.

Pour modifier le modèle de message du Contrôle Internet, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle Internet**.
3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle Internet :
 - **Avertissements.** Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui avertit de la tentative d'accès au site Internet déconseillé est appliquée.
 - **Blocage.** Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui bloque l'accès au site Internet est appliquée.
 - **Message à l'administrateur.** Le champ de saisie contient le modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès au site Internet est intervenu par erreur.
4. Enregistrez vos modifications.

Règles de création de masques d'adresses de sites Internet

Le *masque d'adresse du site Internet* (ci-après également "masque d'adresse") peut vous être utile lorsque vous devez saisir une multitude d'adresses de sites Internet similaires lorsque vous créez une règle d'accès aux sites Internet. Un seul masque correct peut se substituer à une multitude d'adresses des sites Internet.

Pour créer un masque d'adresses, il faut respecter les règles suivantes :

1. Le caractère `*` remplace n'importe quelle séquence de caractères dont le nombre de caractères est zéro ou plus.

Par exemple, lors de la saisie du masque d'adresse `*abc*` la règle d'accès aux sites Internet s'applique à toutes les adresses qui contiennent la séquence `abc`. Exemple : `http://www.example.com/page_0-9abcdef.html`.

2. Une séquence de caractères `*`. (également connue sur le nom de *masque de domaine*) vous permet de sélectionner tous les domaines d'une adresse. Le masque de domaine `*` représente tout nom de domaine, nom de sous-domaine ou une ligne blanche.

Exemple : le masque `*.example.com` représente les adresses suivantes :

- `http://pictures.example.com`. Le masque de domaine `*` représente `pictures`.
- `http://user.pictures.example.com`. Le masque de domaine `*` représente `pictures` et `user`.
- `http://example.com`. Le masque de domaine `*` est interprété comme une ligne blanche.

3. La suite de caractère `www` au début du masque d'adresse est remplacée par `*`.

Exemple : le masque d'adresse `www.example.com` est équivalent à `*.example.com`. Ce masque couvre les adresses `www2.example.com` et `www.pictures.example.com`.

4. Si le masque d'adresse commence par un caractère autre que `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `*`.

5. Si le masque d'adresses se termine par le caractère différent de `/` ou `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `/*`.

Exemple : le masque d'adresse `http://www.example.com` couvre les adresses du type `http://www.example.com/abc`, où `a`, `b`, `c` représentent n'importe quels caractères.

6. Si le masque d'adresse se termine par le caractère `/`, le contenu du masque d'adresse est équivalent au même contenu avec le suffixe `*/`.

7. La séquence des caractères `/*` à la fin du masque d'adresse est traitée comme `/*` ou comme la ligne vide.

8. La vérification des adresses des sites Internet par masque d'adresse est effectuée compte tenu du schéma (`http` ou `https`) :

- S'il n'y a pas de protocole réseau dans le masque d'adresse, ce masque d'adresse couvre l'adresse avec n'importe quel protocole réseau.

Exemple : le masque de l'adresse `example.com` reprend les adresses `http://example.com` et `https://example.com`.

- S'il y a un protocole réseau dans le masque d'adresse, ce masque d'adresse couvre uniquement les adresses avec le protocole réseau identique à celui du masque d'adresse.

Exemple : le masque d'adresse `http://*.example.com` couvre l'adresse `http://www.example.com` et ne couvre pas l'adresse `https://www.example.com`.

9. Le masque d'adresse dans les guillemets doubles est interprété sans aucune permutation supplémentaire, sauf le caractère `*` s'il faisait partie du masque d'adresse d'origine. Les règles 5 et 7 ne s'appliquent pas aux masques d'adresses repris entre double guillemets (cf. exemples 14 à 18 dans le tableau ci-dessous).

10. Lors de la comparaison au masque d'adresse du site Internet ne sont pas pris en compte le nom d'utilisateur et le mot de passe, le port de connexion et le registre de caractères.

| N° | Masque d'adresse | Adresse du site Internet analysée | Est-ce que l'adresse analysée satisfait au masque d'adresse | Commentaires |
|----|----------------------------|---|---|---|
| 1 | *.example.com | http://www.123example.com | Non | Cf. règle 1. |
| 2 | *.example.com | http://www.123.example.com | Oui | Cf. règle 2. |
| 3 | *example.com | http://www.123example.com | Oui | Cf. règle 1. |
| 4 | *example.com | http://www.123.example.com | Oui | Cf. règle 1. |
| 5 | http://www.*.example.com | http://www.123example.com | Non | Cf. règle 1. |
| 6 | www.example.com | http://www.example.com | Oui | Cf. règles 3, 2, 1. |
| 7 | www.example.com | https://www.example.com | Oui | Cf. règles 3, 2, 1. |
| 8 | http://www.*.example.com | http://123.example.com | Oui | Cf. règles 3, 4, 1. |
| 9 | www.example.com | http://www.example.com/abc | Oui | Cf. règles 3, 5, 1. |
| 10 | example.com | http://www.example.com | Oui | Cf. règles 3, 1. |
| 11 | http://example.com/ | http://example.com/abc | Oui | Cf. règle 6. |
| 12 | http://example.com/* | http://example.com | Oui | Cf. règle 7. |
| 13 | http://example.com | https://example.com | Non | Cf. règle 8. |
| 14 | "example.com" | http://www.example.com | Non | Cf. règle 9. |
| 15 | "http://www.example.com" | http://www.example.com/abc | Non | Cf. règle 9. |
| 16 | "*.example.com" | http://www.example.com | Oui | Cf. règles 1, 9. |
| 17 | "http://www.example.com/*" | http://www.example.com/abc | Oui | Cf. règles 1, 9. |
| 18 | "www.example.com" | http://www.example.com ; https://www.example.com | Oui | Cf. règles 9, 8. |
| 19 | www.example.com/abc/123 | http://www.example.com/abc | Non | Le masque d'adresse contient plus d'informations que l'adresse du site Internet |

Migration des règles d'accès aux ressources Internet depuis des versions antérieures de l'application

Lors de la mise à niveau de la version Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou antérieure jusqu'à Kaspersky Endpoint Security for Windows 11.6.0, les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu migrent selon les règles suivantes :

- Les règles d'accès aux ressources Internet qui reposent sur une ou plusieurs catégories de contenu de la liste "Chats et forums", "Emails en ligne", "Réseaux sociaux" reposent sur les catégories de contenu de "Communication via Internet".
- Les règles d'accès aux ressources Internet qui reposent sur une ou plusieurs catégories de contenu de la liste "Boutiques en ligne" et "Systèmes de paiement" reposent sur les catégories de contenu "Boutiques en ligne, banques, systèmes de paiement".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de ressources "Jeux de hasard" reposent sur les catégories de contenu des ressources "Jeux de hasard, loterie, tirages au sort".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu "Jeux en ligne" reposent sur les catégories de contenu des ressources "Jeux".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu qui ne figurent pas dans les catégories ci-dessus migrent sans aucune modification.

Contrôle des appareils

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à l'ordinateur (par exemple, disques durs, caméra ou module Wi-Fi). Cela permet de protéger l'ordinateur contre l'infection lors de la connexion de ces appareils et de prévenir la perte ou la fuite de données.

Niveaux d'accès aux appareils

Le Contrôle des appareils gère l'accès aux niveaux suivants :

- **Type d'appareil.** Par exemple, imprimantes, disques amovibles, lecteurs CD/DVD.

Vous pouvez configurer l'accès des appareils de la manière suivante :

- Autoriser : ✓.
- Interdire : ⛔.
- Dépend du bus connexion (excepté Wi-Fi) : 🌈.
- Interdit, avec des exceptions (seulement Wi-Fi) : 🚫.

- **Bus de connexion.** Un *bus de connexion* est une interface qui permet de connecter des appareils à l'ordinateur (USB, FireWire, etc.). Ainsi, vous pouvez limiter la connexion de tous les appareils, par exemple, via USB.

Vous pouvez configurer l'accès des appareils de la manière suivante :

- Autoriser : ✓.
- Interdire : ⛔.

- **Appareils de confiance** Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Vous pouvez ajouter des appareils de confiance selon les données suivantes :

- **Appareils en fonction de l'identificateur.** Chaque appareil possède un identifiant unique (en anglais, Hardware ID - HWID). Vous pouvez consulter l'identificateur dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Exemple d'identifiant d'appareil : `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'ajout d'un appareil par identifiant est pratique si vous souhaitez ajouter plusieurs appareils spécifiques.
- **Appareils en fonction du modèle.** Chaque appareil possède un identifiant de fabricant (en anglais, Vendor ID - VID) et un identifiant de produit (en anglais, Product ID - PID). Vous pouvez consulter les identificateurs dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Modèle de saisie du VID et du PID : `VID_1234&PID_5678`. L'ajout d'appareil par modèle est pratique si vous utilisez des appareils d'un certain modèle dans votre organisation. Ainsi, vous pouvez ajouter tous les appareils de ce modèle.
- **Appareils en fonction du masque de l'identifiant.** Si vous utilisez plusieurs appareils avec des identifiants similaires, vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `WDC_C*`.
- **Appareils selon le masque du modèle.** Si vous utilisez plusieurs appareils avec des VID ou PID similaires (par exemples, appareils d'un même fabricant), vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `VID_05AC & PID_*`.

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils à l'aide [de règles d'accès](#). Le Contrôle des appareils permet également d'enregistrer les événements de connexion/déconnexion des appareils. Pour enregistrer les événements, vous devez configurer l'envoi des événements dans la stratégie.

Si l'accès à l'appareil dépend du bus de connexion (état 🚦), Kaspersky Endpoint Security n'enregistre pas l'événement de connexion/de déconnexion de l'appareil. Pour que l'application Kaspersky Endpoint Security enregistre les événements de connexion/de déconnexion de l'appareil, autorisez l'accès au type d'appareil correspondant (état ✅) ou ajoutez l'appareil à la liste des appareils de confiance.

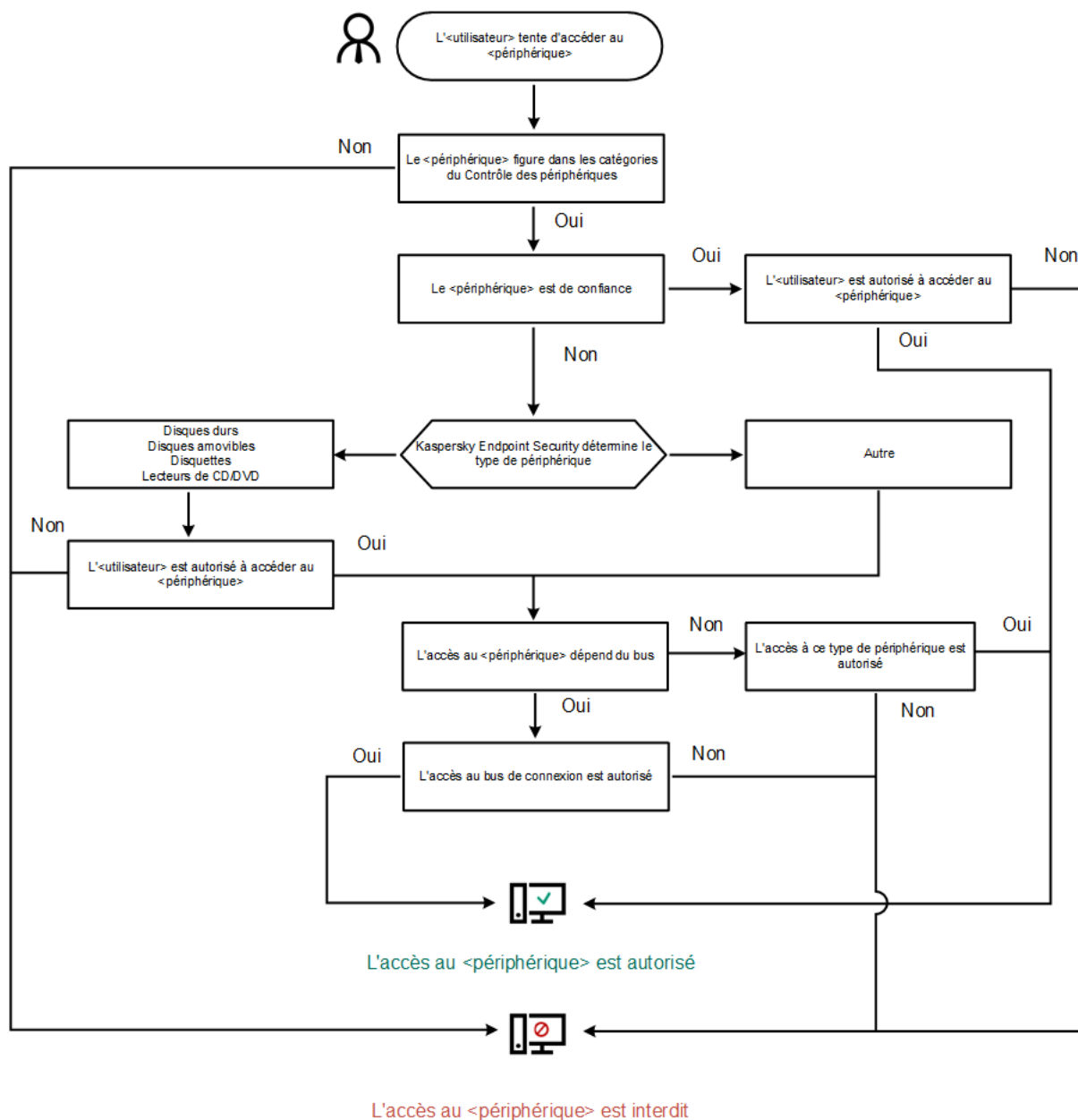
Quand l'appareil se connecte à un ordinateur auquel l'accès est interdit par le Contrôle des appareils, Kaspersky Endpoint Security bloque l'accès et affiche une notification (cf. ill. ci-dessous).



Notification du Contrôle des appareils

Algorithme de fonctionnement du Contrôle des appareils

Une fois que l'utilisateur a connecté un appareil à l'ordinateur, Kaspersky Endpoint Security prend la décision sur l'accès à cet appareil (cf. ill. ci-après).



Algorithme de fonctionnement du Contrôle des appareils


Si l'appareil est connecté et que l'accès est autorisé, vous pouvez modifier la règle d'accès et refuser l'accès. Dans ce cas, lors du prochain accès à l'appareil (consultation de l'arborescence de dossiers, lecture, écriture), Kaspersky Endpoint Security en bloque l'accès. Le blocage de l'appareil sans système de fichiers aura lieu uniquement lors de la connexion suivante de l'appareil.

Si l'utilisateur de l'ordinateur doté de Kaspersky Endpoint Security doit demander l'accès à un appareil qui, d'après lui, a été bloqué par erreur, transmettez lui [l'instruction de demande d'accès](#).

Activation et désactivation du Contrôle des appareils

Le Contrôle des appareils est activé par défaut.

Pour activer ou désactiver le Contrôle des appareils, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Utilisez le commutateur **Contrôle des appareils** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si le Contrôle des appareils est activé, l'application transmet les informations concernant les appareils connectés à Kaspersky Security Center. Vous pouvez consulter la liste des appareils connectés dans Kaspersky Security Center dans le dossier **Matériel**.

À propos des règles d'accès

Les *règles de l'accès* sont un ensemble de paramètres qui définissent l'accès des utilisateurs aux appareils installés sur l'ordinateur ou connectés à celui-ci. Il est impossible d'ajouter un appareil qui n'appartient pas à la classification du Contrôle des appareils. L'accès à ces appareils est autorisé pour tous les utilisateurs.

Règles d'accès aux appareils

Chaque ensemble de paramètres de règle d'accès se distingue en fonction du type d'appareils (cf. le tableau ci-après).

Paramètres de règle d'accès



| Appareils | Contrôle d'accès | Planification de l'accès à l'appareil | Affectation des utilisateurs/groupes d'utilisateurs | Priorité | Autorisation en lecture/en écriture |
|--|------------------|---------------------------------------|---|----------|-------------------------------------|
| Disques durs | ✓ | ✓ | ✓ | ✓ | ✓ |
| Disques amovibles | ✓ | ✓ | ✓ | ✓ | ✓ |
| Imprimantes | ✓ | – | – | – | – |
| Disquettes | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lecteurs de CD/DVD | ✓ | ✓ | ✓ | ✓ | ✓ |
| Modems | ✓ | – | – | – | – |
| Lecteurs de bande | ✓ | – | – | – | – |
| Appareils multifonctions | ✓ | – | – | – | – |
| Appareils de lecture des cartes à puce | ✓ | – | – | – | – |
| Appareils Windows CE USB ActiveSync | ✓ | – | – | – | – |
| Adaptateurs réseau externes | ✓ | – | – | – | – |
| Appareils portables | ✓ | ✓ | ✓ | ✓ | ✓ |


| | | | | | |
|---------------------|---|---|---|---|---|
| (MTP) | | | | | |
| Bluetooth | ✓ | – | – | – | – |
| Caméras et scanners | ✓ | – | – | – | – |

Règles d'accès aux appareils mobiles




Les appareils mobiles tournant sous Android et iOS sont des appareils portables (MTP). Lorsqu'un appareil portable se connecte à un ordinateur, le système d'exploitation en détermine le type. Si Android Debug Bridge (ADB), iTunes ou leurs équivalents sont installés sur l'ordinateur, le système d'exploitation identifie les appareils mobiles en tant qu'appareils ADB ou iTunes. Dans les autres cas, le système d'exploitation peut déterminer le type d'appareil mobile en tant qu'appareil portable (MTP) pour transférer des fichiers, en tant qu'appareil PTP (appareil photo) pour transférer des images ou en tant qu'autre appareil. Le type d'appareil dépend du modèle de l'appareil mobile.

L'accès aux appareils ADB ou iTunes possède les particularités suivantes :



- Il n'est pas possible de planifier l'accès à l'appareil. Autrement dit, si l'accès aux appareils est limité par des règles (état ) , les appareils ADB et iTunes sont toujours accessibles.
- Il est impossible de configurer l'accès à l'appareil pour des utilisateurs individuels ou de configurer les droits d'accès (lecture/écriture). Autrement dit, si l'accès aux appareils est limité par des règles (état ) , les appareils ADB et iTunes sont accessibles pour tous les utilisateurs avec tous les droits.
- Il n'est pas possible de configurer l'accès aux appareils ADB ou iTunes de confiance pour des utilisateurs individuels. Si l'appareil est de confiance, les appareils ADB et iTunes sont disponibles pour tous les utilisateurs.
- Si vous avez installé les applications ADB ou iTunes après avoir connecté l'appareil à l'ordinateur, l'identifiant unique de l'appareil peut être réinitialisé. Autrement dit, Kaspersky Endpoint Security considérera cet appareil comme un nouvel appareil. S'il s'agit d'un appareil de confiance, ajoutez-le à nouveau à la liste des appareils de confiance.

Par défaut, les règles d'accès aux appareils octroient un accès complet aux appareils à tous les utilisateurs à tout moment, pour autant que l'accès au bus de connexion pour les types d'appareils correspondants soit autorisé (état ) .

Règle d'accès aux réseaux Wi-Fi

La règle d'accès aux réseaux Wi-Fi définit l'autorisation (état ) ou l'interdiction (état ) d'utiliser des réseaux Wi-Fi. Vous pouvez ajouter à la règle un *réseau Wi-Fi de confiance* (état ) . L'utilisation du réseau Wi-Fi de confiance est autorisée sans restrictions. Par défaut, la règle d'accès aux réseaux Wi-Fi autorise l'accès à n'importe quel réseau Wi-Fi.


Règles d'accès au bus de connexion

Les règles d'accès au bus de connexion déterminent uniquement l'autorisation (état ) ou l'interdiction (état ) de la connexion d'appareils. Par défaut, les règles qui autorisent l'accès à tous les bus ont été créées pour les bus de connexion de la classification du module Contrôle des appareils.

Modification d'une règle d'accès aux appareils

Une *règle d'accès aux appareils* est un ensemble de paramètres qui déterminent comment les utilisateurs peuvent accéder aux appareils qui sont installés sur l'ordinateur ou connectés à celui-ci. Ces paramètres comprennent l'accès à un appareil particulier, un programme d'accès et des autorisations en lecture ou en écriture.

Pour modifier le privilège d'accès aux appareils, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.

3. Dans le groupe **Configurer l'accès**, cliquez sur le bouton **Appareils et réseaux Wi-Fi**.

La fenêtre qui s'ouvre présente les règles d'accès pour tous les appareils qui sont inclus dans la classification des modules du Contrôle des appareils.

4. Dans le groupe **Accès aux appareils de stockage de masse**, sélectionnez la règle d'accès que vous souhaitez modifier. Le groupe contient des appareils qui possèdent un système de fichiers pour lequel vous pouvez configurer des paramètres d'accès supplémentaires. Par défaut, la règle d'accès aux appareils autorise un accès libre au type d'appareils à tout moment pour tous les utilisateurs.

- a. Dans le groupe **Accès**, sélectionnez l'option d'accès à l'appareil appropriée :

- **Autoriser.**
- **Bloquer.**
- **Dépend du bus de connexion.**

Pour interdire ou autoriser l'accès à un appareil, [configurez l'accès au bus de connexion](#).

- **Limiter à l'aide de règles.**

Cette option vous permet de configurer les droits des utilisateurs, leurs autorisations et un programme d'accès à l'appareil.

- b. Dans le groupe **Droits des utilisateurs**, cliquez sur le bouton **Ajouter**.

Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès à l'appareil.

- c. Désignez la priorité pour la *règle*. Une règle comprend les attributs suivants : compte d'utilisateur, programme, autorisations (lecture/écriture) et priorité.

Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Endpoint Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Endpoint Security autorise l'attribution de priorités de 0 à 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.


Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Endpoint Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

- d. Définissez l'état **Activé** pour la règle d'accès à l'appareil.

- e. Configurez les autorisations d'accès des utilisateurs à l'appareil : lecture et/ou écriture.
 - f. Sélectionnez les utilisateurs ou le groupe d'utilisateurs auxquels vous souhaitez appliquer la règle d'accès à l'appareil.
 - g. Configurez un programme d'accès à l'appareil pour les utilisateurs.
 - h. Cliquez sur le bouton **Ajouter**.
5. Dans le groupe **Accès aux appareils externes**, sélectionnez la règle et configurez l'accès : **Autorisation**, **Interdiction** ou **Dépend du bus de connexion**. Si nécessaire, [configurez l'accès au bus de connexion](#).
 6. Dans le groupe **Accès aux réseaux Wi-Fi**, cliquez sur le lien **Wi-Fi** et configurez l'accès : **Autoriser**, **Interdire** ou **Interdire avec des exceptions**. Si nécessaire, [ajoutez des réseaux Wi-Fi à la liste des réseaux de confiance](#).
 7. Enregistrez vos modifications.

Modification de la règle d'accès au bus de connexion


Pour modifier la règle d'accès au bus de connexion, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Bus de connexion**.
La fenêtre qui s'ouvre présente les règles d'accès pour tous les bus de connexion qui sont inclus dans la classification des modules du Contrôle des appareils.
4. Sélectionnez la règle d'accès que vous souhaitez modifier.
5. Dans la colonne **Accès**, choisissez d'autoriser ou non l'accès au bus de connexion : **Autoriser** ou **Interdire**.
6. Enregistrez vos modifications.

Ajout d'un réseau Wi-Fi à la liste des réseaux de confiance

Vous pouvez permettre aux utilisateurs de se connecter aux réseaux Wi-Fi que vous considérez sûr, par exemple au réseau Wi-Fi de l'entreprise. Pour cela, il faut ajouter ce réseau à la liste des réseaux Wi-Fi de confiance. Le Contrôle des appareils bloquera l'accès à tous les réseaux Wi-Fi, à l'exception de ceux qui figurent dans la liste des réseaux de confiance.

Pour ajouter un réseau Wi-Fi à la liste des réseaux de confiance, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

La fenêtre qui s'ouvre présente les règles d'accès pour tous les appareils qui sont inclus dans la classification des modules du Contrôle des appareils.

4. Dans le groupe **Accès aux réseaux Wi-Fi**, cliquez sur le lien **Wi-Fi**.

La fenêtre ouverte indique les règles d'accès au réseau Wi-Fi.

5. Dans la colonne **Accès**, sélectionnez **Interdire avec des exceptions**.

6. Cliquez sur le bouton **Ajouter** dans le groupe **Réseau Wi-Fi de confiance**.

7. Dans la fenêtre qui s'ouvre, réalisez les opérations suivantes :


- a. Saisissez dans le champ **Nom de réseau** le nom du réseau Wi-Fi que vous souhaitez ajouter à la liste des réseaux de confiance.
- b. Sélectionnez dans la liste déroulante **Type d'authentification** le type d'authentification à utiliser lors de la connexion au réseau Wi-Fi de confiance.
- c. Sélectionnez dans la liste déroulante **Type de chiffrement** choisissez le type de chiffrement à utiliser pour la protection du trafic du réseau Wi-Fi de confiance.
- d. Vous pouvez saisir dans le champ **Commentaires** n'importe quelle information sur le réseau Wi-Fi ajouté.

Le réseau Wi-Fi est considéré de confiance si ses paramètres correspondent à tous les paramètres définis dans la règle.

8. Enregistrez vos modifications.

Surveillance de l'utilisation des disques amovibles

Pour permettre la surveillance de l'utilisation des disques amovibles, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Règles d'accès pour les appareils et les réseaux Wi-Fi**.
La fenêtre qui s'ouvre présente les règles d'accès pour tous les appareils qui sont inclus dans la classification des modules du Contrôle des appareils.
4. Dans le groupe **Accès aux appareils de stockage**, sélectionnez **Disques amovibles**.
5. Cliquez sur le lien **Enregistrement des événements dans le journal**.
6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Enregistrement des événements dans le journal**.
7. Activez le commutateur **Enregistrement des événements dans le journal**.
8. Dans le groupe **Opérations sur les fichiers**, sélectionnez les opérations que vous voulez surveiller : **Écrire**, **Supprimer**.

9. Dans le groupe **Filtrer par formats de fichier**, sélectionnez les formats des fichiers dont les opérations associées doivent être enregistrées par le Contrôle des appareils.
10. Sélectionnez les utilisateurs ou le groupe d'utilisateurs dont vous souhaitez surveiller l'utilisation des disques amovibles.
11. Enregistrez vos modifications.

Par conséquent, lorsque les utilisateurs généreront une entrée dans les fichiers situés sur les disques amovibles ou lorsqu'ils les supprimeront, Kaspersky Endpoint Security enregistrera les informations sur les opérations réalisées dans le journal des événements et les enverra à Kaspersky Security Center. Vous pouvez consulter les événements liés aux fichiers sur les disques amovibles, dans la Console d'administration de Kaspersky Security Center dans l'espace de travail pour l'entrée **Serveur d'administration** de l'onglet **Événements**. Pour que les événements s'affichent dans le journal local des événements de Kaspersky Endpoint Security, il faut cocher la case **Exécution d'une opération sur un fichier** dans les [paramètres des notifications](#) du module Contrôle des appareils.

Modification de la durée de mise en cache

Le module Contrôle des appareils enregistre les événements liés aux appareils surveillés, comme la connexion et la déconnexion d'un appareil, la lecture d'un fichier à partir d'un appareil, l'écriture d'un fichier dans un appareil, et d'autres événements. Le Contrôle des appareils autorise ou interdit alors l'action en fonction des paramètres de Kaspersky Endpoint Security.

Le Contrôle des appareils enregistre des informations à propos des événements pendant une période particulière appelée *période de mise en cache*. Si des informations à propos d'un événement sont mises en cache et que cet événement se répète, il n'est pas nécessaire d'en informer Kaspersky Endpoint Security ni d'afficher une autre invite pour autoriser l'accès à l'action correspondante, par exemple la connexion d'un appareil. Cela rend l'utilisation de l'appareil plus pratique.

Un événement est considéré comme un événement doublon si tous les paramètres d'événement suivants correspondent à l'enregistrement dans la mémoire cache :

- Identifiant de l'appareil
- SID du compte de l'utilisateur qui tente un accès
- Catégorie de l'appareil
- Action effectuée avec l'appareil
- Verdict d'autorisation de l'application pour cette action : autorisée ou interdite
- Chemin d'accès au processus utilisé pour entreprendre l'action
- Fichier consulté

Avant de modifier la période de mise en cache, [désactivez la fonctionnalité Autodéfense de Kaspersky Endpoint Security](#). Après avoir modifié la période de mise en cache, activez la fonctionnalité Autodéfense.

Pour modifier la période de mise en cache, procédez comme suit :

1. Ouvrez l'éditeur du registre sur l'ordinateur.

2. Dans l'éditeur du registre, accédez à la section suivante :

- Pour les systèmes d'exploitation 64 bits :
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
- Pour les systèmes d'exploitation 32 bits :
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]

3. Ouvrez DeviceControlEventsCachePeriod pour effectuer des modifications.

4. Définissez le nombre de minutes pendant lesquelles le Contrôle des appareils doit enregistrer des informations à propos d'un événement avant que ces informations ne soient supprimées.

Actions avec les appareils de confiance

Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Pour pouvoir utiliser les appareils de confiance, vous pouvez accorder l'accès à un utilisateur individuel, à un groupe d'utilisateurs ou à tous les utilisateurs de l'organisation.

Par exemple, si votre organisation n'autorise pas l'utilisation de disques amovibles, mais que les administrateurs utilisent de tels disques dans le cadre de leur travail, vous pouvez autoriser l'utilisation des disques amovibles uniquement pour le groupe d'administrateurs. Pour ce faire, ajoutez un disque amovible à la liste de confiance et configurez les privilèges d'accès des utilisateurs.

Kaspersky Endpoint Security permet d'ajouter un appareil à la liste de confiance des manières suivantes :

- Si la solution Kaspersky Security Center n'est pas déployée dans votre organisation, vous pouvez connecter l'appareil à l'ordinateur et [l'ajouter à la liste des appareils de confiance dans les paramètres de l'application](#). Pour diffuser la liste des appareils de confiance sur tous les ordinateurs de votre organisation, vous pouvez activer la fonction de combinaison des listes d'appareils de confiance dans une stratégie ou utiliser [la procédure d'exportation/importation](#).
- Si la solution Kaspersky Security Center est déployée dans votre organisation, vous pouvez détecter à distance tous les appareils connectés et [créer une liste d'appareils de confiance dans la stratégie](#). La liste des appareils de confiance sera disponible sur tous les ordinateurs auxquels la stratégie est appliquée.


Kaspersky Endpoint Security présente les restrictions suivantes lorsqu'il fonctionne avec des appareils de confiance :

- Les versions 11.0.0 à 11.2.0 du plug-in d'administration de Kaspersky Endpoint Security ne peuvent pas fonctionner avec une liste d'appareils de confiance qui a été créée dans les versions 11.3.0 et 11.4.0 de Kaspersky Endpoint Security. Pour fonctionner avec une liste d'appareils de confiance à partir de ces versions, le plug-in d'administration doit être mis à niveau vers les versions 11.3.0 et 11.4.0, respectivement.
- Les versions 11.3.0 et 11.4.0 du plug-in d'administration de Kaspersky Endpoint Security ne peuvent pas fonctionner avec une liste d'appareils de confiance qui a été créée dans la version 11.2.0 de Kaspersky Endpoint Security ou dans des versions antérieures. Pour que ces versions puissent fonctionner avec une liste d'appareils de confiance, l'application doit être mise à niveau vers les versions 11.3.0 et 11.4.0, respectivement. Vous pouvez également envoyer une demande accompagnée d'une description de votre situation au Support Technique par le biais de [Kaspersky CompanyAccount](#).
- Pour procéder à la migration d'une liste d'appareils de confiance à partir de la version 11.2.0 de Kaspersky Endpoint Security à la version 11.3.0, envoyez une demande accompagnée d'une description de votre situation

Ajout d'appareils à la liste des appareils de confiance via l'interface de l'application

Par défaut, si l'appareil est ajouté à la liste des appareils de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

Pour ajouter un appareil à la liste des appareils de confiance via l'interface de l'application, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Appareils de confiance**.
Cette action permet d'exporter une liste d'appareils de confiance.
4. Cliquez sur le bouton **Sélectionner**.
Cette action permet d'ouvrir la liste des appareils connectés. La liste des appareils dépend de la valeur sélectionnée dans la liste déroulante **Afficher les appareils connectés**.
5. Dans la liste des appareils, sélectionnez l'appareil que vous souhaitez ajouter à la liste des appareils de confiance.
6. Dans le champ **Commentaires**, vous pouvez fournir toute information utile concernant l'appareil de confiance.
7. Sélectionnez les utilisateurs ou le groupe d'utilisateurs pour lesquels vous souhaitez autoriser l'accès aux appareils de confiance.
8. Enregistrez vos modifications.

Ajout d'un appareil à la liste des appareils de confiance de Kaspersky Security Center

Kaspersky Security Center reçoit des informations relatives aux appareils si Kaspersky Endpoint Security est installé sur les ordinateurs et que le [Contrôle des appareils est activé](#). Il n'est pas possible d'ajouter un appareil à la liste de confiance si Kaspersky Security Center ne dispose d'aucune information à son sujet.

Vous pouvez ajouter un appareil à la liste des appareils de confiance en fonction des données suivantes :

- **Appareils en fonction de l'identificateur.** Chaque appareil possède un identifiant unique (en anglais, Hardware ID - HWID). Vous pouvez consulter l'identificateur dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Exemple d'identifiant d'appareil : `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'ajout d'un appareil par identifiant est pratique si vous souhaitez ajouter plusieurs appareils spécifiques.
- **Appareils en fonction du modèle.** Chaque appareil possède un identifiant de fabricant (en anglais, Vendor ID - VID) et un identifiant de produit (en anglais, Product ID - PID). Vous pouvez consulter les identificateurs dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Modèle de saisie du VID et du PID :

VID_1234&PID_5678. L'ajout d'appareil par modèle est pratique si vous utilisez des appareils d'un certain modèle dans votre organisation. Ainsi, vous pouvez ajouter tous les appareils de ce modèle.

- **Appareils en fonction du masque de l'identifiant.** Si vous utilisez plusieurs appareils avec des identifiants similaires, vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `WDC_C*`.
- **Appareils selon le masque du modèle.** Si vous utilisez plusieurs appareils avec des VID ou PID similaires (par exemples, appareils d'un même fabricant), vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `VID_05AC & PID_*`.

Pour ajouter un appareil à la liste des appareils de confiance, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
6. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Appareils de confiance**.
7. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'appareils de confiance pour tous les ordinateurs de l'organisation.

Les listes des appareils de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les appareils de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultés. La modification ou la suppression d'appareils de confiance de la stratégie parent n'est pas possible.
8. Cliquez sur le bouton **Ajouter** et sélectionnez une méthode pour ajouter un appareil à la liste des appareils de confiance.
9. Pour filtrer les appareils, sélectionnez un type d'appareil dans la liste déroulante **Type d'appareil** (par exemple, **Disques amovibles**).
10. Dans le champ **Nom/modèle**, saisissez l'identifiant de l'appareil, le modèle (VID et PID) ou le masque, selon la méthode d'ajout sélectionnée.

L'ajout d'appareils par masque de modèle (VID et PID) fonctionne comme suit : si vous saisissez un masque de modèle qui ne correspond à aucun modèle, Kaspersky Endpoint Security vérifie la conformité de l'identifiant de l'appareil (HWID) avec le masque. Kaspersky Endpoint Security vérifie la conformité uniquement au niveau de la partie de l'identifiant d'appareil qui détermine le fournisseur et le type d'appareil (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Si le masque de modèle correspond à cette partie de l'identifiant d'appareil, les appareils correspondant au masque seront ajoutés à la liste des appareils de confiance sur l'ordinateur. Dans ce cas, dans Kaspersky Security Center, le bouton **Actualiser** affiche une liste vide d'appareils. Pour afficher correctement la liste des appareils, vous pouvez utiliser la méthode d'ajout d'un identifiant d'appareil selon un masque.

11. Pour filtrer les appareils, saisissez dans le champ **Ordinateur** le nom de l'ordinateur ou le masque de nom de l'ordinateur auquel l'appareil est connecté.
Le caractère ***** remplace n'importe quelle combinaison de caractères. Le caractère **?** remplace n'importe quel caractère unique.
12. Cliquez sur le bouton **Actualiser**.
Le tableau affiche une liste d'appareils qui satisfont aux paramètres de filtrage spécifiés.
13. Cochez les cases en regard des noms des appareils que vous souhaitez ajouter à la liste des appareils de confiance.
14. Dans le champ **Commentaires**, saisissez une description de la raison de l'ajout des appareils à la liste de confiance.
15. À droite du champ **Autoriser les utilisateurs et/ou les groupes d'utilisateurs**, cliquez sur le bouton **Sélectionner**.
16. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.
Par défaut, l'accès aux appareils de confiance est autorisé pour le groupe Tous.
17. Enregistrez vos modifications.

Lorsqu'un appareil est connecté, Kaspersky Endpoint Security vérifie la liste des appareils de confiance pour un utilisateur autorisé. Si l'appareil appartient aux appareils de confiance, Kaspersky Endpoint Security autorise l'accès à celui-ci avec tous les privilèges, même si l'accès au type d'appareil ou au bus de connexion est refusé. Si l'appareil est douteux et que l'accès est refusé, vous pouvez [demander l'accès à l'appareil verrouillé](#).

Exportation et importation de la liste des appareils de confiance

Pour distribuer la liste des appareils de confiance à tous les ordinateurs de votre organisation, vous pouvez utiliser la procédure d'exportation/importation.

Par exemple, si vous devez distribuer une liste de disques amovibles de confiance, vous devez effectuer les opérations suivantes :

1. Connectez les disques amovibles à votre ordinateur en série.
2. Dans les paramètres de Kaspersky Endpoint Security, [ajoutez les disques amovibles à la liste des appareils de confiance](#). Si nécessaire, configurez les privilèges d'accès d'utilisateur. Par exemple, autorisez l'accès aux disques amovibles uniquement pour les administrateurs.
3. Exportez la liste des appareils de confiance dans les paramètres de Kaspersky Endpoint Security (cf. instructions ci-dessous).
4. Distribuez le fichier contenant la liste des appareils de confiance aux autres ordinateurs de votre organisation. Par exemple, placez le fichier dans un dossier partagé.
5. Importez la liste des appareils de confiance dans les paramètres de Kaspersky Endpoint Security sur les autres ordinateurs de l'organisation (cf. instructions ci-dessous).

Pour importer ou exporter une liste d'appareils de confiance, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.

3. Dans le groupe **Paramètres**, cliquez sur le bouton **Appareils de confiance**.

Cette action permet d'exporter une liste d'appareils de confiance.

4. Pour exporter une liste d'appareils de confiance, procédez comme suit :

a. Sélectionnez les appareils de confiance que vous souhaitez exporter.

b. Cliquez sur le bouton **Exporter**.

c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des appareils de confiance et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des appareils de confiance dans un fichier XML.

5. Pour importer une liste d'appareils de confiance, procédez comme suit :

a. Dans la liste déroulante **Importer**, sélectionnez l'action appropriée : **Importer et ajouter à celui existant** ou **Importer et remplacer celui existant**.

b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des appareils de confiance.

c. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'appareils de confiance, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

6. Enregistrez vos modifications.

Lorsqu'un appareil est connecté, Kaspersky Endpoint Security vérifie la liste des appareils de confiance pour un utilisateur autorisé. Si l'appareil appartient aux appareils de confiance, Kaspersky Endpoint Security autorise l'accès à celui-ci avec tous les privilèges, même si l'accès au type d'appareil ou au bus de connexion est refusé.

Obtention de l'accès à l'appareil bloqué

Lors de la configuration du Contrôle des appareils, vous pouvez interdire par accident l'accès à un appareil nécessaire à votre travail.

Si la solution Kaspersky Security Center n'est pas déployée dans votre entreprise, vous pouvez octroyer un accès à l'appareil dans les paramètres de Kaspersky Endpoint Security. Par exemple, vous pouvez [ajouter un appareil à la liste des appareils de confiance](#) ou [désactiver temporairement le Contrôle des appareils](#).

Si la solution Kaspersky Security Center est déployée dans votre entreprise et si une stratégie est appliquée aux ordinateurs, vous pouvez octroyer un accès à l'appareil dans la console d'administration.

Octroi de l'accès en mode en ligne

L'octroi d'un accès à un appareil bloqué en mode en ligne est disponible uniquement si l'entreprise a déployé la solution Kaspersky Security Center et si une stratégie a été appliquée à l'ordinateur. L'ordinateur doit pouvoir établir une connexion avec le Serveur d'administration.

L'octroi d'un accès en ligne comprend les étapes suivantes :

1. L'utilisateur envoie une demande d'accès à l'administrateur.

2. L'administrateur ajoute l'appareil à la liste des appareils de confiance.

Vous pouvez ajouter l'appareil de confiance dans la stratégie pour le groupe d'administration ou dans les paramètres locaux de l'application pour un ordinateur distinct.

3. L'administrateur met à jour les paramètres de Kaspersky Endpoint Security sur l'ordinateur de l'utilisateur.

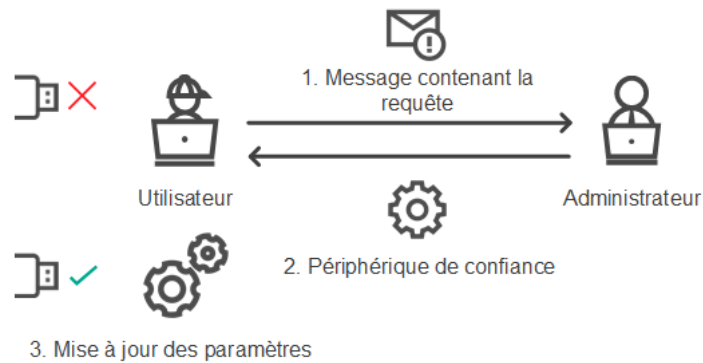


Schéma de l'octroi de l'accès à un appareil en mode en ligne

Octroi de l'accès en mode hors ligne

L'octroi d'un accès à un appareil bloqué en mode hors-ligne est disponible uniquement si l'entreprise a déployé la solution Kaspersky Security Center et si une stratégie a été appliquée à l'ordinateur. Dans les paramètres de stratégie de la section **Contrôle des appareils**, cochez la case **Autoriser la demande d'accès temporaire**.

Si vous devez fournir un accès temporaire à un appareil bloqué et qu'il est impossible d'[ajouter celui-ci à la liste des appareils de confiance](#), vous pouvez octroyer un accès hors ligne à l'appareil. Cela signifie que vous pouvez octroyer un accès à un appareil bloqué si l'ordinateur n'a pas accès au réseau ou si l'ordinateur se trouve hors du réseau.

L'octroi d'un accès hors ligne comprend les étapes suivantes :

1. L'utilisateur crée un fichier de demande et le transmet à l'administrateur.

2. L'administrateur crée une clé d'accès à partir du fichier de demande et la transmet à l'utilisateur.

3. L'utilisateur active la clé d'accès.

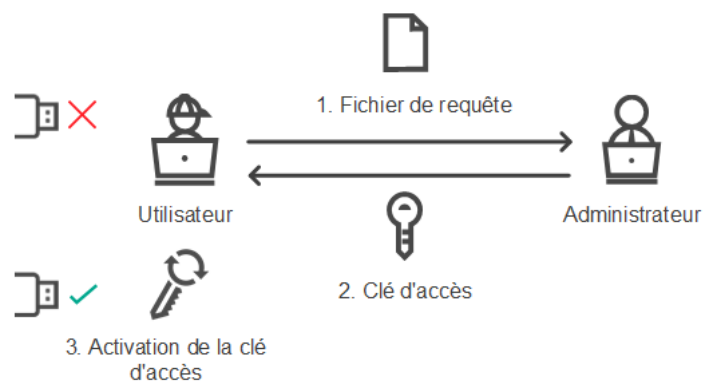


Schéma d'accès à l'appareil en mode hors ligne

Octroi de l'accès en mode en ligne

L'octroi d'un accès à un appareil bloqué en mode en ligne est disponible uniquement si l'entreprise a déployé la solution Kaspersky Security Center et si une stratégie a été appliquée à l'ordinateur. L'ordinateur doit pouvoir établir une connexion avec le Serveur d'administration.

Pour solliciter un accès à un appareil bloqué, procédez comme suit :

1. Connectez l'appareil à l'ordinateur.

Kaspersky Endpoint Security affiche une notification de blocage de l'accès à l'appareil (cf. ill. ci-dessous).

2. Cliquez sur le lien **Demander l'accès**.

La fenêtre **Message de l'administrateur** s'ouvre. Le message contient des informations relatives à l'appareil bloqué.

3. Cliquez sur le bouton **Envoyer**.

L'administrateur recevra un message de demande d'accès, par exemple par email. Pour en savoir plus sur le traitement des demandes des utilisateurs, consultez l'[aide de Kaspersky Security Center](#). Une fois que [l'appareil a été ajouté à la liste de confiance](#) et que les paramètres de Kaspersky Endpoint Security sur l'ordinateur ont été mis à jour, l'utilisateur a accès à l'appareil.



Notification du Contrôle des appareils

Octroi de l'accès en mode hors ligne

L'octroi d'un accès à un appareil bloqué en mode hors-ligne est disponible uniquement si l'entreprise a déployé la solution Kaspersky Security Center et si une stratégie a été appliquée à l'ordinateur. Dans les paramètres de stratégie de la section **Contrôle des appareils**, cochez la case **Autoriser la demande d'accès temporaire**.

Pour solliciter un accès à un appareil bloqué, procédez comme suit :

1. Connectez l'appareil à l'ordinateur.
Kaspersky Endpoint Security affiche une notification de blocage de l'accès à l'appareil (cf. ill. ci-dessous).
2. Cliquez sur le lien **Demander l'accès temporaire**.
La fenêtre **Demande d'accès à l'appareil** s'ouvre et présente une liste d'appareils connectés.
3. Sélectionnez dans la liste des appareils connectés celui auquel vous souhaitez accéder.
4. Cliquez sur le bouton **Créer un fichier de requête**.
5. Indiquez dans le champ **Durée de l'accès à l'appareil** la durée pendant laquelle vous souhaitez avoir accès à l'appareil.
6. Enregistrez le fichier dans la mémoire de votre ordinateur.

Le fichier de requête portant l'extension *.akey est chargé dans la mémoire de l'ordinateur. Transmettez le fichier de requête d'accès à l'appareil à l'administrateur du réseau local de l'organisation via n'importe laquelle des méthodes disponibles.



Notification du Contrôle des appareils


Pour créer la clé d'accès à l'appareil bloqué pour l'administrateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

4. Dans la liste des postes clients, sélectionnez l'ordinateur à l'utilisateur duquel vous souhaitez octroyer un accès temporaire à l'appareil bloqué.
5. Dans le menu contextuel de l'ordinateur, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Contrôle des appareils**.
7. Cliquez sur le bouton **Parcourir** et téléchargez le fichier de requête d'accès envoyé par l'utilisateur.
Les informations relatives à l'appareil bloqué auquel l'utilisateur a sollicité l'accès s'affichent.
8. Le cas échéant, modifiez la valeur du paramètre **Durée de l'accès à l'appareil**.
Par défaut, le paramètre **Durée de l'accès à l'appareil** prend la valeur définie par l'utilisateur lors de la création du fichier de demande.
9. Définissez la valeur du paramètre **Période d'activation**.
Le paramètre définit la période au cours de laquelle l'utilisateur peut activer l'accès à l'appareil bloqué à l'aide de la clé d'accès fournie.
10. Enregistrez le fichier clé d'accès dans la mémoire de l'ordinateur.

La clé d'accès à l'appareil bloqué est alors chargée dans la mémoire de l'ordinateur. Le fichier clé d'accès porte l'extension *.acode. Envoyez la clé d'accès à l'appareil bloqué à l'utilisateur de n'importe quelle manière.

Pour activer une clé d'accès pour un utilisateur, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Demande d'accès**, cliquez sur le bouton **Demande d'accès à l'appareil**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Activer la clé d'accès**.
5. Cette fenêtre permet de choisir le fichier avec la clé d'accès à l'appareil envoyé par l'administrateur du réseau local de l'entreprise. Cliquez sur le bouton **Ouvrir**.
Une fenêtre reprenant des informations sur l'accès octroyé s'ouvre.
6. Cliquez sur le bouton **OK**.


L'utilisateur peut alors accéder à l'appareil pendant une période définie par l'administrateur. L'utilisateur recevra un ensemble complet de droits d'accès à l'appareil (écriture et lecture). Une fois la clé expirée, l'accès à l'appareil sera bloqué. Si l'utilisateur requiert un accès permanent à l'appareil, [ajoutez ce dernier à la liste des appareils de confiance](#).

Modification des modèles de messages du Contrôle des appareils

Quand l'utilisateur tente de s'adresser à l'appareil bloqué, Kaspersky Endpoint Security affiche le message sur le blocage d'accès à l'appareil ou sur l'interdiction de l'opération sur le contenu de l'appareil. Si l'utilisateur considère que le blocage de l'accès à l'appareil ou l'interdiction de l'opération sur le contenu de l'appareil est une erreur, il peut envoyer un message à l'administrateur du réseau local de l'organisation via le lien qui apparaît dans le texte du message relatif au blocage.

Il existe des modèles prévus pour les messages de blocage d'accès à l'appareil ou d'interdiction des opérations sur le contenu ainsi que des modèles de messages pour l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier les modèles de message du Contrôle des appareils, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle des appareils :
 - **Message sur le blocage.** Modèle du message qui apparaît lorsqu'un utilisateur accède à un appareil bloqué. Ce message apparaît également lorsqu'un utilisateur tente d'exécuter une opération interdite sur le contenu de l'appareil.
 - **Message à l'administrateur.** Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès à l'appareil ou l'interdiction des opérations impliquant le contenu de l'appareil sont intervenus par erreur.
4. Enregistrez vos modifications.

Anti-Bridging

L'Anti-Bridging empêche la création de ponts réseau, ce qui élimine la possibilité d'établir simultanément plusieurs connexions réseau pour un ordinateur. Il offre une protection du réseau de l'entreprise contre les attaques via des réseaux non sécurisés et non autorisés.

L'Anti-Bridging régit l'établissement des connexions réseau à l'aide de *règles d'établissement de connexions*.

Il existe des règles d'établissement d'une connexion pour les types d'appareils préinstallés suivants :

- Adaptateurs réseau
- Adaptateurs Wi-Fi
- Modems


Si la règle d'établissement d'une connexion est activée, Kaspersky Endpoint Security exécute les actions suivantes :

- bloque la connexion active lors de l'établissement d'une nouvelle connexion si le type d'appareil indiqué dans la règle est utilisé pour les deux connexions ;
- bloque les connexions établies ou qui vont être établies à l'aide des types d'appareil soumis à des règles d'une priorité inférieure.

Activation de la fonctionnalité Anti-Bridging

La fonctionnalité Anti-Bridging est désactivée par défaut.


Pour activer la fonctionnalité Anti-Bridging, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Anti-Bridging**.
4. Utilisez le commutateur **Activer l'Anti-Bridging** pour activer ou désactiver cette fonctionnalité.
5. Enregistrez vos modifications.

Après l'activation de la fonction Anti-Bridging, Kaspersky Endpoint Security bloque les connexions déjà établies conformément aux règles d'établissement des connexions.


Modification de l'état d'une règle d'établissement de connexion

Pour modifier l'état de la règle d'établissement de la connexion, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Anti-Bridging**.
4. Dans le groupe **Règles des appareils**, sélectionnez la règle dont vous souhaitez modifier l'état.
5. Utilisez les commutateurs dans la colonne **Contrôle** pour activer ou désactiver la règle.
6. Enregistrez vos modifications.

Modification de la priorité d'une règle d'établissement de connexion

Pour modifier l'état de la règle d'établissement de la connexion Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des appareils**.
3. Dans le groupe **Paramètres**, cliquez sur le bouton **Anti-Bridging**.
4. Dans le groupe **Règles des appareils**, sélectionnez la règle dont vous souhaitez modifier la priorité.
5. Utilisez les boutons **Haut/Bas** pour configurer la priorité de la règle de connexion.

Plus la règle se trouve vers le haut du tableau des règles, plus elle bénéficie d'une priorité élevée. La fonction Anti-Bridging bloque toutes les connexions, à l'exception d'une connexion établie à l'aide du type d'appareils pour lequel la règle de priorité supérieure est utilisée.

6. Enregistrez vos modifications.

Contrôle évolutif des anomalies

Ce module est disponible uniquement pour Kaspersky Endpoint Security for Business Advanced et Kaspersky Total Security for Business. Pour en savoir plus à propos de Kaspersky Endpoint Security for Business, veuillez consulter le [site de Kaspersky](#)).

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le module Contrôle évolutif des anomalies surveille et bloque les actions atypiques pour les ordinateurs du réseau d'une organisation. Le Contrôle évolutif des anomalies utilise un ensemble de règles (par exemple, la règle *Lancement de Windows PowerShell depuis une application de bureautique*) pour suivre les actions atypiques. Ces règles sont créées par les experts de Kaspersky sur la base des scénarios typiques d'action malveillantes. Vous pouvez choisir le comportement du Contrôle évolutif des anomalies pour chacune des règles et, par exemple, autoriser le lancement de scripts PowerShell pour automatiser l'exécution des tâches d'entreprise. Kaspersky Endpoint Security met à jour l'ensemble de règles à l'aide des bases de données de l'application. La mise à jour de l'ensemble de règles doit être [confirmer manuellement](#).

Configuration du Contrôle évolutif des anomalies

La configuration du Contrôle évolutif des anomalies comprend les étapes suivantes :

1. Apprentissage du Contrôle évolutif des anomalies

Une fois que le Contrôle évolutif des anomalies a été activé, les règles fonctionnent en *mode d'apprentissage*. Au cours de l'apprentissage, le Contrôle évolutif des anomalies surveille le déclenchement des règles et envoie les événements déclencheurs à Kaspersky Security Center. La durée du mode d'apprentissage est propre à chaque règle. Celle-ci est définie par les experts de Kaspersky. En règle générale, le mode d'apprentissage dure 2 semaines.

Si une règle n'a jamais été déclenchée lors de l'apprentissage, le Contrôle évolutif des anomalies considère les actions associées à cette règle comme atypiques. Kaspersky Endpoint Security bloquera toutes les actions associées à cette règle.

Si la règle s'est déclenchée lors de l'apprentissage, Kaspersky Endpoint Security enregistre les événements dans [rapport sur les déclenchements des règles](#) et dans le stockage **Fonctionnement des règles en mode d'apprentissage**.

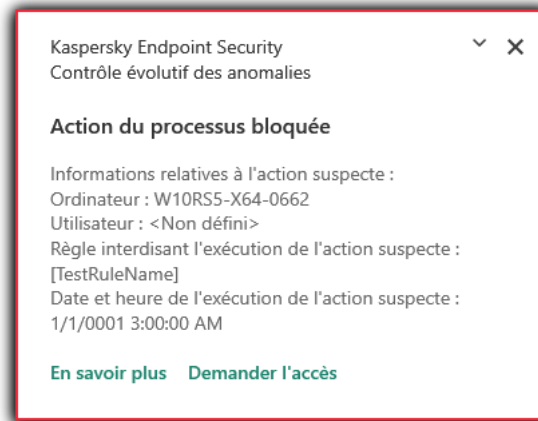
2. Analyse du rapport sur les déclenchements des règles

L'administrateur analyse le [rapport sur les déclenchements des règles](#) ou le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Ensuite, l'administrateur peut sélectionner le comportement du Contrôle évolutif des anomalies lors du déclenchement d'une règle : bloquer ou autoriser. En outre, l'administrateur peut continuer à surveiller le déclenchement de la règle et prolonger le fonctionnement d'application en mode d'apprentissage. Si l'administrateur ne prend aucune mesure, l'application continuera également à fonctionner en mode d'apprentissage. Le décompte de la durée du mode d'apprentissage est remis à zéro.

La configuration du Contrôle évolutif des anomalies se déroule en temps réel. La configuration du Contrôle évolutif des anomalies se déroule de la manière suivante :

- Le Contrôle évolutif des anomalies commence automatiquement à bloquer les actions associées aux règles qui ne se sont pas déclenchées lors de l'apprentissage.
- Kaspersky Endpoint Security ajoute de nouvelles règles ou supprime les règles qui ne sont plus pertinentes.
- L'administrateur configure le fonctionnement du Contrôle évolutif des anomalies après avoir analysé le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Il est recommandé de vérifier le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**.

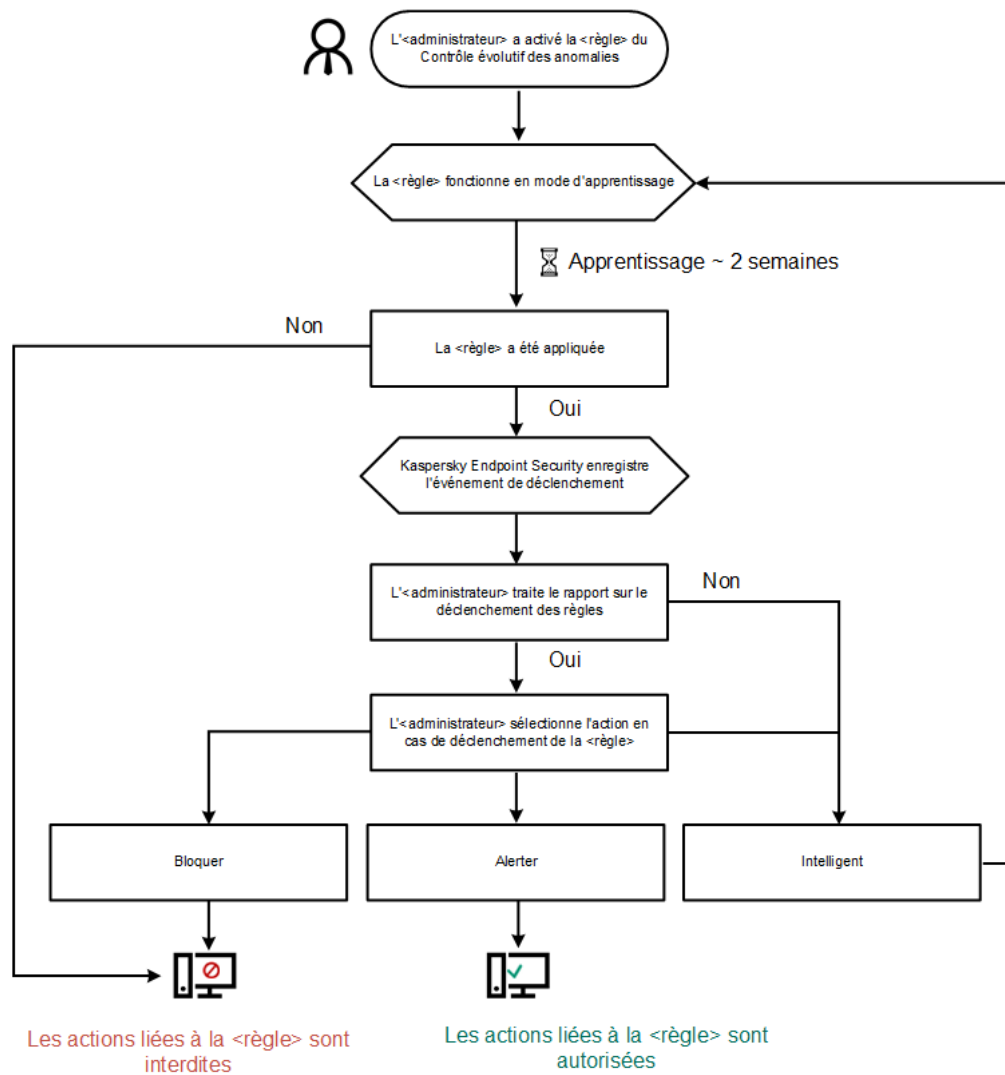
Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



Notification du Contrôle évolutif des anomalies

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Kaspersky Endpoint Security autorise ou non l'exécution d'une action associée à une règle selon l'algorithme suivant (cf. ill. ci-dessous).




Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Activation et désactivation du Contrôle évolutif des anomalies


Le Contrôle évolutif des anomalies est activé par défaut.

Pour activer ou désactiver le Contrôle évolutif des anomalies, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Utilisez le commutateur **Contrôle évolutif des anomalies** pour activer ou désactiver le module.
4. Enregistrez vos modifications.


Activation et désactivation d'une règle du Contrôle évolutif des anomalies

Pour activer ou désactiver une règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Règles**, cliquez sur le bouton **Modifier les règles**.
La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Dans le tableau, sélectionnez un ensemble de règles (par exemple, *Activité des applications de bureau*) et développez l'ensemble.
5. Sélectionnez une règle (par exemple, *Démarrer Windows PowerShell à partir d'applications de bureau*).
6. Utilisez le commutateur dans la colonne **État** pour activer ou désactiver la règle du Contrôle évolutif des anomalies.
7. Enregistrez vos modifications.

Modification de l'action en cas de déclenchement d'une règle du Contrôle évolutif des anomalies

Pour modifier l'action en cas de déclenchement d'une règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Règles**, cliquez sur le bouton **Modifier les règles**.
La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Sélectionnez une règle dans le tableau.
5. Cliquez sur le bouton **Modifier**.
La fenêtre des propriétés des règles du Contrôle évolutif des anomalies s'ouvre.
6. Dans le groupe **Action**, sélectionnez l'une des options suivantes :
 - **Intelligente**. Si vous choisissez cette option, la règle du Contrôle évolutif des anomalies fonctionne en mode d'apprentissage tout au long de la période définie par les experts de Kaspersky. Dans ce mode de fonctionnement de la règle du Contrôle évolutif des anomalies, Kaspersky Endpoint Security autorise toute activité qui tombe sous le coup de cette règle et crée un enregistrement dans le stockage **Fonctionnement des règles en mode d'apprentissage** du Serveur d'administration de Kaspersky Security Center. À l'issue de la période d'apprentissage, Kaspersky Endpoint Security bloque toute activité régie par une règle du Contrôle évolutif des anomalies et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.
 - **Interdire**. Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security bloque l'activité qui tombe sous le coup de la règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

- **Notifier.** Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security autorise l'activité qui tombe sous le coup de cette règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.


7. Enregistrez vos modifications.

Création d'une exclusion pour une règle du Contrôle évolutif des anomalies

Pour les règles du Contrôle évolutif des anomalies, il est impossible de créer plus de 1 000 exclusions. Il est déconseillé de créer plus de 200 exclusions. Pour diminuer la quantité d'exclusions utilisées, il est conseillé d'utiliser des masques dans les paramètres des exclusions.

L'exclusion pour la règle du Contrôle évolutif des anomalies contient une description des objets source et cible. *L'objet source* est l'objet qui exécute l'action. *L'objet cible* est l'objet qui subit l'action. Par exemple, vous avez ouvert le fichier `file.xlsx`. Par conséquent, un fichier de bibliothèque avec l'extension DLL est chargé dans la mémoire de l'ordinateur. Cette bibliothèque est utilisée par un navigateur (fichier exécutable intitulé `browser.exe`). Dans l'exemple donné, `file.xlsx` est l'objet source. Excel est le processus source, `browser.exe` est l'objet cible et Browser, le processus cible.

Pour créer une exclusion pour une règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Règles**, cliquez sur le bouton **Modifier les règles**.
La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Sélectionnez une règle dans le tableau.
5. Cliquez sur le bouton **Modifier**.
La fenêtre des propriétés des règles du Contrôle évolutif des anomalies s'ouvre.
6. Dans le groupe **Exclusions**, cliquez sur le bouton **Ajouter**.
La fenêtre de propriétés des exclusions s'ouvre.
7. Sélectionnez l'utilisateur pour lequel vous souhaitez configurer une exclusion.

Le Contrôle évolutif des anomalies ne prend pas en charge les exclusions pour les groupes d'utilisateurs. Si vous sélectionnez un groupe d'utilisateurs, Kaspersky Endpoint Security n'applique pas l'exclusion.

8. Dans le champ **Description**, saisissez une description de l'exclusion.
9. Définissez les paramètres de l'objet source ou du processus source lancés par l'objet :
 - **Processus source.** Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, `C:\Dir\File.exe` ou `Dir*.exe`).
 - **Hash du processus source.** Hachage du fichier.

- **Objet source.** Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, C:\Dir\File.exe ou Dir*.exe). Par exemple, le chemin d'accès au fichier document.docm qui lance les processus cibles à l'aide d'un script ou d'une macro.

Vous pouvez renseigner également d'autres objets pour l'exclusion, par exemple une adresse Internet, des macros, une commande de la ligne de commande, le chemin d'accès au registre, etc. Désignez l'objet selon le modèle suivant : `object://<objet>`, où <objet> désigne le nom de l'objet, par exemple, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Vous pouvez également utiliser des masques, par exemple, `object://*C:\Windows\temp*`.

- **Hachage de l'objet source.** Hachage du fichier.

La règle du Contrôle évolutif des anomalies ne s'applique pas aux actions exécutées par l'objet, ni aux processus lancés par l'objet.

10. Définissez les paramètres de l'objet cible ou des processus cibles exécutés sur l'objet.


- **Processus cible.** Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, C:\Dir\File.exe ou Dir*.exe).
- **Hachage du processus cible.** Hachage du fichier.
- **Objet cible.** Commande pour lancer le processus cible. Saisissez la commande selon le modèle suivant `object://<commande>`, par exemple, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Vous pouvez également utiliser des masques comme `object://*C:\windows\temp*`.
- **Hachage de l'objet cible.** Hachage du fichier.

La règle du Contrôle évolutif des anomalies ne s'applique pas aux actions exécutées sur l'objet, ni sur processus exécutés sur l'objet.

11. Enregistrez vos modifications.

Exportation et importation d'exclusions pour les règles du Contrôle évolutif des anomalies

Pour exporter ou importer la liste des exclusions pour les règles sélectionnées, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Règles**, cliquez sur le bouton **Modifier les règles**.
La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Pour exporter la liste des règles, procédez comme suit :
 - a. Sélectionnez les règles dont vous souhaitez exporter les exceptions.
 - b. Cliquez sur le bouton **Exporter**.


- c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.
 - e. Cliquez sur le bouton **Enregistrer**.
5. Pour importer la liste des règles, procédez comme suit :
- a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
6. Enregistrez vos modifications.

Application des mises à jour pour les règles du Contrôle évolutif des anomalies

De nouvelles règles du Contrôle évolutif des anomalies peuvent être ajoutées au tableau de règles et des règles existantes peuvent être supprimées du tableau suite à la mise à jour des bases antivirus. Kaspersky Endpoint Security met en évidence les règles du Contrôle évolutif des anomalies à supprimer ou à ajouter dans le tableau si la mise à jour n'a pas été appliquée à ces règles.

Tant que la mise à jour n'est pas appliquée, Kaspersky Endpoint Security affiche les règles du Contrôle évolutif des anomalies supprimées suite à la mise à jour dans le tableau des règles et leur attribue l'état *Désactivé*. Il est impossible de modifier les paramètres de ces règles.

Pour appliquer les mises à jour aux règles du Contrôle évolutif des anomalies, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Règles**, cliquez sur le bouton **Modifier les règles**.
La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Confirmer les mises à jour**.
Le bouton **Confirmer les mises à jour** est accessible si la mise à jour pour les règles du Contrôle évolutif des anomalies est disponible.
5. Enregistrez vos modifications.

Modification des modèles de messages du Contrôle évolutif des anomalies

Quand l'utilisateur tente d'exécuter une action interdite par les règles de Contrôle évolutif des anomalies, Kaspersky Endpoint Security affiche un message sur le blocage des actions potentiellement dangereuses. Si l'utilisateur estime que le blocage n'a pas lieu d'être, il peut cliquer sur un lien dans la notification afin d'envoyer un message à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage des actions potentiellement dangereuses et pour les messages destinés à l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier le modèle de message, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle évolutif des anomalies :
 - **Blocage.** Modèle de message destiné à l'utilisateur et qui s'affiche en cas de déclenchement de la règle du Contrôle évolutif des anomalies qui bloque l'action atypique.
 - **Message à l'administrateur.** Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'action est intervenu par erreur.
4. Enregistrez vos modifications.

Consultation des rapports du Contrôle évolutif des anomalies

Pour consulter le rapport sur le fonctionnement du Contrôle évolutif des anomalies, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la section **Contrôles de sécurité**, choisissez la sous-section **Contrôle évolutif des anomalies**.
Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
6. Exécutez une des actions suivantes :
 - Si vous voulez consulter le rapport sur les paramètres des règles du Contrôle évolutif des anomalies, cliquez sur le bouton **Rapport sur l'état des règles**.
 - Si vous voulez consulter le rapport sur le déclenchement des règles du Contrôle évolutif des anomalies, cliquez sur le bouton **Rapport sur les déclenchements des règles**.

7. Le processus de création du rapport est lancé.

Le rapport s'ouvre dans une nouvelle fenêtre.

Contrôle des applications

Le Contrôle des applications contrôle le lancement des applications sur les ordinateurs des utilisateurs. Cela permet de mettre en œuvre la stratégie de sécurité de l'organisation dans le cadre de l'utilisation des applications. De plus, le Contrôle des applications réduit le risque d'infection de l'ordinateur en limitant l'accès aux applications.

La configuration du Contrôle des applications comprend les étapes suivantes :

1. [Création des catégories d'applications.](#)

L'administrateur crée des catégories d'application que l'administrateur souhaite administrer. Les catégories d'applications sont prévues pour tous les ordinateurs du réseau de l'organisation, quels que soient les groupes d'administration. Pour créer une catégorie, vous pouvez utiliser les critères suivants : catégorie KL (par exemple, *Navigateurs*), hachage du fichier, éditeurs d'applications, etc.

2. [Création de règles de Contrôle des applications.](#)

L'administrateur crée les règles de Contrôle des applications dans la stratégie pour le groupe d'administration. La règle inclut les catégories d'application et l'état du lancement des applications de ces catégories : interdit ou autorisé.

3. [Sélection du mode de fonctionnement du Contrôle des applications.](#)

L'administrateur choisit le mode d'utilisation des applications qui ne figurent dans aucune des règles (liste de refus et liste d'autorisation de l'application).

Lorsqu'un utilisateur tente de lancer une application interdite, Kaspersky Endpoint Security empêche le lancement de celle-ci et affiche une notification (cf. ill. ci-dessous).

Pour vérifier les paramètres du Contrôle des applications, utilisez le *mode de test*. Dans ce mode, Kaspersky Endpoint Security exécute les actions suivantes :

- il autorise le lancement des applications, y compris les applications interdites ;
- il affiche une notification concernant le lancement d'une application interdite et ajoute des informations dans le rapport sur l'ordinateur de l'utilisateur ;
- il envoie des données sur le lancement des applications interdites à Kaspersky Security Center.



Modes de fonctionnement du Contrôle des applications

Le module Contrôle des applications peut fonctionner selon deux modes :

- **Liste de refus.** Mode dans le cadre duquel le Contrôle des applications autorise les utilisateurs à lancer n'importe quelle application, sauf celles interdites dans les règles de Contrôle des applications.
Il s'agit du mode de fonctionnement du Contrôle des applications définies par défaut.
- **Liste d'autorisation.** Mode selon lequel le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception de celles autorisées et non interdites dans les règles de Contrôle des applications.

Si les règles d'autorisation de Contrôle des applications sont les plus strictes, le module interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

Vous pouvez prendre connaissance des [recommandations sur la configuration des règles du Contrôle des applications en mode de liste d'autorisation](#).

La configuration du Contrôle des applications pour le fonctionnement dans ces modes est possible à partir de l'interface locale de Kaspersky Endpoint Security ou via Kaspersky Security Center.

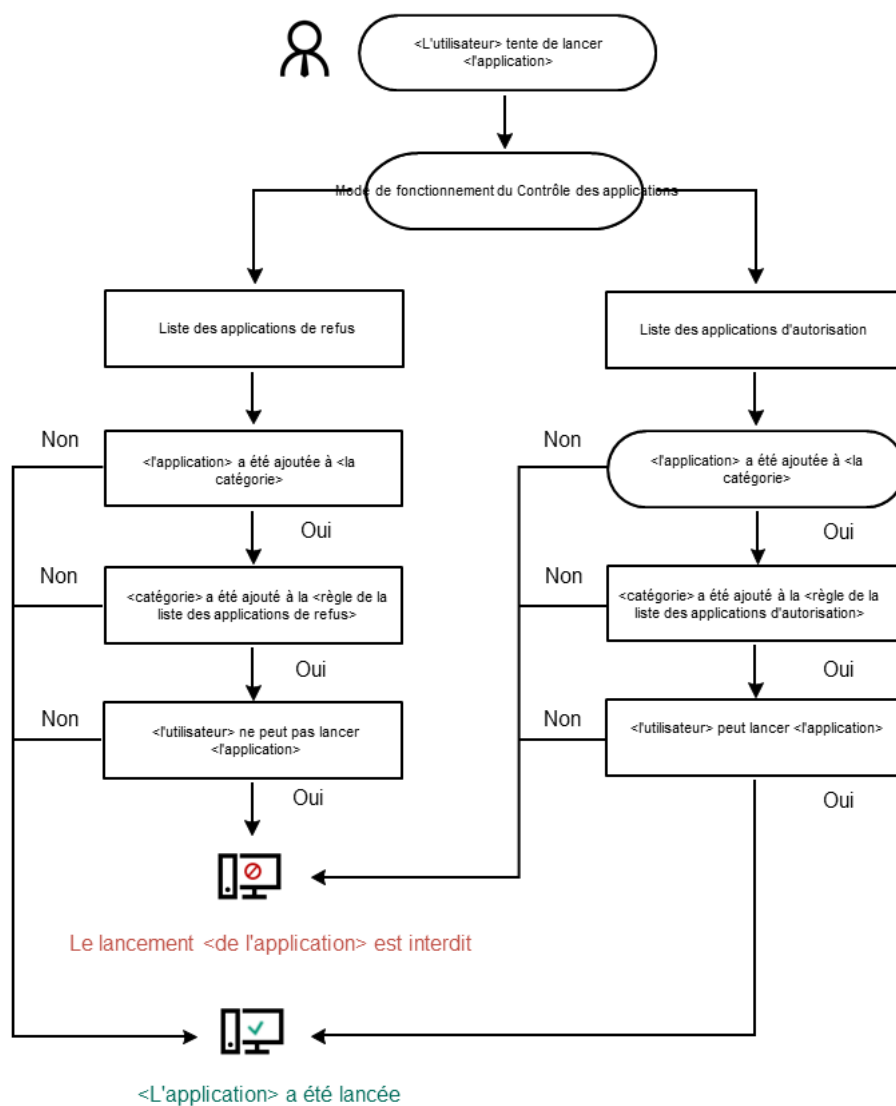
Ceci étant dit, Kaspersky Security Center propose des outils qui ne sont pas accessibles dans l'interface locale de Kaspersky Endpoint Security et qui sont indispensables pour réaliser les tâches suivantes :

- [Création des catégories d'applications](#).
Les règles de Contrôle des applications créées dans la Console d'administration de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.
- [Récupération des informations relatives aux applications installées sur les ordinateurs du réseau local de l'entreprise](#).

C'est pour cette raison qu'il est conseillé de configurer le fonctionnement du module Contrôle des applications via Kaspersky Security Center.

Algorithme de fonctionnement du Contrôle des applications

Kaspersky Endpoint Security utilise un algorithme pour décider de lancer ou non une application (cf. ill. ci-dessous).



Algorithme de fonctionnement du Contrôle des applications

Restrictions sur le fonctionnement du Contrôle des applications

Le fonctionnement du module Contrôle des applications est restreint dans les cas suivants :

- Lors de la mise à jour de la version de l'application, l'importation des paramètres du module Contrôle des applications n'est pas prise en charge.
- Lors de la mise à jour de la version de l'application, l'importation des paramètres du module Contrôle des applications est pris en charge uniquement lors de la mise à jour depuis la version Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes vers Kaspersky Endpoint Security 11.6.0 for Windows.

Lors de la mise à jour des versions de l'application différentes de Kaspersky Endpoint Security 10 Service Pack 2 for Windows, il faut à nouveau configurer les paramètres du module afin de rétablir son fonctionnement.

- En l'absence de connexion avec les serveurs de KSN, Kaspersky Endpoint Security reçoit les informations sur la réputation des applications et de leurs modules uniquement depuis des bases locales.

La liste des applications pour lesquelles Kaspersky Endpoint Security définit la catégorie KL **Applications de confiance selon la réputation dans KSN**, en présence d'une connexion avec les serveurs KSN, peut différer de la liste des applications pour lesquelles Kaspersky Endpoint Security définit la catégorie KL **Applications de confiance conformément à la réputation dans KSN** en l'absence d'une connexion à KSN.

- La base de données de Kaspersky Security Center peut contenir les informations sur 150 000 fichiers traités. Une fois que ce nombre d'enregistrements a été atteint, les nouveaux fichiers ne seront pas traités. Pour rétablir le fonctionnement de l'inventaire, il faut supprimer les fichiers repris dans la base de données de Kaspersky Security Center antérieurement suite à l'inventaire sur l'ordinateur doté de l'application Kaspersky Endpoint Security.
- Le module ne contrôle pas le lancement des scripts si le script est transmis à l'interprète par une méthode autre que la ligne de commande.

Si le lancement de l'interpréteur est autorisé par les règles du Contrôle des applications, le module ne bloque pas le script lancé via cet interpréteur.

Si le lancement d'au moins un des scripts indiqués dans la ligne de commande de l'interpréteur est bloqué par les règles de Contrôle des applications, le module bloque tous les scripts indiqués dans la ligne de commande de l'interpréteur.

- Le module ne contrôle pas le lancement des scripts depuis des interprètes qui ne sont pas pris en charge par l'application Kaspersky Endpoint Security.

Kaspersky Endpoint Security est compatible avec les interprètes suivants :

- Java ;
- PowerShell.

Les types d'interprète suivants sont pris en charge :


- %ComSpec%
- %SystemRoot%\system32\regedit.exe
- %SystemRoot%\regedit.exe
- %SystemRoot%\system32\regedt32.exe
- %SystemRoot%\system32\cscript.exe
- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe

- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Activation et désactivation du Contrôle des applications

Le Contrôle des application est désactivé par défaut.


Pour activer ou désactiver le Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Utilisez le commutateur **Contrôle des applications** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si le Contrôle des applications est activé, l'application transmet les informations concernant l'exécution des fichiers exécutables à Kaspersky Security Center. Vous pouvez consulter la liste des fichiers exécutables en cours d'exécution dans Kaspersky Security Center dans le dossier **Fichiers exécutables**. Pour recevoir des informations à propos de tous les fichiers exécutables plutôt que de les exécuter uniquement, exécutez la tâche [Inventaire](#).

Sélection du mode du Contrôle des applications

Pour sélectionner le mode du Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Dans le groupe **Mode de contrôle de démarrage de l'application**, choisissez l'une des options suivantes :

- **Liste de refus.** Si vous choisissez cette option, le Contrôle des applications permet à tous les utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'interdiction de Contrôle des applications.
- **Liste d'autorisation.** Si vous choisissez cette option, le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'autorisation de Contrôle des applications.

Les règles **Image d'or** et **Programmes de mise à jour de confiance** sont initialement définies pour le mode Liste d'autorisation. Ces règles du Contrôle des applications correspondent aux catégories KL. La catégorie KL "Image d'or" reprend les applications qui garantissent le fonctionnement normal du système d'exploitation. La catégorie KL "Programmes de mise à jour de confiance" reprend les programmes de mise à jour des applications des éditeurs les plus connus. Vous ne pouvez pas supprimer ces règles. Les paramètres de ces règles ne peuvent pas être modifiés. Par défaut, la règle **Système d'exploitation et ses modules** est activée tandis que la règle **Programmes de mise à jour de confiance** est désactivée. Le lancement des applications, correspondant aux conditions de déclenchement de ces règles, est autorisé pour tous les utilisateurs.

Toutes les règles créées dans le mode sélectionné sont enregistrées après le changement de mode afin de pouvoir les utiliser à nouveau. Pour revenir à l'utilisation de ces règles, il vous suffit de sélectionner le mode approprié.

4. Dans la section **Action au démarrage des applications bloquées**, choisissez l'action que le module devra exécuter si l'utilisateur tente de lancer une application interdite par les règles du Contrôle des applications.
5. Cochez la case **Contrôler le téléchargement des modules DLL** si vous voulez que l'application Kaspersky Endpoint Security contrôle le chargement des modules DLL lorsque les utilisateurs lancent des applications.

Les informations relatives au module et à l'application qui ont chargé ce module seront enregistrées dans le rapport.

Kaspersky Endpoint Security contrôle uniquement les modules DLL et les pilotes chargés à partir du moment où la case a été cochée. Redémarrez l'ordinateur après avoir coché la case si vous voulez que l'application Kaspersky Endpoint Security contrôle tous les modules DLL et les pilotes, y compris ceux qui se chargent avant le lancement de Kaspersky Endpoint Security.

Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Image d'or** ou toute autre règle qui contient la catégorie KL "Certificats de confiance" est activée dans les paramètres du Contrôle des applications et qu'elle garantit le chargement des modules DLL et des pilotes de confiance avant le lancement de Kaspersky Endpoint Security. L'activation du contrôle du chargement des modules DLL et des pilotes lorsque la règle **Image d'or** est désactivée peut provoquer l'instabilité du système d'exploitation.

Il est recommandé d'[activer la protection par mot de passe](#) de la configuration des paramètres de l'application afin de pouvoir désactiver les règles d'interdiction qui bloquent le lancement de modules DLL et de pilotes critiques sans modifier les paramètres de la stratégie de Kaspersky Security Center.

6. Enregistrez vos modifications.

Utilisation des règles du Contrôle des applications dans l'interface de l'application

Kaspersky Endpoint Security utilise des règles pour contrôler le lancement des applications par l'utilisateur. La règle du Contrôle des applications contient les conditions de déclenchement et l'action exécutée par le module Contrôle des applications en cas de déclenchement de la règle (autoriser ou non les utilisateurs à démarrer l'application).

Condition de déclenchement de la règle

Une condition déclenchant une règle présente la corrélation suivante : "type de condition – critère de condition – valeur de la condition". Sur la base des conditions de déclenchement de la règle Kaspersky Endpoint Security applique ou non la règle à l'application.

Les règles utilisent les types de conditions suivantes :

- *Conditions d'inclusion.* Kaspersky Endpoint Security applique la règle à l'application si l'application remplit au moins une des conditions d'inclusion.
- *Conditions d'exclusion.* Kaspersky Endpoint Security n'applique pas la règle à l'application si l'application remplit au moins une des conditions d'exclusion ou ne remplit aucune des conditions d'inclusion.

Les conditions de déclenchement de la règle sont définies à l'aide de critères. Les critères suivants interviennent dans la composition des conditions dans Kaspersky Endpoint Security :

- chemin d'accès au dossier contenant le fichier exécutable de l'application ou le chemin d'accès au fichier exécutable de l'application ;
- métadonnées : nom du fichier exécutable de l'application, version du fichier exécutable de l'application, nom de l'application, version de l'application, éditeur de l'application ;
- hachage du fichier exécutable de l'application ;
- certificat : éditeur, le sujet, empreinte ;
- appartenance de l'application à une catégorie KL ;
- emplacement du fichier exécutable de l'application sur le disque amovible.

Il faut définir la valeur de chaque critère utilisé dans une condition. Si les paramètres de l'application lancée correspondent aux valeurs des critères repris dans les conditions d'inclusion, la règle se déclenche. Dans ce cas, le Contrôle des applications exécute l'action définie dans la règle. Si les paramètres de l'application correspondent aux valeurs des critères repris dans les conditions d'exclusion, le Contrôle des applications ne contrôle pas le lancement de l'application.

Décisions du Contrôle des applications en cas de déclenchement de la règle

En cas de déclenchement de la règle, le Contrôle des applications, conformément à la règle établie, permet ou non à l'utilisateur (ou à un groupe d'utilisateurs) de lancer l'application. Vous pouvez sélectionner des utilisateurs individuels ou des groupes d'utilisateurs autorisés ou non à lancer les applications qui déclenchent la règle.

Si la règle ne désigne aucun utilisateur autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'interdiction*.

Si la règle ne désigne aucun utilisateur non autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'autorisation*.

Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Par exemple, si une règle d'autorisation de Contrôle des applications a été définie pour un groupe d'utilisateurs et qu'un des membres de ce groupe est soumis à une règle d'interdiction de Contrôle des applications, ce membre n'est pas autorisé à exécuter l'application.


État de fonctionnement de la règle

Les règles de Contrôle des applications peuvent avoir un des états de fonctionnement suivant :

- **Activé.** Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
- **Désactivé.** Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.
- **Test.** L'état signifie que Kaspersky Endpoint Security autorise le lancement des applications soumises à la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

Ajout d'une règle du Contrôle des applications

Pour ajouter ou modifier une règle de Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Cliquez sur le bouton **Applications bloquées** ou **Applications autorisées**.
Cette action permet d'ouvrir la liste des règles du Contrôle des applications.
4. Cliquez sur le bouton **Ajouter**.
La fenêtre **Règle de Contrôle des applications** s'ouvre.
5. Sous l'onglet **Paramètres généraux**, définissez les principaux paramètres de la règle :
 - a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.
 - b. Dans le champ **Description**, saisissez une description de la règle.
 - c. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés ou non à lancer les applications qui répondent aux conditions de déclenchement de la règle. Pour ce faire, cliquez sur le bouton **Ajouter** dans le tableau **Sujets et leurs droits**.
La valeur **Tous** est ajoutée par défaut à la liste des utilisateurs. La règle s'applique à tous les utilisateurs.

Si aucun utilisateur n'est repris dans le tableau, la règle ne peut pas être enregistrée.

- d. Dans le tableau **Sujets et leurs droits**, utilisez le commutateur pour définir le droit des utilisateurs à lancer des applications.

- e. Cochez la case **Interdire aux autres utilisateurs** si vous voulez que l'application interdise le lancement des applications qui répondent aux conditions du fonctionnement de la règle à tous les utilisateurs qui ne figurent pas dans la colonne **Objet** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans la colonne **Objet**.

Si la case **Interdire aux autres utilisateurs** est décochée, Kaspersky Endpoint Security ne contrôle pas le lancement des applications par les utilisateurs qui ne figurent pas dans le tableau **Sujets et leurs droits** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans le tableau **Sujets et leurs droits**.

- f. Cochez la case **Programmes de mise à jour de confiance** si vous souhaitez que les applications qui répondent aux conditions de déclenchement de la règle soient considérées comme des applications de mise à jour de confiance par Kaspersky Endpoint Security et qu'il les autorise à créer d'autres fichiers exécutable dont le lancement sera autorisé à l'avenir.

6. Sous l'onglet **Conditions**, [créez](#) ou modifiez la liste des conditions d'inclusion permettant de déclencher la règle.


7. Sous l'onglet **Exclusions**, créez ou modifiez la liste des conditions d'exclusions permettant de déclencher la règle.

Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutable créés par les programmes de mise à jour de confiance migre également.

8. Enregistrez vos modifications.

Ajout d'une condition de déclenchement de la règle de Contrôle des applications

Pour ajouter une nouvelle condition de déclenchement à la règle de Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Cliquez sur le bouton **Applications bloquées** ou **Applications autorisées**.
Cette action permet d'ouvrir la liste des règles du Contrôle des applications.
4. Sélectionnez la règle pour laquelle vous souhaitez configurer une condition de déclenchement.
Les propriétés de la règle du Contrôle des applications s'ouvrent.
5. Sélectionnez l'onglet **Conditions** ou **Exclusions** et cliquez sur le bouton **Ajouter**.
6. Sélectionnez les conditions de déclenchement de la règle du Contrôle des applications :
 - **Conditions à partir des propriétés des applications lancées**. Dans la liste des applications en cours d'exécution, vous pouvez sélectionner les applications auxquelles la règle du Contrôle des applications sera appliquée. Kaspersky Endpoint Security fournit également une liste des applications qui étaient exécutées auparavant sur l'ordinateur. Vous devez sélectionner le critère que vous souhaitez utiliser pour créer une ou plusieurs conditions de déclenchement de la règle : **Hachage du fichier**, **Certificat**, **Catégorie KL**, **Métadonnées** ou **Chemin d'accès au dossier**.

- **Conditions "Catégorie KL".** Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe® Acrobat® et d'autres.
- **Condition manuelle.** Vous pouvez sélectionner le fichier d'application et choisir une des conditions de déclenchement de la règle : **Hachage du fichier**, **Certificat**, **Métadonnées** ou **Chemin d'accès au fichier ou au dossier**.
- **Condition par lecteur de fichiers (lecteur amovible).** La règle du Contrôle des applications s'applique uniquement aux fichiers qui sont exécutés sur un disque amovible.
- **Conditions à partir des propriétés du fichier du dossier indiqué.** La règle du Contrôle des applications s'applique uniquement aux fichiers qui figurent dans le dossier indiqué. Vous pouvez également inclure ou exclure des fichiers de sous-dossiers. Vous devez sélectionner le critère que vous souhaitez utiliser pour créer une ou plusieurs conditions de déclenchement de la règle : **Hachage du fichier**, **Certificat**, **Catégorie KL**, **Métadonnées** ou **Chemin d'accès au dossier**.


7. Enregistrez vos modifications.

Lorsque vous ajoutez des conditions, veuillez tenir compte des considérations particulières suivantes pour le Contrôle des applications :

- Kaspersky Endpoint Security ne prend pas en charge l'hachage MD5 du fichier et ne contrôle pas le lancement des applications sur la base de l'hachage MD5. Le hachage SHA256 fait office de condition de déclenchement de la règle.
- Il est déconseillé d'utiliser uniquement **Éditeur** et **Objet** en tant que condition de déclenchement des règles. L'utilisation de ces critères n'est pas fiable.
- Si vous utilisez un lien symbolique dans le champ **Chemin d'accès au fichier ou au dossier**, il est conseillé de développer le lien symbolique pour garantir le bon fonctionnement de la règle de Contrôle du lancement des applications. Pour ce faire, cliquez sur le bouton **Résoudre le lien symbolique**.

Modification de l'état de la règle de Contrôle des applications

Pour modifier l'état de la règle de Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Cliquez sur le bouton **Applications bloquées** ou **Applications autorisées**.
Cette action permet d'ouvrir la liste des règles du Contrôle des applications.
4. Dans la colonne **État**, ouvrez le menu contextuel et sélectionnez un des éléments suivants :
 - **Activé.** Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
 - **Désactivé.** Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.

- **Test.** L'état signifie que Kaspersky Endpoint Security autorise toujours le lancement des applications soumises à cette règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

5. Enregistrez vos modifications.

Gestion des règles du Contrôle des applications dans Kaspersky Security Center

Kaspersky Endpoint Security utilise des règles pour contrôler le lancement des applications par l'utilisateur. La règle du Contrôle des applications contient les conditions de déclenchement et l'action exécutée par le module Contrôle des applications en cas de déclenchement de la règle (autoriser ou non les utilisateurs à démarrer l'application).

Condition de déclenchement de la règle

Une condition déclenchant une règle présente la corrélation suivante : "type de condition – critère de condition – valeur de la condition". Sur la base des conditions de déclenchement de la règle Kaspersky Endpoint Security applique ou non la règle à l'application.

Les règles utilisent les types de conditions suivantes :

- *Conditions d'inclusion.* Kaspersky Endpoint Security applique la règle à l'application si l'application remplit au moins une des conditions d'inclusion.
- *Conditions d'exclusion.* Kaspersky Endpoint Security n'applique pas la règle à l'application si l'application remplit au moins une des conditions d'exclusion ou ne remplit aucune des conditions d'inclusion.

Les conditions de déclenchement de la règle sont définies à l'aide de critères. Les critères suivants interviennent dans la composition des conditions dans Kaspersky Endpoint Security :

- chemin d'accès au dossier contenant le fichier exécutable de l'application ou le chemin d'accès au fichier exécutable de l'application ;
- métadonnées : nom du fichier exécutable de l'application, version du fichier exécutable de l'application, nom de l'application, version de l'application, éditeur de l'application ;
- hachage du fichier exécutable de l'application ;
- certificat : éditeur, le sujet, empreinte ;
- appartenance de l'application à une catégorie KL ;
- emplacement du fichier exécutable de l'application sur le disque amovible.

Il faut définir la valeur de chaque critère utilisé dans une condition. Si les paramètres de l'application lancée correspondent aux valeurs des critères repris dans les conditions d'inclusion, la règle se déclenche. Dans ce cas, le Contrôle des applications exécute l'action définie dans la règle. Si les paramètres de l'application correspondent aux valeurs des critères repris dans les conditions d'exclusion, le Contrôle des applications ne contrôle pas le lancement de l'application.

Décisions du Contrôle des applications en cas de déclenchement de la règle

En cas de déclenchement de la règle, le Contrôle des applications, conformément à la règle établie, permet ou non à l'utilisateur (ou à un groupe d'utilisateurs) de lancer l'application. Vous pouvez sélectionner des utilisateurs individuels ou des groupes d'utilisateurs autorisés ou non à lancer les applications qui déclenchent la règle.

Si la règle ne désigne aucun utilisateur autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'interdiction*.

Si la règle ne désigne aucun utilisateur non autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'autorisation*.

Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Par exemple, si une règle d'autorisation de Contrôle des applications a été définie pour un groupe d'utilisateurs et qu'un des membres de ce groupe est soumis à une règle d'interdiction de Contrôle des applications, ce membre n'est pas autorisé à exécuter l'application.

État de fonctionnement de la règle

Les règles de Contrôle des applications peuvent avoir un des états de fonctionnement suivant :

- **Activé.** Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
- **Désactivé.** Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.

Test. L'état signifie que Kaspersky Endpoint Security autorise le lancement des applications soumises à la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

Récupération des informations relatives aux applications installées sur les ordinateurs des utilisateurs

Pour créer des règles optimales pour le Contrôle des applications, il est conseillé de s'informer sur les applications utilisées par les ordinateurs du réseau local de l'entreprise. Pour ce faire, vous pouvez obtenir les informations suivantes :

- les éditeurs, les versions et les localisations des applications utilisées dans le réseau local de l'entreprise ;
- la fréquence des mises à jour des applications ;
- les stratégies d'utilisation des applications adoptées dans l'entreprise (il peut s'agir de stratégies de sécurité ou de stratégies d'administration) ;
- l'emplacement des stockages des distributions des applications.

Pour récupérer les informations relatives aux applications utilisées sur les ordinateurs du réseau local de l'entreprise, vous devez utiliser les données présentées dans les dossiers **Registre des applications** et **Fichiers exécutables**. Les dossiers **Registre des applications** et **Fichiers exécutables** font partie du dossier **Administration des applications** de l'arborescence de la Console d'administration de Kaspersky Security Center.

Le dossier **Registre des applications** contient la liste des applications détectées sur les postes clients par l'[Agent d'administration](#) installé sur ces postes.

Le dossier **Fichiers exécutables** contient la liste des fichiers exécutables lancés à un moment ou l'autre sur les postes clients ou détectés pendant l'exécution de la tâche d'inventaire pour Kaspersky Endpoint Security.

Après avoir ouvert la fenêtre des propriétés de l'application sélectionnée dans le dossier **Registre des applications** ou **Fichiers exécutables**, vous pouvez obtenir les informations générales sur l'application ou sur ses fichiers exécutables ainsi que consulter la liste des ordinateurs sur lesquels cette application est installée.

*Pour ouvrir la fenêtre des propriétés de l'application dans le dossier **Registre des applications**, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez **Avancé** → **Administration des applications** → **Registre des applications**.
3. Sélectionnez l'application.
4. Dans le menu contextuel de l'application, sélectionnez l'option **Propriétés**.

*Pour ouvrir la fenêtre des propriétés du fichier exécutable dans le dossier **Fichiers exécutables**, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Administration des applications** → **Fichiers exécutables**.
3. Choisissez le fichier exécutable.
4. Dans le menu contextuel du fichier exécutable, sélectionnez l'option **Propriétés**.

Création des catégories d'applications

Pour simplifier la création de règles de Contrôle des applications, vous pouvez créer des catégories d'applications.

Il est conseillé de créer une catégorie "Applications pour le travail" qui reprend la sélection standard d'applications utilisées dans l'entreprise. Si différents groupes d'utilisateurs utilisent différentes sélections d'applications, vous pouvez créer une catégorie d'applications distincte pour chaque groupe d'utilisateurs.

Pour créer une catégorie d'applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Administration des applications** → **Catégories d'applications**.
3. Dans la zone de travail, cliquez sur **Créer une catégorie**.
L'Assistant de création de catégories personnalisée s'ouvre.
4. Suivez les instructions de l'Assistant de création de catégories personnalisées.

Étape 1. Sélection du type de catégorie

Cette étape permet de choisir un des types suivants de catégories d'applications :

- **Catégorie enrichie manuellement.** Si vous avez choisi ce type de catégorie, vous pouvez définir à l'étape "Configuration des conditions d'inclusion des applications dans une catégorie" et à l'étape "Configuration des conditions d'exclusion des applications hors d'une catégorie" les critères selon lesquels les fichiers exécutables sont repris dans la catégorie.
- **Catégorie qui contient les fichiers exécutables des appareils sélectionnés.** Si vous avez choisi ce type de catégorie, vous pourrez à l'étape "Paramètres" désigner l'ordinateur dont les fichiers exécutables seront automatiquement repris dans la catégorie.
- **Catégorie qui contient les fichiers exécutables du dossier sélectionné.** Si vous avez choisi ce type de catégorie, vous pourrez à l'étape "Dossier de stockage" désigner le dossier dont les fichiers exécutables seront repris automatiquement dans la catégorie.

Lors de la création de la catégorie enrichie automatiquement, Kaspersky Security Center réalise l'inventaire des formats de fichiers suivants : EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX et SCR.

Étape 2. Saisie du nom de la catégorie personnalisée

Indiquez à cette étape le nom de la catégorie d'applications.

Étape 3. Configuration des conditions d'inclusion des applications dans une catégorie

Cette étape n'est pas proposée si vous avez choisi le type de catégorie **Catégorie enrichie manuellement**.

À cette étape, dans la liste déroulante **Ajouter**, sélectionnez une des conditions suivantes d'inclusion des applications dans la catégorie :

- **De la liste des fichiers exécutables.** Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.
- **Des propriétés du fichier.** Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Métadonnées des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les métadonnées de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Hachage des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les hachages de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Certificats des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables signés par les certificats. Kaspersky Security Center désigne les certificats de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.

Il est déconseillé d'utiliser les conditions dont les propriétés ne définissent pas le paramètre **Empreinte du certificat**.

- **Métadonnées des fichiers de l'installateur MSI.** Sélectionnez le paquet MSI. Kaspersky Security Center désigne les métadonnées des fichiers exécutables contenus dans le paquet MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Sommes de contrôle des fichiers du programme d'installation mis de l'application.** Sélectionnez le paquet MSI. Kaspersky Security Center désigne les hachages des fichiers exécutables contenus dans ce paquet MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Catégorie KL.** Indiquez la catégorie KL en tant que condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.
Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.
- **Chemin d'accès à l'application.** Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.
- **Certificats du stockage de certificats.** Sélectionnez les certificats utilisés pour signer les fichiers exécutables en guise de condition d'ajout des applications à la catégorie personnalisée.

Il est déconseillé d'utiliser les conditions dont les propriétés ne définissent pas le paramètre **Empreinte du certificat**.

- **Type de support.** Indiquez le type d'appareil de stockage (tous les disques durs et les disques amovibles ou uniquement les disques amovibles) en tant que condition d'ajout des applications à la catégorie utilisateur.

Étape 4. Configuration des conditions d'exclusions des applications hors d'une catégorie

Cette étape n'est pas proposée si vous avez choisi le type de catégorie **Catégorie enrichie manuellement**.

Les applications renseignées à cette étape sont exclues de la catégorie, même si ces applications avaient été renseignées à l'étape "Configuration des conditions d'inclusion des applications dans une catégorie".

À cette étape, dans la liste déroulante **Ajouter**, sélectionnez une des conditions d'exclusion des applications hors de la catégorie :

- **De la liste des fichiers exécutables.** Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.
- **Des propriétés du fichier.** Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Métadonnées des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les métadonnées de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.

- **Hachage des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les hachages de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Certificats des fichiers du dossier.** Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables signés par les certificats. Kaspersky Security Center désigne les certificats de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Métadonnées des fichiers de l'installateur MSI.** Sélectionnez le paquet MSI. Kaspersky Security Center désigne les métadonnées des fichiers exécutables contenus dans le paquet MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Sommes de contrôle des fichiers du programme d'installation mis de l'application.** Sélectionnez le paquet MSI. Kaspersky Security Center désigne les hachages des fichiers exécutables contenus dans ce paquet MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Catégorie KL.** Indiquez la catégorie KL en tant que condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.
Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.
- **Chemin d'accès à l'application.** Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.
- **Certificats du stockage de certificats.** Sélectionnez les certificats utilisés pour signer les fichiers exécutables en guise de condition d'ajout des applications à la catégorie personnalisée.
- **Type de support.** Indiquez le type d'appareil de stockage (tous les disques durs et les disques amovibles ou uniquement les disques amovibles) en tant que condition d'ajout des applications à la catégorie utilisateur.

Étape 5. Paramètres

Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui contient les fichiers exécutables des appareils sélectionnés**.

À cette étape, cliquez sur le bouton **Ajouter** et indiquez les ordinateurs dont les fichiers exécutables vont être ajoutés par Kaspersky Security Center à la catégorie d'applications. Kaspersky Security Center ajoute à la catégorie d'applications tous les fichiers exécutables des ordinateurs indiqués et repris dans le dossier [Fichiers exécutables](#).

Cette étape permet également de configurer les paramètres suivants :

- algorithme de calcul de l'hachage par l'application Kaspersky Security Center. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :
 - **Calculer SHA-256 pour les fichiers de la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows versions ultérieures).**
 - **Calculer MD5 pour les fichiers de la catégorie (pris en charge dans les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**
- la case **Synchronisation des données avec le stockage du Serveur d'administration**. Cochez cette case si vous voulez que Kaspersky Security Center nettoie périodiquement la catégorie d'applications et y ajoute tous

les fichiers exécutables des ordinateurs indiqués présentés dans le dossier **Fichiers exécutables**.

Si la case **Synchronisation des données avec le stockage du Serveur d'administration** est décochée, Kaspersky Security Center ne va pas modifier la catégorie d'applications après sa création.

- Champ **Période d'analyse (h)**. Ce champ permet de définir le délai, en heures, à l'issue duquel Kaspersky Security Center nettoie la catégorie d'applications et y ajoute tous les fichiers exécutables des ordinateurs qui figurent dans le dossier **Fichiers exécutables**.

Le champ est accessible quand la case **Synchronisation des données avec le stockage du Serveur d'administration** est cochée.

Étape 6. Dossier du stockage

Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui contient les fichiers exécutables du dossier sélectionné**.

Dans le cadre de cette étape, cliquez sur le bouton **Parcourir** et indiquez le dossier dans lequel Kaspersky Security Center doit exécuter la recherche de fichiers exécutables en vue d'un ajout automatique à la catégorie d'applications.

Cette étape permet également de configurer les paramètres suivants :

- La case **Inclure les bibliothèques de liens dynamiques (DLL) dans la catégorie**. Cochez cette case si vous souhaitez que les bibliothèques de liens dynamiques (fichiers DLL) soient incluses dans la catégorie d'applications.

Lorsque des fichiers DLL sont ajoutés à une catégorie d'applications, il se peut que les performances de Kaspersky Security Center diminuent.

- Case **Inclure les données sur les scripts dans la catégorie**. Cochez cette case si vous souhaitez que les scripts soient inclus dans la catégorie d'applications.

Lorsque les scripts sont ajoutés à une catégorie d'applications, il se peut que les performances de Kaspersky Security Center diminuent.

- algorithme de calcul de l'hachage par l'application Kaspersky Security Center. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :

- **Calculer SHA-256 pour les fichiers de la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows versions ultérieures)**.
- **Calculer MD5 pour les fichiers de la catégorie (pris en charge dans les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- la case **Forcer la recherche de modifications dans le dossier**. Cochez cette case si vous voulez que Kaspersky Security Center recherche à intervalle régulier des fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications.

Si la case **Forcer la recherche de modifications dans le dossier** est décochée, Kaspersky Security Center recherche des fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications uniquement en cas de modification, d'ajout ou de suppression de fichiers dans ce dossier.

- Champ **Période d'analyse (h)**. Ce champ permet de définir, en heures, la période à l'issue de laquelle Kaspersky Security Center recherche la présence de fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications.

Le champ est accessible si la case **Forcer la recherche de modifications dans le dossier** est cochée.

Étape 7. Création d'une catégorie personnalisée

Pour quitter l'Assistant d'installation de l'application, cliquez sur **Terminer**.

Ajout à une catégorie d'applications de fichiers exécutables issus du dossier Fichiers exécutables

Le dossier **Fichiers exécutables** affiche la liste des fichiers exécutables détectés sur les ordinateurs. Kaspersky Endpoint Security compose la liste des fichiers exécutables après l'exécution de la tâche d'inventaire.

*Pour ajouter des fichiers du dossier **Fichiers exécutables** à la catégorie d'applications, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez **Avancé** → **Administration des applications** → **Fichiers exécutables**.
3. Dans l'espace de travail, choisissez les fichiers exécutables que vous voulez ajouter à la catégorie d'applications.
4. Cliquez-droit pour ouvrir le menu contextuel des fichiers exécutable sélectionnés et sélectionnez l'option **Ajouter à la catégorie**.

La fenêtre **Sélectionnez la catégorie d'applications** s'ouvre.

5. Dans la fenêtre **Choisissez la catégorie des applications**, procédez comme suit :
 - Choisissez dans la partie supérieure de la fenêtre une des options suivantes :
 - **Créer une catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.
 - **Ajouter les règles à la catégorie indiquée**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.
 - Dans le groupe **Type de la règle**, sélectionnez une des options suivantes :
 - **Ajouter aux règles d'inclusion**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.
 - **Ajouter aux règles d'exclusion**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.
 - Dans le groupe **Type d'informations sur le fichier**, choisissez une des options suivantes :
 - **Données du certificat (ou SHA-256 pour les fichiers sans certificat)**.
 - **Données du certificat (les fichiers sans certificat sont ignorés)**.

- Uniquement SHA-256 (les fichiers sans SHA-256 sont ignorés).
- Uniquement MD5 (pour la compatibilité avec Kaspersky Endpoint Security 10 Service Pack 1).

6. Cliquez sur le bouton OK.

Ajout à une catégorie d'applications de fichiers exécutables liés à des événements

Pour ajouter à la catégorie d'applications des fichiers exécutables associés aux événements du module Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.
3. Choisissez la sélection d'événements relatives au fonctionnement du module Contrôle des applications ([Consultation des événements à l'issue du fonctionnement du module Contrôle des applications](#), [Consultation des événements à l'issue du fonctionnement d'essai du module Contrôle des applications](#)) dans la liste déroulante **Événements de la sélection**.
4. Cliquez sur le bouton **Lancer la sélection**.
5. Choisissez les événements associés aux fichiers exécutables que vous souhaitez ajouter à la catégorie d'applications.
6. Cliquez-droit pour ouvrir le menu contextuel des événements sélectionnés et choisissez l'option **Ajouter à la catégorie**.

La fenêtre **Sélectionnez la catégorie d'applications** s'ouvre.

7. Dans la fenêtre **Choisissez la catégorie des applications**, procédez comme suit :
 - Choisissez dans la partie supérieure de la fenêtre une des options suivantes :
 - **Créer une catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.
 - **Ajouter les règles à la catégorie indiquée**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.
 - Dans le groupe **Type de la règle**, sélectionnez une des options suivantes :
 - **Ajouter aux règles d'inclusion**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.
 - **Ajouter aux règles d'exclusion**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.
 - Dans le groupe **Type d'informations sur le fichier**, choisissez une des options suivantes :
 - **Données du certificat (ou SHA-256 pour les fichiers sans certificat)**.

- **Données du certificat (les fichiers sans certificat sont ignorés).**
- **Uniquement SHA-256 (les fichiers sans SHA-256 sont ignorés).**
- **Uniquement MD5 (pour la compatibilité avec Kaspersky Endpoint Security 10 Service Pack 1).**

8. Cliquez sur le bouton **OK**.

Ajout et modification des règles de Contrôle des applications à l'aide de Kaspersky Security Center

Pour ajouter ou modifier une règle de Contrôle des applications à l'aide de Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.
Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
6. Exécutez une des actions suivantes :
 - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
 - Pour modifier une règle existante, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

La fenêtre **Règle de Contrôle des applications** s'ouvre.

7. Exécutez une des actions suivantes :
 - Si vous voulez créer une catégorie, procédez comme suit :
 - a. Cliquez sur le bouton **Créer une catégorie**.
L'Assistant de création de catégories personnalisée s'ouvre.
 - b. Suivez les instructions de l'Assistant de création de catégories personnalisées.
 - c. De la liste déroulante **Catégorie**, choisissez la catégorie d'applications créée.
 - Si vous voulez modifier une catégorie existante, procédez comme suit :
 - a. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée que vous voulez modifier.
 - b. Cliquez sur le bouton **Propriétés**.
La fenêtre **Propriétés <nom de la catégorie>** s'ouvre.

c. Modifier les paramètres de la catégories d'applications sélectionnée.

d. Cliquez sur le bouton **OK**.

e. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée sur la base de laquelle vous souhaitez créer la règle.

8. Cliquez sur le bouton **Ajouter** dans le tableau **Sujets et leurs droits**.

La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

9. Dans la fenêtre **Sélectionnez Utilisateurs ou Groupes**, composez la liste des utilisateurs et/ou des groupes d'utilisateurs que vous souhaitez autoriser à lancer les applications qui appartiennent à la catégorie sélectionnée.

10. Dans le tableau **Sujets et leurs droits**, réalisez les opérations suivantes :

- Si vous voulez permettre aux utilisateurs et/ou aux groupes d'utilisateurs de lancer des applications qui appartiennent à la catégorie sélectionnée, cochez la case **Autoriser** sur les lignes requises.
- Si vous voulez interdire aux utilisateurs et/ou aux groupes d'utilisateurs de lancer des applications qui appartiennent à la catégorie sélectionnée, cochez la case **Interdire** sur les lignes requises.

11. Cochez la case **Interdire aux autres utilisateurs** si vous voulez que l'application interdise le lancement des applications, appartenant à la catégorie choisie à tous les utilisateurs qui ne figurent pas dans la colonne **Objet** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans la colonne **Objet**.

12. Cochez la case **Programmes de mise à jour de confiance** si vous souhaitez que les qui appartiennent à la catégories d'applications sélectionnée soient considérées comme des applications de mise à jour de confiance par Kaspersky Endpoint Security et qu'il les autorise à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.

Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutables créés par les programmes de mise à jour de confiance migre également.

13. Enregistrez vos modifications.

Modification de l'état de la règle de Contrôle des applications via Kaspersky Security Center

Pour modifier l'état de la règle de Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.

Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

6. Dans la colonne **État**, cliquez-gauche pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :

- **Activé.** Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
- **Désactivé.** Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.
- **Test.** L'état signifie que Kaspersky Endpoint Security autorise toujours le lancement des applications soumises à la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

L'état **Test** permet de désigner l'[action semblable à l'option Tester les règles](#) pour une partie des règles quand l'option **Appliquer les règles** a été choisie dans la liste déroulante **Action**.

7. Enregistrez vos modifications.

Exportation et importation de règles du Contrôle des applications

Vous pouvez exporter la liste des règles du Contrôle des applications dans un fichier XML. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles du Contrôle des applications ou pour procéder à la migration de la liste vers un autre serveur.

Lorsque vous exportez et importez des règles du Contrôle des applications, veuillez garder à l'esprit les points particuliers suivants :

- Kaspersky Endpoint Security exporte la liste des règles uniquement pour le mode actif du Contrôle des applications. Autrement dit, si le Contrôle des applications fonctionne en mode de liste de refus, Kaspersky Endpoint Security exporte des règles uniquement pour ce mode. Pour exporter la liste des règles pour le mode de liste d'autorisation, vous devez changer de mode et relancer l'opération d'exportation.
- Kaspersky Endpoint Security utilise des catégories d'applications pour que les règles du Contrôle des applications fonctionnent. Lorsque vous procédez à la migration de la liste des règles du Contrôle des applications vers un autre serveur, vous devez également migrer la liste des catégories d'applications. Pour en savoir plus sur l'exportation ou l'importation de catégories d'applications, *veuillez consulter l'[aide de Kaspersky Security Center](#)*.

[Comment exporter et importer une liste de règles du Contrôle des applications dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.
6. Pour exporter la liste des règles du Contrôle des applications, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.
Si vous n'avez sélectionné aucune règle, Kaspersky Endpoint Security exportera toutes les règles.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des règles et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.
7. Pour exporter une liste de règles du Contrôle des applications, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

[Comment exporter et importer une liste de règles du Contrôle des applications dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer la liste des règles.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôles de sécurité** → **Contrôle des applications**.
5. Cliquez sur le lien **Paramètres des listes de règles**.
6. Sélectionnez une liste de règles : liste de refus ou liste d'autorisation d'application.
7. Pour exporter la liste des règles du Contrôle des applications, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les règles sélectionnées ou exporter la liste complète.
 - d. Cliquez sur le bouton **Exporter**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML dans le dossier des téléchargements par défaut.
8. Pour exporter une liste de règles du Contrôle des applications, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
9. Enregistrez vos modifications.

Test des règles de Contrôle des applications via Kaspersky Security Center

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles. Quand le test des règles de Contrôle des applications est activé, Kaspersky Endpoint Security ne bloque pas les applications dont le lancement est interdit par le Contrôle des applications, mais envoie des notifications de lancement au Serveur d'administration.

Pour analyser le fonctionnement des règles de Contrôle des applications, il faut étudier les événements sur la base des résultats du fonctionnement du module Contrôle des applications survenus dans Kaspersky Security Center. Si aucune des applications indispensables au travail de l'utilisateur de l'ordinateur n'affiche des événements d'interdiction de lancement en mode test, les règles créées sont correctes. Dans le cas contraire, il est conseillé de préciser les paramètres des règles que vous avez créées, de créer des règles complémentaires ou de supprimer des règles existantes.

Par défaut, Kaspersky Endpoint Security permet de lancer toutes les applications à l'exception des applications interdites par les règles.

Pour activer ou désactiver le test des règles de Contrôle des applications dans Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.
Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
6. Dans la liste déroulante **Mode de contrôle** choisissez une des options suivantes :
 - **Liste de refus**. Si vous choisissez cette option, le Contrôle des applications permet à tous les utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'interdiction de Contrôle des applications.
 - **Liste d'autorisation**. Si vous choisissez cette option, le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'autorisation de Contrôle des applications.
7. Exécutez une des actions suivantes :
 - Si vous voulez activer les tests pour les règles de Contrôle des applications, choisissez l'option **Tester les règles** dans la liste déroulante **Action**.
 - Si vous voulez activer le Contrôle des applications pour l'administration du lancement des applications sur les ordinateurs des utilisateurs, choisissez l'option **Appliquer les règles** dans la liste déroulante **Action**.
8. Enregistrez vos modifications.

Consultation des événements à l'issue du fonctionnement d'essai du module Contrôle des applications

Pour consulter les événements survenus dans Kaspersky Security Center à l'issue de l'essai du module Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.
3. Cliquez sur le bouton **Créer une sélection**.
La fenêtre **Propriétés <nom de la sélection>** s'ouvre.
4. Ouvrez la section **Événements**.
5. Cliquez sur le bouton **Tout désélectionner**.
6. Dans le tableau **Événements**, cochez les cases **Lancement de l'application interdit en mode test** et **Lancement de l'application autorisé en mode test**.
7. Cliquez sur le bouton **OK**.
8. Dans la liste déroulante **Événements de la sélection**, choisissez la sélection créée.
9. Cliquez sur le bouton **Lancer la sélection**.

Consultation du rapport sur les applications interdites en mode d'essai

Pour consulter le rapport sur les applications interdites en mode d'essai, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.
L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. À l'étape **Sélection du type de modèle du rapport**, sélectionnez **Autre** → **Rapport sur les applications interdites en mode d'essai**.
Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.
5. Ouvrez le rapport d'un double-clic.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Consultation des événements à l'issue du fonctionnement du module Contrôle des applications

Pour consulter les événements survenus dans Kaspersky Security Center à l'issue du fonctionnement du module Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.

3. Cliquez sur le bouton **Créer une sélection**.
La fenêtre **Propriétés <nom de la sélection>** s'ouvre.
4. Ouvrez la section **Événements**.
5. Cliquez sur le bouton **Tout désélectionner**.
6. Dans le tableau **Événements**, cochez la case **Le lancement de l'application est interdit**.
7. Cliquez sur le bouton **OK**.
8. Dans la liste déroulante **Événements de la sélection**, choisissez la sélection créée.
9. Cliquez sur le bouton **Lancer la sélection**.

Consultation du rapport sur les applications interdites

Pour consulter le rapport sur les applications interdites, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.
L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. À l'étape **Sélection du type de modèle du rapport**, sélectionnez **Autre** → **Rapport sur les applications interdites**.
Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.
5. Ouvrez le rapport d'un double-clic.


Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Test des règles du Contrôle des applications

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles.

Pour analyser le fonctionnement des règles de Contrôle des applications, il faut étudier les événements sur la base des résultats du fonctionnement du module Contrôle des applications survenus dans Kaspersky Security Center. Si aucune des applications indispensables au travail de l'utilisateur de l'ordinateur n'affiche des événements d'interdiction de lancement en mode test, les règles créées sont correctes. Dans le cas contraire, il est conseillé de préciser les paramètres des règles que vous avez créées, de créer des règles complémentaires ou de supprimer des règles existantes.

Pour activer le test des règles de Contrôle des applications ou pour sélectionner une règle d'interdiction du Contrôle des applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
Cette action permet d'ouvrir la liste des règles du Contrôle des applications.
3. Dans la colonne **État**, sélectionnez l'option **Test**.
L'état signifie que Kaspersky Endpoint Security autorise toujours le lancement des applications soumises à cette règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.
4. Enregistrez vos modifications.

Kaspersky Endpoint Security ne bloquera pas les applications dont le lancement est interdit par le module Contrôle des applications, mais enverra des notifications de lancement au Serveur d'administration.

Surveillance des applications

Le *Contrôle de l'activité des applications* est un outil conçu pour consulter les informations relatives à l'activité des applications sur l'ordinateur d'un utilisateur en temps réel.

L'utilisation de la Surveillance des applications requiert l'installation des modules Contrôle des applications et Prévention des intrusions. Si ces modules ne sont pas installés, la section Surveillance des applications de la [fenêtre principale de l'application](#) est masquée.

Pour lancer le Contrôle de l'activité des applications, procédez comme suit :

Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Surveillance des applications**.

La fenêtre **Activité des applications** s'ouvre. Dans cette fenêtre, les informations relatives à l'activité des applications sur l'ordinateur de l'utilisateur sont présentées sur trois onglets :

- L'onglet **Toutes les applications** affiche des informations concernant toutes les applications installées sur l'ordinateur.
- L'onglet **En cours d'exécution** affiche des informations concernant la consommation de ressources informatiques par chaque application en temps réel. À partir de cet onglet, vous pouvez également procéder à la configuration des autorisations pour une application individuelle.
- L'onglet **Exécuter au démarrage** affiche la liste des applications qui sont lancées lorsque le système d'exploitation démarre.

Règles de création de masques de noms de fichiers ou de dossiers

Le *masque du nom de fichier ou de dossier* est une représentation du nom du dossier ou du nom et de l'extension du fichier à l'aide de caractères génériques.

Vous pouvez utiliser les caractères génériques suivants pour créer un masque de nom de fichier ou de dossier :


- Le caractère `*` (astérisque), qui prend la place de tout ensemble de caractères (y compris un ensemble vide). Par exemple, le masque `C:*.txt` inclura tous les chemins vers les fichiers avec l'extension `.txt` situés dans des dossiers et des sous-dossiers sur le disque (C:).
- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension `TXT` et un nom composé de trois caractères.

Modification des modèles de messages du Contrôle des applications

Quand l'utilisateur tente de lancer une application interdite par la règle de Contrôle des applications, Kaspersky Endpoint Security affiche un message sur le blocage du lancement. Si l'utilisateur estime que le blocage du lancement de l'application n'a pas lieu d'être, il peut cliquer sur un lien dans la notification afin d'envoyer un message à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage du lancement de l'application et pour les messages destinés à l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier le modèle de message, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres d'application, sélectionnez la section **Protection** → **Contrôles de sécurité** → **Contrôle des applications**.
3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle des applications :
 - **Blocage**. Modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application.
 - **Message à l'administrateur**. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'application est intervenu par erreur.
4. Enregistrez vos modifications.

Pratiques exemplaires en matière de mise en œuvre d'une liste d'applications autorisées

Dans le cadre de la planification de l'introduction d'une liste d'applications autorisées, il est recommandé d'exécuter les actions suivantes :

1. Créer les types de regroupement suivants :
 - Groupes d'utilisateurs. Les groupes d'utilisateurs pour lesquels il faut autoriser l'utilisation de différentes sélections d'applications.
 - Groupes d'administration. Un ou plusieurs groupes d'ordinateurs auxquels Kaspersky Security Center appliquera la liste des applications autorisées. Il est nécessaire de créer plusieurs groupes d'ordinateurs si différents paramètres de la liste d'autorisation sont utilisés pour ces groupes.

2. Composer la liste des applications dont le lancement doit être autorisé.

Avant de créer la liste, il est conseillé de réaliser les opérations suivantes :

a. Lancer la tâche de l'inventaire.

Les informations relatives à la création, à la modification des paramètres et au lancement de la tâche d'inventaire sont accessibles dans la section Gestion des tâches.

b. Consulter la [liste des fichiers exécutables](#).

Configuration du mode de liste d'autorisation pour les applications

Dans le cadre de la configuration du mode de liste d'autorisation, il est recommandé d'exécuter les actions suivantes :

1. Créer les [catégories d'applications](#) contenant les applications dont il faut autoriser le lancement.

Vous pouvez choisir un des modes suivants de création d'une catégorie d'applications :

• **Catégorie enrichie manuellement.** Vous pouvez enrichir cette catégorie manuellement en utilisant les conditions suivantes :

- Métadonnées du fichier. Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables qui possèdent les métadonnées indiquées.
- Hachage du fichier. Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables qui possèdent l'hachage indiqué.

L'utilisation de cette condition exclut la possibilité d'installer automatiquement les mises à jour car les fichiers de différentes versions auront un hachage différent.

- Certificat du fichier. Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables signés par le certificat indiqué.
- Catégorie KL. Kaspersky Security Center ajoute à la catégorie des applications toutes les applications qui appartiennent à la catégorie KL indiquée.
- Dossier de l'application. Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables de ce dossier.

L'utilisation de la condition Dossier de l'application n'est pas sans risques car le lancement de n'importe quelle application depuis le dossier indiqué est autorisé. Il est conseillé d'appliquer les règles qui utilisent les catégories d'applications avec la condition Dossier de l'application uniquement aux utilisateurs pour lesquels il faut absolument autoriser l'installation automatique des mises à jour.

- **Catégorie qui contient les fichiers exécutables du dossier sélectionné.** Vous pouvez indiquer le dossier qui contient les fichiers exécutables qui vont se retrouver automatiquement dans la catégorie d'applications créée.
- **Catégorie qui contient les fichiers exécutables des appareils sélectionnés.** Vous pouvez indiquer l'ordinateur dont tous les fichiers exécutables vont se retrouver automatiquement dans la catégories d'applications créée.

Si vous utilisez ce mode de création de catégories d'applications, Kaspersky Security Center tire les informations sur les applications de l'ordinateur du [dossier Fichiers exécutables](#).

2. [Sélectionner le mode de liste d'autorisation](#) pour le module Contrôle des applications.

3. [Créer les règles de Contrôle des applications](#) à l'aide des catégories d'applications créées.

Les règles **Image d'or** et **Programmes de mise à jour de confiance** sont initialement définies pour le mode Liste d'autorisation. Ces règles du Contrôle des applications correspondent aux catégories KL. La catégorie KL "Image d'or" reprend les applications qui garantissent le fonctionnement normal du système d'exploitation. La catégorie KL "Programmes de mise à jour de confiance" reprend les programmes de mise à jour des applications des éditeurs les plus connus. Vous ne pouvez pas supprimer ces règles. Les paramètres de ces règles ne peuvent pas être modifiés. Par défaut, la règle **Système d'exploitation et ses modules** est activée tandis que la règle **Programmes de mise à jour de confiance** est désactivée. Le lancement des applications, correspondant aux conditions de déclenchement de ces règles, est autorisé pour tous les utilisateurs.

Image d'or

4. Définir les applications pour lesquelles il faut autoriser l'installation automatique des mises à jour.

Vous pouvez autoriser l'installation automatique des mises à jour d'une des manières suivantes :

- Désigner la liste étendue des applications autorisées en autorisant le lancement de toutes les applications appartenant à n'importe laquelle des catégories KL.
- Désigner la liste étendue des applications autorisées en autorisant le lancement de toutes les applications signées par des certificats.

Pour autoriser le lancement de toutes les applications signées par des certificats, vous pouvez créer une catégorie avec une condition en fonction du certificat dans laquelle seul le paramètre **Objet** avec la valeur * est utilisé.

- Pour les règles de contrôle des applications, définir le paramètre **Programmes de mise à jour de confiance**. Si cette case est cochée, Kaspersky Endpoint Security considère les applications reprises dans la règle comme des programmes de mise à jour de confiance. Kaspersky Endpoint Security autorise le démarrage d'applications qui ont été installées ou mises à jour par des applications incluses dans la règle, à condition qu'aucune règle de blocage ne soit appliquée à ces applications.

Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutables créés par les programmes de mise à jour de confiance migre également.

- Créer le dossier et y placer les fichiers exécutables des applications pour lesquelles vous voulez autoriser l'installation automatique des mises à jour. Créer ensuite la catégorie d'applications avec la condition Dossier de l'application et indiquer le chemin vers ce dossier. Puis créer une règle d'autorisation et sélectionner cette catégorie.

L'utilisation de la condition Dossier de l'application n'est pas sans risques car le lancement de n'importe quelle application depuis le dossier indiqué est autorisé. Il est conseillé d'appliquer les règles qui utilisent les catégories d'applications avec la condition Dossier de l'application uniquement aux utilisateurs pour lesquels il faut absolument autoriser l'installation automatique des mises à jour.

Test du mode de liste d'autorisation

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles. Quand le mode test est activé, Kaspersky Endpoint Security ne bloque pas les applications dont le lancement est interdit par les règles de Contrôle des applications, mais envoie des notifications de lancement au Serveur d'administration.

Dans le cadre du test du mode de liste d'autorisation, il est recommandé d'exécuter les actions suivantes :

1. Définir la période du test (de quelques jours à deux mois).
2. Activer le [test des règles du Contrôle des applications](#).
3. Analyser les résultats du test en utilisant les [événements survenus suite au fonctionnement en mode test du Module de l'application](#) et les [rapports sur les applications interdites en mode d'essai](#).
4. Sur la base des résultats de l'analyse, introduire des modifications dans les paramètres du mode de liste d'autorisation.

En particulier, sur la base des résultats du test, vous pouvez [ajouter à la catégorie d'applications des fichiers exécutables liés aux événements](#).

Prise en charge du mode de liste d'autorisation

Après [avoir sélectionné l'action d'interdiction du Contrôle des applications](#), il est conseillé de maintenir la prise en charge du mode de liste d'autorisation de la manière suivante :

- Analyser le fonctionnement des règles de Contrôle des applications à l'aide des [événements survenus lors du fonctionnement du Contrôle des applications](#) et des [rapports sur les lancements interdits](#).
- Analyser les demandes d'accès aux applications envoyées par les utilisateurs.
- Analyser les fichiers exécutables inconnus en vérifiant leur réputation dans [Kaspersky Security Network](#).
- Avant d'installer les mises à jour pour le système d'exploitation ou pour une application, il convient d'installer ces mises à jour sur le groupe d'ordinateurs d'essai afin de voir comment les règles de Contrôle des applications vont les traiter.
- Ajouter les applications nécessaires aux catégories utilisées dans les règles de Contrôle des applications.


Contrôle des ports réseau

Lors du fonctionnement de Kaspersky Endpoint Security, les modules [Contrôle Internet](#), [Protection contre les menaces par emails](#) et [Protection contre les menaces Internet](#) contrôlent les flux de données transmis via des protocoles déterminés sur les ports TCP et UDP définis et ouverts de l'ordinateur de l'utilisateur. Par exemple, le module Protection contre les menaces par emails analyse les informations transmises via le protocole SMTP et le module Protection contre les menaces Internet, les informations transmises via les protocoles HTTP et FTP.

Kaspersky Endpoint Security répartit les ports TCP et UDP de l'ordinateur de l'utilisateur en plusieurs groupes en fonction de la probabilité d'une attaque réussie contre ceux-ci. Certains ports réseau sont réservés aux services vulnérables. Il est conseillé de soumettre ces ports à un contrôle plus strict, car ceux-ci courent un risque plus élevé d'être pris pour cible par une attaque réseau. Si vous utilisez des services non standards quelconques affectés à des ports réseau inhabituels, sachez que ces ports peuvent être eux-aussi soumis à une attaque. Vous pouvez préciser une liste de ports réseau et une liste d'applications qui demandent un accès au réseau. Lors de la surveillance du trafic réseau, ces ports et applications font ensuite l'objet d'une attention particulière de la part des modules Protection contre les menaces par emails et Protection contre les menaces Internet.


Activation du contrôle de tous les ports réseau

Pour activer le contrôle de tous les ports réseau, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler tous les ports réseau**.
4. Enregistrez vos modifications.

Constitution de la liste des ports réseau contrôlés

Pour créer la liste des ports réseau contrôlés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
4. Cliquez sur le bouton **Sélectionner**.

Cette action permet d'ouvrir la liste des ports réseau utilisés habituellement pour le transfert du courrier électronique et du trafic réseau. Cette liste est livrée avec Kaspersky Endpoint Security.
5. Utilisez le commutateur dans la colonne **État** pour activer ou désactiver la surveillance des ports réseau.
6. Si le port réseau contrôlé ne figure pas sur la liste des ports réseau, ajoutez-la de la manière suivante :
 - a. Cliquez sur le bouton **Ajouter**.
 - b. Dans la fenêtre qui s'ouvre, indiquez le numéro de port réseau ainsi qu'une brève description.
 - c. Définissez l'état **Actif** ou **Inactif** pour la surveillance des ports réseau.
7. Enregistrez vos modifications.


Lors de l'utilisation du protocole FTP en mode passif, la connexion peut être établie via un port réseau aléatoire qui n'a pas été ajouté dans la liste des ports réseau contrôlés. Pour protéger de telles connexions, [activez la surveillance de tous les ports réseau](#) ou [configurez le contrôle des ports réseau pour les applications qui établissent des connexions FTP](#).

Constitution de la liste des applications dont tous les ports réseau sont contrôlés

Vous pouvez composer une liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security.

Il est conseillé d'ajouter à cette liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security les applications qui reçoivent ou envoient les données via le protocole FTP.

Pour composer la liste des applications dont tous les ports réseau seront contrôlés, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Paramètres du réseau**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
4. Cochez la case **Contrôler tous les ports pour les applications de la liste recommandée par Kaspersky**.

Si vous cochez cette case, Kaspersky Endpoint Security contrôle tous les ports pour les applications suivantes :

- Adobe Reader.
- Apple Application Support.
- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.

- Navigateur Yandex.

5. Cochez la case **Contrôler tous les ports pour les applications indiquées**.

6. Cliquez sur le bouton **Sélectionner**.

Cette action permet d'ouvrir la liste des applications dont les ports réseau seront contrôlés par Kaspersky Endpoint Security.

7. Utilisez le commutateur dans la colonne **État** pour activer ou désactiver la surveillance des ports réseau.

8. Si l'application ne figure pas dans la liste des applications, ajoutez-la d'une des manières suivantes :

- a. Cliquez sur le bouton **Ajouter**.
- b. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au fichier exécutable de l'application ainsi qu'une brève description.
- c. Définissez l'état **Actif** ou **Inactif** pour la surveillance des ports réseau.

9. Enregistrez vos modifications.

Exportation et importation de listes de ports contrôlés

Kaspersky Endpoint Security utilise les listes suivantes pour surveiller les ports réseau : liste des ports réseau et liste des applications dont les ports sont contrôlés par Kaspersky Endpoint Security. Vous pouvez exporter des listes de ports contrôlés dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre de ports présentant la même description. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder les listes des ports contrôlés ou pour procéder à la migration des listes vers un autre serveur.

[Comment exporter et importer des listes de ports contrôlés dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez la section **Paramètres généraux** → **Paramètres du réseau**.
6. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
7. Cliquez sur le bouton **Paramètres**.

La fenêtre **Ports réseau** s'ouvre. La fenêtre **Ports réseau** contient la liste des ports réseau utilisés habituellement pour le transfert du courrier électronique et du trafic réseau. Cette liste est livrée avec Kaspersky Endpoint Security.

8. Pour exporter une liste de ports réseau, procédez comme suit :
 - a. Dans la liste des ports réseau, sélectionnez les ports que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucun port, Kaspersky Endpoint Security exportera tous les ports.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des ports réseau et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des ports réseau dans un fichier XML.
9. Pour exporter la liste des applications dont les ports sont contrôlés par Kaspersky Endpoint Security, procédez comme suit :
 - a. Cochez la case **Contrôler tous les ports pour les applications indiquées**.
 - b. Dans la liste des applications, sélectionnez les applications que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.

Si vous n'avez sélectionné aucune application, Kaspersky Endpoint Security exportera toutes les applications.
 - c. Cliquez sur le bouton **Exporter**.
 - d. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des applications et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - e. Cliquez sur le bouton **Enregistrer**.

Kaspersky Endpoint Security exporte la liste complète des applications dans un fichier XML.
10. Pour importer une liste de ports réseau, procédez comme suit :

a. Dans la liste des ports réseau, cliquez sur le bouton **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des ports réseau.

b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste de ports réseau, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

11. Pour importer une liste d'applications dont les ports sont contrôlés par Kaspersky Endpoint Security, procédez comme suit :

a. Dans la liste des applications, cliquez sur le bouton **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications.

b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'applications, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

12. Enregistrez vos modifications.

[Comment exporter et importer des listes de ports contrôlés dans Web Console et Cloud Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer des listes de ports contrôlés.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Pour exporter une liste de ports réseau, procédez comme suit :
 - a. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
 - b. Cliquez sur le lien **X ports sélectionnés**.
La fenêtre **Ports réseau** s'ouvre. La fenêtre **Ports réseau** contient la liste des ports réseau utilisés habituellement pour le transfert du courrier électronique et du trafic réseau. Cette liste est livrée avec Kaspersky Endpoint Security.
 - c. Dans la liste des ports réseau, sélectionnez les ports que vous souhaitez exporter.
 - d. Cliquez sur le bouton **Exporter**.
 - e. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des ports réseau et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - f. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des ports réseau dans un fichier XML.
6. Pour exporter la liste des applications dont les ports sont contrôlés par Kaspersky Endpoint Security, procédez comme suit :
 - a. Dans le groupe **Ports contrôlés**, cochez la case **Contrôler tous les ports pour les applications indiquées**.
 - b. Cliquez sur le lien **X applications sélectionnées**.
 - c. Dans la liste des applications, sélectionnez les applications que vous souhaitez exporter.
 - d. Cliquez sur le bouton **Exporter**.
 - e. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des applications et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - f. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des applications dans un fichier XML.
7. Pour importer une liste de ports réseau, procédez comme suit :
 - a. Dans la liste des ports réseau, cliquez sur le bouton **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des ports réseau.

b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste de ports réseau, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

8. Pour importer une liste d'applications dont les ports sont contrôlés par Kaspersky Endpoint Security, procédez comme suit :

a. Dans la liste des applications, cliquez sur le bouton **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications.

b. Cliquez sur le bouton **Ouvrir**.

Si l'ordinateur dispose déjà d'une liste d'applications, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

9. Enregistrez vos modifications.

Protection élargie contre les menaces

Managed Detection and Response

Le module Managed Detection and Response a été ajouté à Kaspersky Endpoint Security version 11.6.0. Ce module facilite l'interaction avec la solution connue sous le nom de Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* recherche, détecte et élimine en permanence les menaces qui visent votre organisation. Pour en savoir plus à propos du fonctionnement de la solution, *veuillez consulter le [guide d'aide de Kaspersky Managed Detection and Response](#)*.

Lorsque vous interagissez avec le module Kaspersky Managed Detection and Response, l'application vous permet d'exécuter les fonctions suivantes :

- Activer le module Managed Detection and Response à l'aide d'un fichier de configuration BLOB.
- Exécuter des commandes à partir du module Kaspersky Managed Detection and Response.
- Envoyer des données télémétriques au module Kaspersky Managed Detection and Response pour détecter les menaces.

Intégration avec Kaspersky Managed Detection and Response

L'intégration avec Kaspersky Managed Detection and Response comprend les étapes suivantes :

1 Configuration du Kaspersky Security Network privé

Passez cette étape si vous utilisez Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configure automatiquement Kaspersky Security Network local lors de l'installation du plug-in MDR.

Le KSN privé prend en charge l'échange de données entre les ordinateurs et les serveurs dédiés de Kaspersky Security Network, mais pas le KSN global.

Chargez le fichier de configuration de Kaspersky Security Network dans les propriétés du Serveur d'administration. Le fichier de configuration de Kaspersky Security Network se trouve dans l'archive ZIP du fichier de configuration MDR. Vous pouvez obtenir l'archive ZIP dans le module Kaspersky Managed Detection and Response Console. Pour en savoir plus sur la configuration de KSN privé, consultez l'[aide de Kaspersky Security Center](#). Vous pouvez également charger un fichier de configuration de Kaspersky Security Network sur l'ordinateur à partir de la ligne de commande (voir les instructions ci-dessous).

[Configuration de KSN privé à partir de la ligne de commande](#)

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le paquet de distribution Kaspersky Endpoint Security.
3. Exécutez la commande :

```
avp.com KSN /private <nom du fichier>
```

<nom du fichier> est le nom du fichier de configuration contenant les paramètres de KSN privé (format de fichier PKCS7 ou PEM).

Exemple :

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

En conséquence, Kaspersky Endpoint Security utilisera le KSN privé pour déterminer la réputation des fichiers, des applications et des sites Internet. Les paramètres de stratégie de la section **Kaspersky Security Network** afficheront l'état de fonctionnement suivant : *Réseau KSN : KSN privé*.

Vous devez [activer le mode KSN étendu](#) pour que Managed Detection and Response puisse fonctionner.

2 Activez le module Managed Detection and Response.

Chargez le fichier de configuration BLOB dans la stratégie de Kaspersky Endpoint Security (voir les instructions ci-dessous). Le fichier BLOB contient l'identifiant du client ainsi que des informations à propos de la licence pour Kaspersky Managed Detection and Response. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR. Vous pouvez obtenir l'archive ZIP dans le module Kaspersky Managed Detection and Response Console. Pour en savoir plus à propos d'un fichier BLOB, [veuillez consulter le guide d'aide de Kaspersky Managed Detection and Response](#).

[Procédure d'activation du module Managed Detection and Response dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Protection élargie contre les menaces** → **Detection and Response**.
6. Cochez la case **Managed Detection and Response**.
7. Dans le groupe **Paramètres**, cliquez sur **Importer** et sélectionnez le fichier BLOB reçu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.
8. Enregistrez vos modifications.

[Procédure d'activation du module Managed Detection and Response dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez **Protection élargie contre les menaces** → **Detection and Response**.
5. Activez le commutateur **Managed Detection and Response**.
6. Cliquez sur **Importer** et sélectionnez le fichier BLOB qui a été obtenu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.
7. Enregistrez vos modifications.

Procédure d'activation du module Managed Detection and Response à partir de la ligne de commande

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le paquet de distribution Kaspersky Endpoint Security.
3. Exécutez la commande :
 - Si les paramètres de l'application ne sont pas [protégés par un mot de passe](#) :
`avp.com MDRLICENSE /ADD <nom du fichier>`
<nom du fichier> est le nom du fichier de configuration BLOB pour l'activation du module Managed Detection and Response (format de fichier P7).
 - Si les paramètres de l'application sont [protégés par un mot de passe](#) :
`avp.com MDRLICENSE /ADD <nom du fichier> /login=<nom d'utilisateur>
/password=<mot de passe>`

Kaspersky Endpoint Security vérifie alors le fichier BLOB. La vérification du fichier BLOB comprend la vérification de la signature numérique et la validité de la licence. Si le fichier BLOB est validé, Kaspersky Endpoint Security chargera le fichier et l'enverra à l'ordinateur lors de la prochaine synchronisation avec Kaspersky Security Center. Vérifiez l'état de fonctionnement du module en consultant le *rapport sur l'état des modules de l'application*. Vous pouvez également consulter l'état de fonctionnement d'un module dans les rapports de l'interface locale de Kaspersky Endpoint Security. Le module **Managed Detection and Response** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Vous devez activer les composants suivants pour que Managed Detection and Response puisse fonctionner :

- [Kaspersky Security Network \(mode élargi\)](#);
- [Détection comportementale](#).

L'activation de ces modules est obligatoire. Dans le cas contraire, Kaspersky Managed Detection and Response ne peut pas fonctionner, car il ne reçoit pas les données télémétriques exigées.

En outre, Kaspersky Managed Detection and Response utilise les données reçues de la part d'autres modules d'application. L'activation de ces modules est facultative. Les modules qui fournissent des données supplémentaires sont les suivants :

- [Protection contre les menaces Internet.](#)
- [Protection contre les menaces par emails.](#)
- [Pare-feu.](#)

Migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security version 11 et les versions ultérieures prennent en charge la solution MDR. Les versions 11 à 11.5.0 de Kaspersky Endpoint Security envoient uniquement des données télémétriques à Kaspersky Managed Detection and Response pour permettre la détection des menaces. La version 11.6.0 de Kaspersky Endpoint Security dispose de toutes les fonctionnalités de l'agent intégré (Kaspersky Endpoint Agent).

Si vous utilisez Kaspersky Endpoint Security 11 – 11.5.0, vous devez mettre à jour les bases de données vers la dernière version pour pouvoir utiliser la solution MDR. Vous devez également installer Kaspersky Endpoint Agent.

Si vous utilisez Kaspersky Endpoint Security 11.6.0 ou une version ultérieure, vous devez sélectionner le module Managed Detection and Response lors de l'installation de l'application pour pouvoir utiliser la solution MDR. Dans ce cas, vous n'avez pas besoin d'installer Kaspersky Endpoint Agent.

Pour procéder à la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows, procédez comme suit :

1. Configurez l'intégration avec Kaspersky Managed Detection and Response dans la stratégie de Kaspersky Endpoint Security.
2. Désactivez le module Managed Detection and Response dans la stratégie de Kaspersky Endpoint Agent.

Si la stratégie de Kaspersky Endpoint Security s'applique également à des ordinateurs sur lesquels Kaspersky Endpoint Security 11 – 11.5.0 n'est pas installé, vous devez d'abord créer une stratégie de Kaspersky Endpoint Agent distincte pour ces ordinateurs. Dans la nouvelle stratégie, configurez l'intégration avec Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent permet à l'application d'interagir avec d'autres solutions de Kaspersky pour détecter les menaces complexes (par exemple, Kaspersky Sandbox). Les solutions de Kaspersky prises en charge par Kaspersky Endpoint Agent dépendent de la version de Kaspersky Endpoint Agent.

Pour en savoir plus à propos de Kaspersky Endpoint Agent for Windows inclus dans la solution logicielle que vous utilisez et à propos de la solution autonome, veuillez consulter le guide d'aide du produit en question :

- *Guide d'aide de Kaspersky Anti Targeted Attack Platform*
- *Guide d'aide de Kaspersky Sandbox*
- *Guide d'aide de Kaspersky Endpoint Detection and Response Optimum*

- *Guide d'aide de Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent fait partie du [kit de distribution de Kaspersky Endpoint Security](#). Vous pouvez installer Kaspersky Endpoint Agent en même temps que Kaspersky Endpoint Security. Pour ce faire, vous devez sélectionner le module Endpoint Agent lors de l'installation de l'application (par exemple, dans le [paquet d'installation](#)). Après avoir installé l'application avec Endpoint Agent, Kaspersky Endpoint Security et Kaspersky Endpoint Agent apparaissent dans la liste des applications installées. Après la suppression de Kaspersky Endpoint Security, l'application Kaspersky Endpoint Agent est également supprimée automatiquement.

Suppression des données

Kaspersky Endpoint Security vous permet de configurer une tâche pour supprimer à distance les données sur les ordinateurs des utilisateurs.

Kaspersky Endpoint Security supprime les données comme suit :

- en mode silencieux ;
- sur des disques durs et amovibles ;
- pour tous les comptes utilisateur de l'ordinateur.

Kaspersky Endpoint Security exécute la tâche *Suppression des données* pour tout type de licence, même après son expiration.

Modes de suppression des données

Celle-ci vous permet de supprimer les données dans les modes suivants :

- Suppression instantanée des données.
Ce mode vous permet, par exemple, de supprimer des données obsolètes pour libérer de l'espace sur le disque.
- Suppression différée des données.
Ce mode est destiné, par exemple, à protéger les données d'un ordinateur portable en cas de perte ou de vol. Vous pouvez configurer la suppression automatique des données pour le cas où l'ordinateur portable ne se trouve plus sur le réseau de l'entreprise et qu'il n'a pas été synchronisé depuis longtemps avec Kaspersky Security Center.

Il est impossible de planifier la suppression des données dans les propriétés de la tâche. Vous pouvez uniquement supprimer des données immédiatement après le lancement manuel d'une tâche ou configurer une suppression de données différée en l'absence de connexion à Kaspersky Security Center.

Restrictions

La suppression de données possède les restrictions suivantes :

- L'administration de la tâche *Suppression de données* n'est disponible que pour l'administrateur de Kaspersky Security Center. Il n'est pas possible de configurer ou d'exécuter une tâche dans l'interface locale de Kaspersky Endpoint Security.
- Pour le système de fichiers NTFS, Kaspersky Endpoint Security supprime uniquement les noms des principaux flux de données. Il est impossible de supprimer les noms de flux de données alternatifs.
- Lorsque vous supprimez un fichier de lien symbolique, Kaspersky Endpoint Security supprime également les fichiers dont le chemin est indiqué dans le lien symbolique.

Création d'une tâche de suppression de données

Pour supprimer des données sur les ordinateurs des utilisateurs, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

b. Dans la liste déroulante **Type de tâche**, choisissez **Suppression des données**.

c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, **Suppression de données (Antivol)**.

d. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

Si de nouveaux ordinateurs sont ajoutés au groupe d'administration de la zone d'action de la tâche, la tâche de suppression instantanée est lancée sur les nouveaux ordinateurs uniquement si moins de 5 minutes se sont écoulées entre la fin de l'exécution de la tâche et l'ajout de nouveaux ordinateurs.

5. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la tâche **Suppression des données** de Kaspersky Endpoint Security.

La fenêtre des propriétés de la tâche s'ouvre.

7. Choisissez l'onglet **Paramètres de l'application**.

8. Sélectionnez une méthode de suppression des données :

- **Supprimer via les outils du système d'exploitation.** Kaspersky Endpoint Security supprime les fichiers à l'aide des outils du système d'exploitation sans les placer dans la corbeille.
- **Supprimer sans possibilité de récupération.** Kaspersky Endpoint Security écrase les fichiers avec des données aléatoires. Il est pratiquement impossible de récupérer les données après cette suppression.

9. Si vous souhaitez utiliser la suppression de données différée, cochez la case **Supprimer automatiquement les données en cas d'absence de connexion à Kaspersky Security Center depuis plus de N jours**. Définissez le nombre de jours.

La tâche en mode de suppression différée des données est exécutée chaque fois que le délai d'absence de connexion à Kaspersky Security Center est dépassé.

Lors de la configuration de la suppression différée des données, n'oubliez pas qu'il arrive parfois, par exemple, qu'un employé éteigne son ordinateur avant de partir en vacances. Dans ce cas, la période d'absence de connexion pourrait être dépassée et les données seront supprimées. Pensez également à l'horaire de travail des utilisateurs itinérants. Pour en savoir plus sur les ordinateurs déconnectés et les utilisateurs itinérants, consultez l'[aide de Kaspersky Security Center](#).

Si la case n'est pas cochée, la tâche est exécutée immédiatement après la synchronisation avec Kaspersky Security Center.

10. Créez une liste d'objets à supprimer :

- **Dossiers.** Kaspersky Endpoint Security supprime tous les fichiers du dossier, ainsi que les sous-dossiers. Kaspersky Endpoint Security ne prend pas en charge les masques ou les variables d'environnement pour la saisie d'un chemin d'accès au dossier.
- **Fichiers selon l'extension.** Kaspersky Endpoint Security recherche les fichiers portant les extensions définies sur tous les disques de l'ordinateur, y compris les disques amovibles. Pour indiquer plusieurs extensions, utilisez les caractères ";" ou ",".
- **Dossiers standards.** Kaspersky Endpoint Security supprimera les fichiers des zones suivantes :
 - **Documents.** Fichiers dans le dossier standard *Documents* du système d'exploitation, ainsi que dans ses sous-dossiers.
 - **Cookies.** Fichiers dans lesquels le navigateur enregistre les données des sites Internet visités par l'utilisateur (par exemple, les données pour l'autorisation de l'utilisateur).
 - **Bureau.** Fichiers dans le dossier standard *Bureau* du système d'exploitation, ainsi que dans ses sous-dossiers.
 - **Fichiers temporaires Internet Explorer.** Fichiers temporaires associés à Internet Explorer : copies de pages Internet, d'images et de fichiers multimédias.
 - **Fichiers temporaires.** Fichiers temporaires associés au fonctionnement des applications installées sur l'ordinateur. Par exemple, les applications Microsoft Office créent des fichiers temporaires avec les copies de sauvegarde des documents.
 - **Fichiers Outlook.** Fichiers associés au fonctionnement du client de messagerie Outlook : fichiers de données (.pst), fichiers de données hors ligne (.ost), fichiers du carnet d'adresses en mode hors connexion (.ab) et fichiers du carnet d'adresses personnel (.pab).
 - **Profil d'utilisateur.** Ensemble des fichiers et des dossiers dans lequel sont enregistrés les paramètres du système d'exploitation du compte utilisateur local.

Vous pouvez créer une liste d'objets à supprimer sur chacun des onglets. Kaspersky Endpoint Security crée une liste générale consolidée et supprime les fichiers de cette liste lors de l'exécution de la tâche.

Il est impossible de supprimer les fichiers indispensables au fonctionnement de Kaspersky Endpoint Security.

11. Cliquez sur le bouton **Enregistrer**.

12. Cochez la case en regard de la tâche.

13. Cliquez sur le bouton **Démarrer**.

En conséquence, les données sont supprimées sur les ordinateurs des utilisateurs conformément au mode sélectionné : immédiatement ou en l'absence de connexion. Si Kaspersky Endpoint Security ne peut pas supprimer un fichier, par exemple, si l'utilisateur l'utilise à ce moment, l'application n'essaiera pas de le supprimer à nouveau. Pour terminer la suppression des données, lancez à nouveau la tâche.

Protection par mot de passe

L'ordinateur peut être utilisé par plusieurs personnes dont les connaissances informatiques varient. L'accès illimité des utilisateurs à Kaspersky Endpoint Security et à ses paramètres peut entraîner une réduction du niveau de sécurité de l'ordinateur dans son ensemble. La Protection par mot de passe permet de limiter l'accès des utilisateurs à Kaspersky Endpoint Security en fonction d'autorisations octroyées (par exemple, autorisation pour quitter l'application).

Si l'utilisateur qui a ouvert la session Windows (*l'utilisateur de la session*) est autorisé à réaliser l'action, Kaspersky Endpoint Security ne demande pas le nom d'utilisateur et le mot de passe ou le mot de passe temporaire. L'utilisateur a accès à Kaspersky Endpoint Security conformément aux autorisations octroyées.

Si l'utilisateur de session n'est pas autorisé à réaliser des actions, il peut accéder à l'application d'une des manières suivantes :

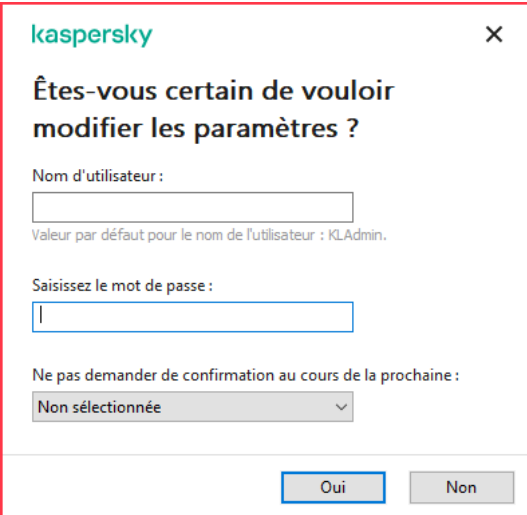
- Saisie du nom d'utilisateur et du mot de passe.

Ce mode est pratique pour l'utilisation quotidienne. Pour exécuter une action protégée par un mot de passe, il faut saisir les données du compte utilisateur du domaine de l'utilisateur qui possède l'autorisation requise. Dans ce cas, l'ordinateur doit se trouver dans le domaine. Si l'ordinateur n'est pas dans le domaine, vous pouvez utiliser le compte utilisateur KLAdmin.

- Saisie d'un mot de passe temporaire.

Cette méthode est pratique quand l'utilisateur se trouve en-dehors du réseau de l'entreprise et doit absolument obtenir un accès temporaire pour pouvoir réaliser une action interdite (par exemple, quitter l'application). À l'issue de la validité du mot de passe temporaire ou à la fin de la session, l'application rétablit les valeurs antérieures des paramètres de Kaspersky Endpoint Security.

Si l'utilisateur tente d'exécuter une action protégée par un mot de passe, Kaspersky Endpoint Security propose à l'utilisateur de saisir le nom d'utilisateur et le mot de passe ou le mot de passe temporaire (cf. ill. ci-après).



The image shows a Kaspersky dialog box with the following elements:

- Logo: kaspersky
- Close button: X
- Title: Êtes-vous certain de vouloir modifier les paramètres ?
- Field: Nom d'utilisateur : (with a text input box)
- Text: Valeur par défaut pour le nom de l'utilisateur : KLAdmin.
- Field: Saisissez le mot de passe : (with a text input box)
- Text: Ne pas demander de confirmation au cours de la prochaine :
- Dropdown menu: Non sélectionnée
- Buttons: Oui, Non

Sollicitation du mot de passe d'accès à Kaspersky Endpoint Security

Nom d'utilisateur et mot de passe

Pour pouvoir accéder à Kaspersky Endpoint Security, il faut absolument saisir les données du compte utilisateur du domaine. La Protection par mot de passe fonctionne avec les comptes utilisateur suivants :

- **KLAdmin.** Compte d'administrateur sans aucune restriction d'accès à Kaspersky Endpoint Security. Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe. Il est impossible de

retirer l'autorisation pour le compte utilisateur KLAdmin. Kaspersky Endpoint Security exige la définition du mot de passe du compte utilisateur KLAdmin lors de l'activation de la Protection par mot de passe.

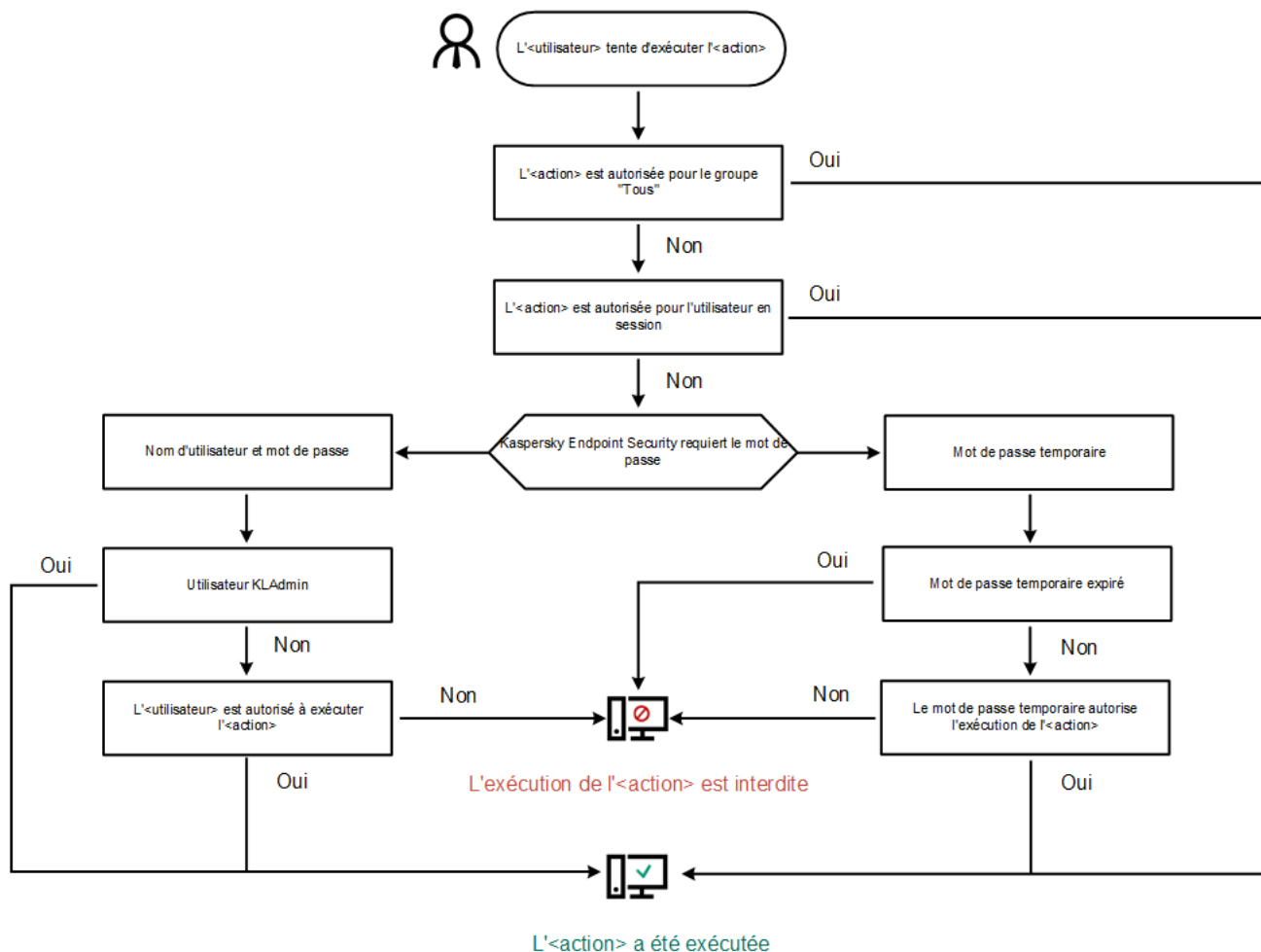
- **Groupe "Tous"**. Groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise. Les utilisateurs du groupe "Tous" peuvent accéder à l'application avec certaines restrictions.
- **Utilisateurs ou groupes distincts**. Comptes utilisateurs pour lesquels vous pouvez configurer des autorisations particulières. Par exemple, si une action est interdite pour le groupe "Tous", vous pouvez l'autoriser pour un utilisateur ou un groupe en particulier.
- **Utilisateur de session**. Compte de l'utilisateur qui a ouvert une session Windows. Vous pouvez changer d'utilisateur de session lors de la saisie du mot de passe (case **Mémoriser le mot de passe**). Dans ce cas, Kaspersky Endpoint Security désigne comme utilisateur de session. L'utilisateur dont vous avez saisi les identifiants au lieu de l'utilisateur qui a ouvert la session Windows.

Mot de passe temporaire

Le mot de passe temporaire permet d'octroyer un accès temporaire à Kaspersky Endpoint Security pour un ordinateur particulier hors du réseau de l'entreprise. L'administrateur crée un mot de passe temporaire pour un ordinateur distinct dans Kaspersky Security Center dans les propriétés de l'ordinateur de l'utilisateur. L'administrateur sélectionne les actions couvertes par le mot de passe temporaire, ainsi que la durée de validité de ce dernier.

Algorithme de fonctionnement de la Protection par mot de passe

Kaspersky Endpoint Security autorise ou non l'exécution d'une action protégée par mot de passe selon l'algorithme suivante (cf. ill. ci-dessous).




Algorithme de fonctionnement de la Protection par mot de passe

Activation de la Protection par mot de passe

La Protection par mot de passe permet de limiter l'accès des utilisateurs à Kaspersky Endpoint Security en fonction d'autorisations octroyées (par exemple, autorisation pour quitter l'application).

Pour activer la Protection par mot de passe, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
2. Utilisez le commutateur **Protection par mot de passe** pour activer ou désactiver le module.
3. Définissez le mot de passe pour le compte utilisateur KLAdmin et confirmez-le.
Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe.

Si l'ordinateur est administré par une stratégie, l'administrateur doit réinitialiser le mot de passe pour le compte utilisateur KLAdmin dans les propriétés de la stratégie. Si l'ordinateur n'est pas connecté à Kaspersky Security Center et si vous avez oublié le mot de passe du compte utilisateur KLAdmin, il est impossible de récupérer le mot de passe.

4. Définissez les autorisations pour tous les utilisateurs du réseau de l'entreprise.

a. Dans le tableau **Autorisations**, cliquez sur le bouton **Modifier** pour ouvrir la liste des autorisations pour le groupe Tous.

Le groupe "Tous" est un groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise.

b. Cochez la case en regard des actions que les utilisateurs pourront exécuter sans mot de passe.

Si une case n'est pas cochée, les utilisateurs ne peuvent pas réaliser cette action. Par exemple, si la case en regard de **Quitter l'application** est décochée, vous pouvez quitter l'application uniquement à l'aide du compte utilisateur KLAdmin, d'un [compte utilisateur particulier possédant l'autorisation requise](#) ou à l'aide d'un [mot de passe temporaire](#).

Les autorisations de la Protection par mot de passe se caractérisent par une [série de particularités](#). Assurez-vous que toutes les conditions sont remplies pour l'accès à Kaspersky Endpoint Security.

c. Cliquez sur le bouton **OK**.

5. Enregistrez vos modifications.

Une fois que la Protection par mot de passe a été activée, l'application limite l'accès des utilisateurs à Kaspersky Endpoint Security conformément aux restrictions du groupe "Tous". Les actions interdites pour le groupe "Tous" peuvent être exécutées uniquement sous le compte utilisateur KLAdmin, sous un [compte particulier doté des autorisations requises](#) ou à l'aide d'un [mot de passe temporaire](#).

Vous pouvez désactiver la protection par mot de passe uniquement avec le compte KLAdmin. Il n'est pas possible de désactiver la protection par mot de passe avec un autre compte ou avec un mot de passe temporaire.


Pendant la vérification du mot de passe, vous pouvez cocher la case **Mémoriser le mot de passe pour la session actuelle**. Dans ce cas, Kaspersky Endpoint Security n'exigera pas la saisie du mot de passe quand l'utilisateur tentera d'exécuter une autre action autorisée, protégée par un mot de passe, au cours de la session actuelle.

Octroi d'autorisations à des utilisateurs ou des groupes distincts

Vous pouvez octroyer l'accès à Kaspersky Endpoint Security à des utilisateurs ou groupes distincts. Par exemple si le groupe "Tous" ne peut pas quitter l'application, vous pouvez octroyer l'autorisation **Quitter l'application** à un utilisateur en particulier. Dès lors, il sera possible de quitter l'application uniquement sous ce compte utilisateur ou sous le compte utilisateur KLAdmin.

Vous pouvez utiliser les informations du compte utilisateur pour accéder à l'application uniquement si l'ordinateur se trouve dans le domaine. Si l'ordinateur n'est pas dans le domaine, vous pouvez utiliser un compte utilisateur KLAdmin ou un [mot de passe temporaire](#).

Pour octroyer une autorisation à des utilisateurs ou groupes distincts, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
2. Dans le tableau **Protection par mot de passe**, cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Sélectionner un utilisateur**.

La fenêtre standard de Windows pour la sélection d'utilisateurs ou de groupes s'ouvre.

4. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.
5. Dans la liste **Autorisations**, cochez les cases en regard des actions que l'utilisateur ou le groupe ajouté pourra exécuter sans saisir le mot de passe.

Si une case n'est pas cochée, les utilisateurs ne peuvent pas réaliser cette action. Par exemple, si la case en regard de **Quitter l'application** est décochée, vous pouvez quitter l'application uniquement à l'aide du compte utilisateur KLAdmin, d'un [compte utilisateur particulier possédant l'autorisation requise](#) ou à l'aide d'un [mot de passe temporaire](#).

Les autorisations de la Protection par mot de passe se caractérisent par une [série de particularités](#). Assurez-vous que toutes les conditions sont remplies pour l'accès à Kaspersky Endpoint Security.

6. Enregistrez vos modifications.

Par conséquent, si l'accès à l'application est restreint pour le groupe "Tous", les utilisateurs auront accès à Kaspersky Endpoint Security conformément aux autorisations définies pour eux.

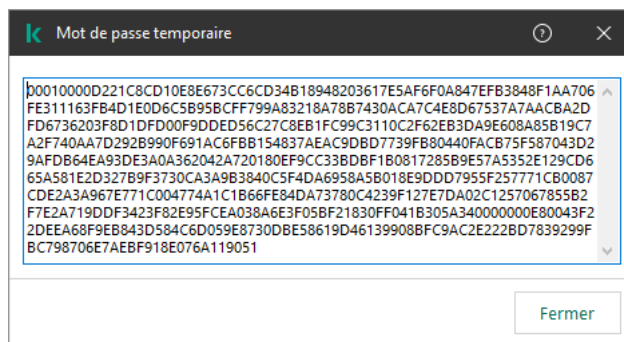
Utilisation du mot de passe temporaire pour octroyer un accès

Le mot de passe temporaire permet d'octroyer un accès temporaire à Kaspersky Endpoint Security pour un ordinateur particulier hors du réseau de l'entreprise. Ceci s'impose pour autoriser l'exécution d'une action interdite sans transmettre à l'utilisateur les identifiants du compte KLAdmin. Pour pouvoir utiliser un mot de passe temporaire, l'ordinateur doit être ajouté à Kaspersky Security Center.

Pour permettre à un utilisateur d'exécuter une action interdite via la saisie d'un mot de passe temporaire, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Ouvrez les propriétés de l'ordinateur d'un double clic.
5. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.
6. Dans la liste des applications de Kaspersky installées sur l'ordinateur, choisissez **Kaspersky Endpoint Security for Windows**, puis ouvrez les propriétés de l'application d'un double-clic.
7. Dans la fenêtre des propriétés de l'application, sélectionnez la section **Paramètres généraux** → **Interface**.
8. Dans le groupe **Protection par mot de passe**, cliquez sur le bouton **Paramètres**.
La fenêtre **Protection par mot de passe** s'ouvre.
9. Dans le groupe **Mot de passe temporaire**, cliquez sur le bouton **Paramètres**.
La fenêtre **Création d'un mot de passe temporaire** s'ouvre.
10. Dans le champ **Date d'expiration**, définissez la durée de validité du mot de passe temporaire.

11. Dans le tableau **Zone d'action du mot de passe temporaire**, cochez la case en regard des opérations que l'utilisateur pourra réaliser après avoir saisi le mot de passe temporaire.
12. Cliquez sur le bouton **Générer**.
La fenêtre du mot de passe temporaire s'ouvre (cf. ill. ci-dessous).
13. Copiez et transmettez celui-ci à l'utilisateur.




Mot de passe temporaire

Particularités des autorisations de la Protection par mot de passe

Les autorisations de la Protection par mot de passe se caractérisent par une série de particularités et limites.


Configuration des paramètres de l'application

Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs  ouverts).


Quitter l'application

Il n'y a aucune particularité ou restriction.

Désactivation des modules de la protection

- Il n'est pas possible d'accorder l'autorisation de désactiver des modules de la protection au groupe Tous. Pour autoriser non seulement l'utilisateur KLAdmin, mais également un autre utilisateur à désactivation des modules de la protection, [ajoutez l'utilisateur ou le groupe](#) avec l'autorisation **Désactivation des modules de la protection** dans les paramètres de la Protection par mot de passe.
- Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs  ouverts).
- Pour désactiver les modules de la protection dans les paramètres de l'application, l'utilisateur doit avoir l'autorisation **Configuration des paramètres de l'application**.
- Pour désactiver les modules de la protection via le menu contextuel (option **Suspendre la protection**), l'utilisateur doit avoir l'autorisation **Désactivation des modules de contrôle** en plus de l'autorisation **Désactivation des modules de la protection**.

Désactivation des modules de contrôle

- Il n'est pas possible d'accorder l'autorisation de désactivation des modules de contrôle au groupe Tous. Pour autoriser non seulement l'utilisateur KLAdmin, mais également un autre utilisateur à désactiver des modules de la protection, [ajoutez l'utilisateur ou le groupe](#) avec l'autorisation **Désactivation des modules de contrôle** dans les paramètres de la Protection par mot de passe.
- Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs  ouverts).
- Pour désactiver les modules de contrôle dans les paramètres de l'application, l'utilisateur doit avoir l'autorisation **Configuration des paramètres de l'application**.
- Pour désactiver les modules de contrôle via le menu contextuel (option **Suspendre la protection**), l'utilisateur doit avoir l'autorisation **Désactivation des modules de la protection** en plus de l'autorisation **Désactivation des modules de contrôle**.

Désactivation de la stratégie de Kaspersky Security Center

Il n'est pas possible d'autoriser la désactivation de la stratégie de Kaspersky Security Center pour le groupe "Tous". Pour autoriser la désactivation d'une stratégie non seulement par l'utilisateur KLAdmin, mais également par un autre utilisateur, [ajoutez l'utilisateur ou le groupe](#) avec l'autorisation **Désactivation de la stratégie de Kaspersky Security Center** dans les paramètres de la Protection par mot de passe.

Suppression de la clé

Il n'y a aucune particularité ou restriction.

Suppression/modification/réparation de l'application

Si vous avez autorisé le retrait, la modification et la restauration de l'application pour le groupe "Tous", Kaspersky Endpoint Security ne demande pas de mot de passe lorsque l'utilisateur tente d'effectuer ces opérations. Par conséquent, tout utilisateur, y compris les utilisateurs extérieurs au domaine, peut installer, modifier ou restaurer l'application.

Restauration de l'accès aux données sur les appareils chiffrés

Le compte utilisateur KLAdmin est le seul qui peut restaurer l'accès aux données sur les appareils chiffrés. Il est impossible de permettre à un autre utilisateur d'exécuter cette action.

Consulter les rapports

Il n'y a aucune particularité ou restriction.

Restauration depuis la Sauvegarde

Il n'y a aucune particularité ou restriction.

Zone de confiance

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger. Un administrateur peut également autoriser un utilisateur à créer sa propre zone de confiance locale pour un ordinateur particulier. De cette façon, les utilisateurs peuvent créer leurs propres listes locales d'exclusions et d'applications de confiance en plus de la zone de confiance générale proposée par une stratégie.

Définition de l'exclusion de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Les exclusions de l'analyse permettent d'utiliser des applications légitimes qui pourraient être employées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être exploitées par des individus malintentionnés. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'[Encyclopédie de virus de Kaspersky](#).

Kaspersky Endpoint Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des exclusions de l'analyse sur les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque du nom de la menace conformément au classement de l'Encyclopédie des virus de Kaspersky. Par exemple, vous utilisez souvent dans le cadre de votre travail l'application Radmin prévue pour l'administration à distance des ordinateurs. Kaspersky Endpoint Security classe cette activité parmi les activités suspectes et peut la bloquer. Pour exclure le blocage d'une application, il est nécessaire de créer une exclusion de l'analyse dans laquelle vous indiquerez le nom ou le masque du nom selon la classification de l'Encyclopédie des virus de Kaspersky.

Si votre ordinateur est doté d'une application qui récolte et envoie des informations à traiter, Kaspersky Endpoint Security peut la considérer comme une application malveillante. Pour éviter cela, vous pouvez exclure ce programme de l'analyse, en configurant Kaspersky Endpoint Security de manière décrite dans ce document.

Les exclusions de l'analyse peuvent être utilisées pendant le fonctionnement des modules et des tâches suivantes de l'application définis par l'administrateur du système :

- [Détection comportementale](#).
- [Protection contre les Exploits](#).
- [Prévention des intrusions](#).
- [Protection contre les fichiers malicieux](#).
- [Protection contre les menaces Internet](#).
- [Protection contre les menaces par emails](#).
- [Tâches d'analyse](#).

Kaspersky Endpoint Security n'analyse pas l'objet si au lancement d'une des tâches d'analyse le disque dur ou le dossier d'emplacement de cet objet figure dans la zone d'analyse. Cependant, lors du lancement de la tâche d'analyse personnalisée, l'exclusion de l'analyse n'est pas appliquée à cet objet.

[Création d'une exclusion d'analyse dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions**.
6. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Exclusions de l'analyse**.
Une fenêtre reprenant la liste des exclusions s'ouvre.
8. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.
9. Cochez la case **Autoriser l'utilisation des exclusions locales** si vous souhaitez permettre à l'utilisateur de créer une liste locale d'exclusions. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les fichiers figurant dans la liste.
10. Cliquez sur le bouton **Ajouter**.
11. Si vous souhaitez exclure un fichier ou un dossier de l'analyse, procédez comme suit :
 - a. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.
 - b. Le lien **sélectionnez le fichier ou le dossier** situé dans le groupe **Description de l'exclusion de l'analyse** permet d'ouvrir la fenêtre **Nom du fichier ou du dossier**.
 - c. Saisissez le nom du fichier ou du dossier, le masque du nom du fichier ou du dossier ou choisissez le fichier ou le dossier dans l'arborescence des dossiers après avoir cliqué sur le bouton **Parcourir**.
Utilisez des masques :
 - Le caractère ***** remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque **C:**.txt** inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
 - Deux caractères ***** qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le

masque `C:\Dossier***.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:***.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

d. Cliquez sur le bouton **OK** dans la fenêtre **Nom du fichier ou du dossier**.

Le lien vers le fichier ou le dossier ajouté apparaît dans le groupe **Description de l'exclusion de l'analyse** de la fenêtre **Exclusion de l'analyse**.

12. Si vous voulez exclure de l'analyse des objets portant un nom précis, procédez comme suit :

a. Dans le groupe **Propriétés**, cochez la case **Nom de l'objet**.

b. Le lien **saisissez le nom de l'objet** situé dans le groupe **Description de l'exclusion de l'analyse** permet d'ouvrir la fenêtre **Nom de l'objet**.

c. Saisissez le nom du type d'objet en fonction de la classification de l'[Encyclopédie Kaspersky](#) (par exemple, `Vers de courrier`, `Rootkit` ou `RemoteAdmin`).

Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, Kaspersky Endpoint Security exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.

d. Cliquez sur le bouton **OK** dans la fenêtre **Nom de l'objet**.

Le lien vers le nom de l'objet ajouté apparaît dans le groupe **Description de l'exclusion de l'analyse** de la fenêtre **Exclusion de l'analyse**.

13. Si vous souhaitez exclure un fichier individuel des analyses, procédez comme suit :

a. Dans le groupe **Propriétés**, cochez la case **Hachage de l'objet**.

b. Cliquez sur le lien d'entrée de l'hachage de l'objet pour ouvrir la fenêtre **Hachage de l'objet**.

c. Saisissez l'hachage du fichier ou sélectionnez le fichier en cliquant sur le bouton **Parcourir**.

Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

d. Cliquez sur le bouton **OK** dans la fenêtre **Hachage de l'objet**.

Le lien vers l'objet ajouté apparaît dans le groupe **Description de l'exclusion de l'analyse** de la fenêtre **Exclusion de l'analyse**.

14. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

15. Définissez les modules de Kaspersky Endpoint Security qui doivent appliquer l'exclusion de l'analyse :

a. Cliquez sur le lien **quelconque** situé dans le groupe **Description de l'exclusion de l'analyse** pour activer le lien **sélectionnez les modules**.

b. Cliquez sur le lien **sélectionnez les modules** pour ouvrir la fenêtre **Modules de la protection**.

c. Cochez les cases en regard modules auxquels s'appliqueront les exclusions de l'analyse.

d. Cliquez sur le bouton **OK** dans la fenêtre **Modules de la protection**.

Si les modules sont indiqués dans les paramètres de l'exclusion de l'analyse, l'exclusion n'est appliquée que lorsque l'analyse est effectuée par ces modules de Kaspersky Endpoint Security.

Si les modules ne sont pas indiqués dans les paramètres de l'exclusion de l'analyse, l'exclusion est appliquée lors de l'analyse effectuée par tous les modules de Kaspersky Endpoint Security.

16. Vous pouvez utiliser la case pour [mettre fin à une exclusion](#) à tout moment.

17. Enregistrez vos modifications.

[Création d'une exclusion d'analyse dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez ajouter une exclusion.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez **Paramètres généraux** → **Exclusions**.
5. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le lien **Exclusions de l'analyse**.
6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.
7. Cochez la case **Autoriser l'utilisation des exclusions locales** si vous souhaitez permettre à l'utilisateur de créer une liste locale d'exclusions. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les fichiers figurant dans la liste.
8. Cliquez sur le bouton **Ajouter**.
9. Sélectionnez la manière dont vous souhaitez ajouter l'exclusion : **Fichier ou dossier**, **Nom de l'objet** ou **Hachage de l'objet**.
10. Si vous souhaitez exclure un fichier ou un dossier des analyses, sélectionnez le fichier ou le dossier en cliquant sur le bouton **Parcourir**.

Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les caractères * et ? lors de la saisie d'un masque :

- Le caractère ***** remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque **C:**.txt** inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
- Deux caractères ***** qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque **C:\Dossier***.txt** inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé **Dossier** et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque **C:***.txt** n'est pas un masque valide.
- Le caractère **?** remplace n'importe quel caractère unique, sauf les caractères **** et **/** (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le

masque C:\Dossier\???.txt inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé Dossier qui ont l'extension TXT et un nom composé de trois caractères.

11. Si vous souhaitez exclure un type particulier d'objet des analyses, saisissez, dans le champ **Objet**, le nom du type d'objet selon la classification de l'[Encyclopédie Kaspersky](#) (par exemple, Email-Worm, Rootkit ou RemoteAdmin).

Vous pouvez utiliser des masques avec le caractère ? (remplace n'importe quel caractère unique) et le caractère * (remplace n'importe quel nombre de caractères). Par exemple, si le masque Client* est spécifié, Kaspersky Endpoint Security exclut les objets Client-IRC, Client-P2P et Client-SMTP des analyses.

12. Si vous souhaitez exclure un fichier individuel des analyses, saisissez l'hachage du fichier dans le champ **Hachage du fichier**.

Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.


13. Dans le groupe **Modules de la protection**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

14. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

15. Vous pouvez utiliser le commutateur pour [mettre fin à une exclusion](#) à tout moment.

16. Enregistrez vos modifications.

[Création d'une exclusion d'analyse dans l'interface de l'application](#)

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

4. Cliquez sur le bouton **Ajouter**.

5. Si vous souhaitez exclure un fichier ou un dossier des analyses, sélectionnez le fichier ou le dossier en cliquant sur le bouton **Parcourir**.

Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les caractères * et ? lors de la saisie d'un masque :

- Le caractère * remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:**.txt inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
- Deux caractères * qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier***.txt inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé Dossier et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque C:***.txt n'est pas un masque valide.
- Le caractère ? remplace n'importe quel caractère unique, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque C:\Dossier\???.txt inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé Dossier qui ont l'extension TXT et un nom composé de trois caractères.

6. Si vous souhaitez exclure un type particulier d'objet des analyses, saisissez, dans le champ **Objet**, le nom du type d'objet selon la classification de l'[Encyclopédie Kaspersky](#) (par exemple, **Email-Worm**, **Rootkit** ou **RemoteAdmin**).

Vous pouvez utiliser des masques avec le caractère ? (remplace n'importe quel caractère unique) et le caractère * (remplace n'importe quel nombre de caractères). Par exemple, si le masque **Client*** est spécifié, Kaspersky Endpoint Security exclut les objets **Client-IRC**, **Client-P2P** et **Client-SMTP** des analyses.

7. Si vous souhaitez exclure un fichier individuel des analyses, saisissez l'hachage du fichier dans le champ **Hachage du fichier**.

Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

8. Dans le groupe **Modules de la protection**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

9. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

10. Sélectionnez l'état **Actif** pour l'exclusion.

Vous pouvez utiliser le commutateur pour [mettre fin à une exclusion](#) à tout moment.

11. Enregistrez vos modifications.

Exemples de masque de chemin d'accès :

Chemins d'accès à des fichiers situés dans n'importe quel dossier :

- Le masque `*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe.
- Le masque `exemple` reprend tous les chemins d'accès aux fichiers dont le nom est EXAMPLE.

Chemins d'accès à des fichiers situés dans le dossier indiqué :


- Le masque `C:\dir*.*` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir*` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir\` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe dans le dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir*\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\ et dans les sous-dossiers du dossier C:\dir\.

Chemin d'accès aux fichiers situés dans tous les dossiers portant le nom indiqué :

- Le masque `dir*.*` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir*` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir\` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.

Lancement et arrêt du fonctionnement de l'exclusion de l'analyse

Pour lancer ou arrêter une exclusion de l'analyse, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.
4. Sélectionnez l'exclusion souhaitée dans la liste des exclusions.
5. Utilisez le commutateur à côté d'un objet pour inclure cet objet dans la zone d'analyse ou l'exclure.
6. Enregistrez vos modifications.

Composition de la liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et réseau (y compris l'activité malveillante), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Endpoint Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Cependant, une application qui a été ajoutée à la liste des applications de confiance est exclue des analyses par Kaspersky Endpoint Security.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance. L'analyse ignore ensuite les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Endpoint Security considère comme suspectes peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic réseau d'un ordinateur par Kaspersky Endpoint Security et un autre logiciel antivirus) et d'améliorer les performances de l'ordinateur, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autres programmes présentant une menace. Pour exclure entièrement l'application de l'analyse Kaspersky Endpoint Security, il est nécessaire d'utiliser les exclusions de l'analyse.

[Comment ajouter une application à la liste des applications de confiance dans la Console d'administration \(MMC\)](#)



1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions**.
6. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre **Exclusions de l'analyse pour l'application**, sélectionnez l'onglet **Applications de confiance**.

Une fenêtre reprenant la liste des applications de confiance s'ouvre.

8. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'applications de confiance pour tous les ordinateurs de l'organisation. Les listes des applications de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les applications de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'applications de confiance de stratégie parent n'est pas possible.
 9. Cochez la case **Autoriser l'utilisation des applications de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale d'applications de confiance en plus de la liste générale d'applications de confiance créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.
- Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des applications de confiance créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les applications de confiance figurant dans la liste.
10. Cliquez sur le bouton **Ajouter**.
 11. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier exécutable de l'application de confiance.

Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères ***** et **?** lors de la saisie d'un masque.

Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'applications de confiance sur la console Kaspersky Security Center. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère `*` (par exemple, `C:\Users*\Documents\File.exe`).

Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

12. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).
13. Vous pouvez utiliser la case pour [exclure une application de la zone de confiance](#) à tout moment.

14. Enregistrez vos modifications.

[Comment ajouter une application à la liste des applications de confiance dans Web Console et Cloud Console ?](#)


1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez ajouter l'application à la liste des applications de confiance.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Sélectionnez **Paramètres généraux** → **Exclusions**.
5. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le lien **Applications de confiance**.
Une fenêtre reprenant la liste des applications de confiance s'ouvre.
6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'applications de confiance pour tous les ordinateurs de l'organisation. Les listes des applications de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les applications de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'applications de confiance de stratégie parent n'est pas possible.
7. Cochez la case **Autoriser l'utilisation des applications de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale d'applications de confiance en plus de la liste générale d'applications de confiance créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des applications de confiance créée dans le cadre de la stratégie. Si une liste locale a été créée, une fois que cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les applications de confiance figurant dans la liste.
8. Cliquez sur le bouton **Ajouter**.
9. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier exécutable de l'application de confiance.
Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères ***** et **?** lors de la saisie d'un masque.

Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'applications de confiance sur la console Kaspersky Security Center. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère `*` (par exemple, `C:\Users*\Documents\File.exe`).

Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.
10. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).
11. Vous pouvez utiliser la case pour [exclure une application de la zone de confiance](#) à tout moment.
12. Enregistrez vos modifications.

Comment ajouter une application à la liste des applications de confiance dans l'interface de l'application

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Sélectionnez le fichier exécutable de l'application de confiance.

Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.

Kaspersky Endpoint Security prend en charge les variables d'environnement et convertit le chemin dans l'interface locale de l'application. Autrement dit, si vous saisissez le chemin d'accès au fichier `%userprofile%\Documents\File.exe`, une entrée `C:\Users\Fred123\Documents\File.exe` est ajoutée dans l'interface locale de l'application pour l'utilisateur Fred123. Par conséquent, Kaspersky Endpoint Security ignore le programme de confiance `File.exe` pour les autres utilisateurs. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère `*` (par exemple, `C:\Users*\Documents\File.exe`).

Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

6. Dans la fenêtre des propriétés de l'application de confiance, configurez les paramètres avancés (cf. tableau ci-après).
7. Vous pouvez utiliser le commutateur pour [exclure une application de la zone de confiance](#) à tout moment.
8. Enregistrez vos modifications.


Paramètres des applications de confiance

| Paramètre | Description |
|--|---|
| Ne pas analyser les fichiers ouverts | Tous les fichiers qui sont ouverts par l'application sont exclus des analyses par Kaspersky Endpoint Security. Par exemple, si vous utilisez des applications pour effectuer des sauvegardes de fichiers, cette fonctionnalité permet de réduire la consommation de ressources par Kaspersky Endpoint Security. |
| Ne pas surveiller l'activité de l'application | Kaspersky Endpoint Security ne surveille pas l'activité des fichiers et du réseau de l'application dans le système d'exploitation. L'activité de l'application est contrôlée par les modules suivants : Détection comportementale , Protection contre les Exploits , Prévention des intrusions , Réparation des actions malicieuses et Pare-feu . |
| Ne pas hériter les restrictions du processus parent (application) | Les restrictions configurées pour le processus parent ne seront pas appliquées par Kaspersky Endpoint Security à un processus enfant. Le processus parent est lancé par une application pour laquelle des droits d'application (Prévention des intrusions) et des règles réseau d'application (Pare-feu) sont configurés. |
| Ne pas surveiller l'activité des | Kaspersky Endpoint Security ne surveille pas l'activité des fichiers ni du réseau des applications qui sont lancées par cette application. |

| | |
|---|---|
| applications enfants | |
| Autoriser l'interaction avec l'interface de Kaspersky Endpoint Security | Kaspersky Endpoint Security Self-Defense bloque toute tentative de gestion des services d'application à partir d'un ordinateur distant. Si la case est cochée, l'application d'accès à distance à l'ordinateur peut gérer les paramètres de Kaspersky Endpoint Security via l'interface de Kaspersky Endpoint Security. |
| Ne pas bloquer l'interaction avec le module Protection AMSI <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | Kaspersky Endpoint Security ne surveille pas les demandes de l'application de confiance visant à ce que les objets soient analysés par le module de la protection AMSI . |
| Ne pas analyser le trafic chiffré/Ne pas analyser l'ensemble du trafic | Le trafic réseau amorcé par l'application sera exclu des analyses par Kaspersky Endpoint Security. Vous pouvez exclure des analyses l'ensemble du trafic ou seulement le trafic chiffré. Vous pouvez également exclure des analyses des adresses IP et des numéros de port individuels. |
| Commentaire | Si nécessaire, vous pouvez fournir un court commentaire concernant l'application de confiance. Les commentaires permettent de simplifier les recherches et le tri des applications de confiance. |
| État | État de l'application de confiance : <ul style="list-style-type: none"> • L'état Actif signifie que l'application se trouve dans la zone de confiance. • L'état Inactif signifie que l'application est exclue de la zone de confiance. |

Activation et désactivation de l'effet des règles de la zone de confiance sur l'application de la liste des applications de confiance


Pour activer ou désactiver l'effet des règles de la zone de confiance sur une application de la liste des applications de confiance, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.
4. Sélectionnez l'application de confiance requise dans la liste des applications de confiance.
5. Utilisez le commutateur dans la colonne **État** pour inclure une application de confiance dans la zone d'analyse ou l'exclure.
6. Enregistrez vos modifications.

Utilisation du stockage système sécurisé des certificats

L'utilisation du stockage système sécurisé des certificats permet d'exclure de l'analyse antivirus les applications signées par une signature numérique de confiance. Kaspersky Endpoint Security attribue automatiquement ces applications au groupe *De confiance*

Pour commencer à utiliser le stockage système sécurisé des certificats, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans la liste déroulante **Stockage système sécurisé des certificats**, choisissez le stockage système que Kaspersky Endpoint Security devra considérer comme sécurisé.
4. Enregistrez vos modifications.

Utilisation de la sauvegarde

La *Sauvegarde* est le stockage qui contient les copies de sauvegarde des objets qui ont été modifiés ou supprimés lors de la désinfection. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier C:\ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès total à ce dossier sont accordées aux utilisateurs du groupe Administrateurs. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Kaspersky Endpoint Security n'offre pas la possibilité de configurer les autorisations d'accès des utilisateurs aux copies de sauvegarde des fichiers.


Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations critiques partiellement ou complètement perdues suite à la désinfection, vous pouvez tenter de restaurer le fichier depuis sa copie de sauvegarde dans son dossier d'origine.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les copies de sauvegarde des fichiers peuvent être transmises au serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur l'utilisation des copies de sauvegarde des fichiers dans Kaspersky Security Center, consultez l'Aide de Kaspersky Security Center.

Configuration de la durée de conservation maximale des fichiers dans la sauvegarde

Par défaut, la durée maximale de conservation des copies dans le dossier de sauvegarde est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens de la sauvegarde.


Pour configurer la durée de conservation maximale des fichiers dans le dossier de sauvegarde, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Rapports et stockage**.
3. Si vous souhaitez limiter la durée de conservation des copies de fichiers dans le dossier de sauvegarde, cochez la case **Supprimer les objets après X jours** dans le groupe **Sauvegarde et restauration**. Dans le champ situé à droite de **Supprimer les objets après X jours**, saisissez la durée de conservation maximale des copies de fichiers dans le dossier de sauvegarde.
4. Enregistrez vos modifications.

Configuration de la taille maximale de la Sauvegarde

Vous pouvez définir la taille maximale de la sauvegarde. Par défaut, la taille de la sauvegarde n'est pas limitée. Quand le stockage des données atteint la taille maximale configurée, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens du dossier de sauvegarde afin de ne plus dépasser la limite.

Pour configurer la taille maximale du dossier de sauvegarde, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Rapports et stockage**.
3. Si vous souhaitez limiter la taille de la sauvegarde, cochez la case **Limiter la taille de la sauvegarde à X Mo** dans le groupe **Sauvegarde et restauration**. Définir la taille maximale de la sauvegarde.
4. Enregistrez vos modifications.

Restauration des fichiers depuis la sauvegarde

Si Kaspersky Endpoint Security détecte un code malveillant dans un fichier, il bloque celui-ci, lui attribue l'état *Infecté* et place une copie dans le dossier de sauvegarde avant de tenter de le désinfecter. Si le fichier est réparé, l'état de la copie de sauvegarde devient *Réparé*. Le fichier est accessible dans le dossier d'origine. En cas d'échec de la désinfection, Kaspersky Endpoint Security le supprime du dossier d'origine. Vous pouvez restaurer le fichier à partir de sa copie de sauvegarde dans le dossier d'origine.

Les fichiers portant l'état *Sera désinfecté lors du redémarrage l'ordinateur* ne pourront pas être restaurés. Redémarrez l'ordinateur et l'état du fichier devient *Désinfecté* ou *Supprimé*. Dans ce cas, vous pouvez restaurer le fichier à partir de sa copie de sauvegarde dans le dossier d'origine.

En cas de détection d'un code malveillant dans un fichier qui appartient à une app de Windows Store, Kaspersky Endpoint Security ne place pas la copie de fichier dans la sauvegarde, mais le supprime directement. Dans ce cas, pour restaurer l'intégrité de l'app de Windows Store, vous pouvez utiliser les outils du système d'exploitation Microsoft Windows 8 (pour en savoir plus sur la restauration d'une app de Windows Store, lisez *l'Aide de Microsoft Windows 8*).

La liste des copies de sauvegarde des fichiers se présente sous la forme d'un tableau. Pour la copie de sauvegarde du fichier, le chemin d'accès au dossier d'emplacement d'origine de ce fichier apparaît. Ce chemin d'accès peut contenir des données personnelles.

Si la Sauvegarde contient plusieurs fichiers portant le même nom, mais de contenu différent placés dans le même dossier, seul le fichier placé en dernier dans la Sauvegarde peut être restauré.

Pour restaurer des fichiers depuis le dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Stockage**.
La fenêtre **Sauvegarde et restauration** s'ouvre.
2. Dans le tableau de la fenêtre **Sauvegarde et restauration**, sélectionnez un ou plusieurs fichiers du dossier de sauvegarde.
3. Cliquez sur le bouton **Restaurer**.

Kaspersky Endpoint Security restaure tous les fichiers sélectionnés depuis le dossier de sauvegarde vers leurs dossiers d'origine.

Suppression des copies de sauvegarde des fichiers depuis le dossier de sauvegarde

Kaspersky Endpoint Security supprime les copies de sauvegarde des fichiers de n'importe quel état automatiquement à l'issue de la période définie dans les paramètres de l'application. Vous pouvez aussi supprimer vous-même n'importe quelle copie de fichier dans la sauvegarde.

Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Stockage**.

La fenêtre **Sauvegarde et restauration** s'ouvre.

2. Sélectionnez les copies de sauvegarde des fichiers que vous souhaitez supprimer du dossier de sauvegarde et cliquez sur le bouton **Supprimer**. Vous pouvez également supprimer tous les fichiers du dossier de sauvegarde en cliquant sur le bouton **Tout supprimer**.

Kaspersky Endpoint Security supprimera les copies de sauvegarde sélectionnées des fichiers de la sauvegarde.

Service des notifications

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Endpoint Security. Les notifications relatives à ces événements peuvent avoir un caractère informatif ou importants. Par exemple, la notification peut signaler la réussite de la mise à jour des bases et des modules de l'application ou signaler une erreur dans le fonctionnement d'un module que vous devrez rectifier au plus vite.

Kaspersky Endpoint Security permet de consigner les informations relatives aux événements survenus dans le fonctionnement de l'application dans le journal des événements Microsoft Windows et/ou dans le journal de Kaspersky Endpoint Security.

Kaspersky Endpoint Security peut remettre les notifications de la manière suivante :

- Via des pop-ups de notification dans la zone de notification de la barre des tâches de Microsoft Windows.
- Par email.


Vous pouvez configurer les modes de remise des notifications. Le mode de remise des notifications est défini pour chaque type d'événement.

Grâce au tableau des événements pour la configuration du service des notifications, vous pouvez réaliser les opérations suivantes :

- filtrer les événements du service des notifications en fonction de la valeur des colonnes ou selon un filtre complexe ;
- utiliser la fonction de recherche des événements du service des notifications ;
- trier les événements du service des notifications ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des événements du service des notifications.

Configuration des paramètres des journaux des événements

Pour configurer les paramètres des journaux des événements, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
3. Cliquez sur le bouton **Configurer les notifications** dans la section **Notifications**.

La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

Les événements peuvent contenir les données suivantes de l'utilisateur :


- chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;
- chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
- nom d'utilisateur Microsoft Windows ;
- adresses des pages Internet ouvertes par l'utilisateur.

4. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer les paramètres des journaux des événements.
5. Cochez les cases en regard des événements requis dans les colonnes **Enregistrer dans le rapport local** et **Enregistrer dans le journal d'événements Windows**.

Les événements dont la case a été cochée dans la colonne **Enregistrer dans le rapport local** s'affichent dans les **Journaux des applications et des services** de la section **Journal des événements Kaspersky**. Les événements dont la case a été cochée dans la colonne **Enregistrer dans le journal d'événements Windows** s'affichent dans les **Journaux Windows** de la section **Application**. Pour ouvrir les journaux des événements, sélectionnez **Démarrer** → **Panneau de configuration** → **Administration** → **Consultation des événements**.
6. Enregistrez vos modifications.

Configuration de l'affichage et la remise des notifications

Pour configurer les paramètres d'affichage et de remise des notifications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
3. Cliquez sur le bouton **Configurer les notifications** dans la section **Notifications**.

La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

Les événements peuvent contenir les données suivantes de l'utilisateur :

 - chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;
 - chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
 - nom d'utilisateur Microsoft Windows ;
 - adresses des pages Internet ouvertes par l'utilisateur.
4. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer la remise des notifications.
5. Dans la colonne **Notifier à l'écran**, cochez les cases en regard des événements requis.


Les informations relatives aux événements sélectionnés sont affichées dans des messages contextuels dans la zone de notification de la barre des tâches de Microsoft Windows.
6. Dans la colonne **Notifier par email**, cochez les cases en regard des événements requis.


Les informations relatives aux événements sélectionnés sont remises par email si les paramètres de remise des notifications par courrier ont été définis.
7. Cliquez sur le bouton **OK**.
8. Si vous avez activé les notifications par email, configurez les paramètres de livraison par email :
 - a. Cliquez sur le bouton **Paramètres des notifications par email**.

- b. Cochez la case **Activer les notifications** si vous souhaitez activer la remise des informations sur les événements du fonctionnement de Kaspersky Endpoint Security, sélectionnés dans la colonne **Notifier par email**.
 - c. Définissez les paramètres de remise des messages électroniques.
 - d. Cliquez sur le bouton **OK**.
9. Enregistrez vos modifications.

Configuration de l'affichage des avertissements sur l'état de l'application dans la zone de notification

Pour configurer l'affichage des avertissements sur l'état de l'application à la zone de notification, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Interface**.
3. Dans la section **Afficher l'état de l'application dans la zone de notifications**, cochez les cases en regard des catégories d'événements pour lesquels vous souhaitez voir des notifications dans la zone de notification de Microsoft Windows.
4. Enregistrez vos modifications.

Quand un événement de la catégorie choisie survient, l'[icône de l'application](#) dans la zone de notification se transformera en  ou  en fonction de l'importance de l'avertissement.


Utilisation des rapports

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'exécution de chaque tâche d'analyse, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans des rapports.

Les rapports se trouvent dans le dossier C:\ProgramData\Kaspersky Lab\KES\Report.

Les rapports peuvent contenir les données suivantes de l'utilisateur :

- chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;
- chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
- nom d'utilisateur Microsoft Windows ;
- adresses des pages Internet ouvertes par l'utilisateur.


Les données du rapport sont présentées sous forme de tableau. Chaque ligne du tableau contient des informations sur un événement distinct. Les attributs des événements sont situés dans les colonnes du tableau. Certaines colonnes sont complexes et contiennent des sous-colonnes avec des attributs complémentaires. Pour consulter les attributs supplémentaires, cliquez sur le bouton  à côté du nom de la colonne. Les événements enregistrés durant le fonctionnement des différents modules ou pendant l'exécution des différentes tâches ont différentes sélections d'attributs.


Les rapports suivants sont disponibles :

- Rapport **Système d'audit**. Ce rapport contient les informations relatives aux événements survenus pendant l'interaction de l'utilisateur avec l'application, ainsi que pendant le fonctionnement de l'application dans son ensemble mais sans rapport avec un module ou une tâche particuliers de Kaspersky Endpoint Security.
- Rapports sur le fonctionnement des modules de Kaspersky Endpoint Security.
- Rapports d'exécution des tâches de Kaspersky Endpoint Security.
- Rapport **Chiffrement des données**. Contient les informations relatives aux événements survenus pendant le chiffrement et le déchiffrement des données.

Les niveaux d'importance suivants sont utilisés dans les rapports :


 **Messages d'information**. Événements à caractère informatif qui en général ne contiennent aucune information importante.

 **Avertissements**. Événements qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement de l'application.

 **Événements critiques**. Événements critiques entraînant des problèmes dans le fonctionnement de Kaspersky Endpoint Security ou des vulnérabilités dans la protection de l'ordinateur.

Pour faciliter l'utilisation des rapports, vous pouvez modifier la représentation des données à l'écran d'une des manières suivantes :

- filtrer la liste des événements selon divers critères ;
- utiliser la fonction de recherche d'un événement en particulier ;

- consulter l'événement sélectionné dans un groupe distinct ;
- trier la liste des événements selon chaque colonne du rapport ;
- afficher et masquer les événements regroupés à l'aide d'un filtre d'événement à l'aide du bouton  ;
- modifier l'ordre et la sélection des colonnes affichées dans le rapport.

Le cas échéant vous pouvez exporter le rapport obtenu dans un fichier texte. Vous pouvez également [supprimer des informations des rapports](#) selon les modules ou les tâches de Kaspersky Endpoint Security regroupés dans le rapport.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les informations relatives aux événements peuvent être transmises au Serveur d'administration de Kaspersky Security Center (pour en savoir plus, consultez l'[aide de Kaspersky Security Center](#)).

Consulter les rapports

Si l'affichage des rapports est disponible pour l'utilisateur, celui-ci peut consulter tous les événements repris dans les rapports.


Pour consulter les rapports, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Rapports**.
2. Sélectionnez le module ou la tâche dans la liste proposée dans la partie gauche de la fenêtre **Rapports**.
La partie droite de la fenêtre affiche le rapport qui contient la liste des événements survenus suite au fonctionnement du module sélectionné ou de la tâche de Kaspersky Endpoint Security. Vous pouvez trier les événements dans le rapport selon les valeurs des cellules d'une des colonnes. Par défaut, les événements dans le rapport sont classés selon l'ordre croissant des valeurs des cellules la colonne **Date de l'événement**.
3. Si vous souhaitez consulter des informations détaillées sur un événement, sélectionnez l'événement souhaité dans le rapport.
Une section reprenant des informations de synthèse sur l'événement apparaît dans la partie inférieure de la fenêtre.

Configuration de la durée maximale de conservation des rapports

Par défaut, la durée maximale de conservation des rapports sur les événements détectés par Kaspersky Endpoint Security est de 30 jours. À l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport.

Pour configurer la durée maximale de conservation des rapports, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Rapports et stockage**.


3. Si vous souhaitez limiter la durée de stockage des rapports, cochez la case **Supprimer les rapports après X jours** dans le groupe **Rapports**. Définir la durée maximale de stockage des rapports.

4. Enregistrez vos modifications.

Configuration de la taille maximale du fichier de rapport

Vous pouvez définir la taille maximale du fichier contenant le rapport. Par défaut, la limite sur la taille du fichier du rapport est de 1 024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale.

Pour configurer la taille maximale du fichier de rapport, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Rapports et stockage**.
3. Dans le groupe **Rapports**, cochez la case **Limiter la taille du fichier de rapports à X Mo** si vous souhaitez limiter la taille d'un fichier de rapports. Définir la taille maximale du fichier de rapports.
4. Enregistrez vos modifications.

Enregistrement du rapport dans un fichier

L'utilisateur est seul responsable de la sécurité des informations du rapport enregistré dans le fichier et, plus particulièrement, du contrôle et de la restriction de l'accès à ces informations.

Le rapport composé peut être enregistré dans le fichier texte au format TXT ou CSV.

Kaspersky Endpoint Security enregistre l'événement dans un rapport de la même manière qu'il est présenté à l'écran, c'est-à-dire avec la même composition et avec la même séquence d'attributs de l'événement.


Pour enregistrer le rapport dans un fichier, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur **Plus de fonctionnalités** → **Rapports**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le module ou la tâche.
La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche de Kaspersky Endpoint Security.
3. S'il faut, modifiez la présentation des données dans le rapport à l'aide des moyens suivants :
 - filtrage des événements ;
 - recherche d'événements ;
 - modification de l'emplacement des colonnes ;

- classement des événements.
4. Cliquez sur le bouton **Enregistrer le rapport** situé dans la partie supérieure droite de la fenêtre.
 5. Dans la fenêtre qui s'ouvre, indiquez le dossier cible pour le rapport.
 6. Saisissez le nom du fichier du rapport dans le champ **Nom du fichier**.
 7. Dans le champ **Type de fichier**, sélectionnez le format requis du fichier de rapport : TXT ou CSV.
 8. Enregistrez vos modifications.

Suppression des informations des rapports

Pour supprimer les informations des rapports, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Rapports et stockage**.
3. Cliquez sur le bouton **Nettoyer** dans le groupe **Rapports**.
4. Si [la protection par mot de passe est activée](#), Kaspersky Endpoint Security peut vous demander des identifiants de compte utilisateur. L'application demande des identifiants de compte si l'utilisateur ne dispose pas des autorisations requises.

Kaspersky Endpoint Security supprimera tous les rapports pour tous les modules et tâches de l'application.

Autodéfense de Kaspersky Endpoint Security

Kaspersky Endpoint Security protège les ordinateurs contre les programmes malveillants, qui tentent de bloquer le fonctionnement de Kaspersky Endpoint Security ou de le supprimer de l'ordinateur. L'ensemble de technologies d'autodéfense disponibles pour Kaspersky Endpoint Security dépend du système d'exploitation (32 bits ou 64 bits) (consultez le tableau ci-dessous).


Technologies d'autodéfense de Kaspersky Endpoint Security

| Technologie | Description | Ordinateur x86 | Ordinateur x64 |
|--|---|----------------|----------------------------|
| Mécanisme d'autodéfense | Cette technologie bloque l'accès aux modules d'application suivants : <ul style="list-style-type: none">Fichiers du dossier d'installation de Kaspersky Endpoint SecurityClés de registre avec des enregistrements appartenant à l'applicationProcessus que l'application exécute | ✓ | ✓ |
| AM-PPL (Antimalware Protected Process Light) | La technologie protège les processus de Kaspersky Endpoint Security contre les actions malveillantes. Pour en savoir plus sur la technologie AM-PPL, consultez le site de Microsoft ² . <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019.</div> | ✓ | – |
| Mécanisme de protection contre l'administration externe | Cette technologie limite la gestion de Kaspersky Endpoint Security à l'aide d'applications spéciales d'administration à distance (comme TeamViewer ou RemotelyAnywhere). | ✓ | – (sauf pour Windows 7) |

Activation et désactivation du mécanisme de l'autodéfense

Par défaut, le mécanisme de l'autodéfense de Kaspersky Endpoint Security est activé.

Pour activer ou désactiver le mécanisme de l'autodéfense procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Utilisez la case **Activer l'autodéfense** pour activer ou désactiver le mécanisme d'autodéfense.
4. Enregistrez vos modifications.

Activation et désactivation de la prise en charge de la technologie AM-PPL

Kaspersky Endpoint Security prend en charge la technologie Antimalware Protected Process Light (ci-après "AM-PPL") de Microsoft. La technologie AM-PPL protège les processus de Kaspersky Endpoint Security contre les actions malveillantes (par exemple, l'arrêt d'une application). La technologie AM-PPL autorise uniquement l'exécution de processus de confiance. Les processus de Kaspersky Endpoint Security sont signés conformément aux exigences de sécurité de Windows et sont dès lors considérés comme des processus de confiance. Pour en savoir plus sur la technologie AM-PPL, consultez le [site de Microsoft](#). La technologie est activée par défaut AM-PPL.

Kaspersky Endpoint Security intègre également des mécanismes de protection des processus de l'application. La prise en charge de la technologie AM-PPL permet de déléguer les fonctions de protection des processus au système d'exploitation. Ainsi, vous augmentez la rapidité de l'application et réduisez la consommation des ressources de l'ordinateur.

Le service AM-PPL est disponible pour les systèmes d'exploitation Windows 10 versions 1703 (RS2) et suivants et Windows Server 2019.

Pour activer ou désactiver la prise en charge de la technologie AM-PPL, procédez comme suit :

1. [Désactivez le mécanisme d'autodéfense de l'application.](#)

Le mécanisme d'autodéfense empêche la modification et la suppression de processus de l'application dans la mémoire de l'ordinateur, y compris la modification de l'état de la technologie AM-PPL.

2. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.

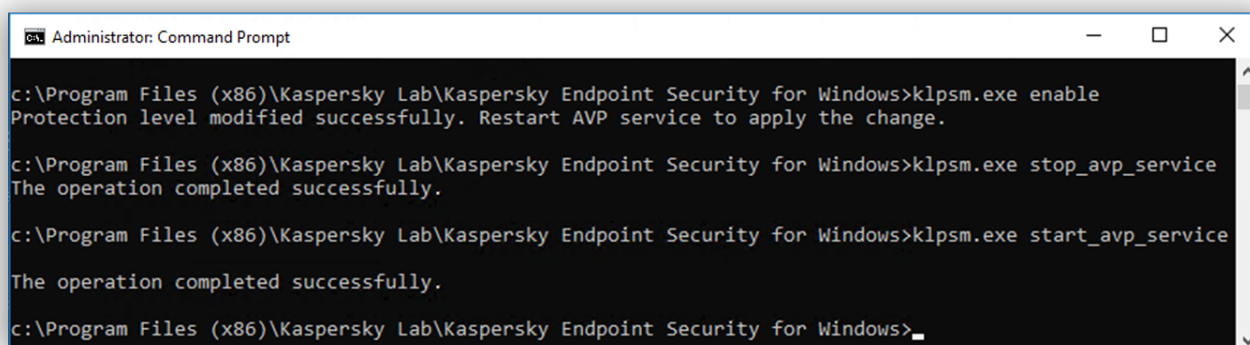
3. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

4. Saisissez sur la ligne de commande :

- `klpsm.exe enable` pour activer la prise en charge de la technologie AM-PPL (cf. ill. ci-dessous).
- `klpsm.exe disable` pour désactiver la prise en charge de la technologie AM-PPL.

5. Relancez Kaspersky Endpoint Security.

6. [Restaurez le mécanisme d'autodéfense de l'application.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.

c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```


Activation et désactivation du mécanisme de l'autodéfense contre l'administration externe

La protection contre l'administration externe vous permet d'interdire l'administration de Kaspersky Endpoint Security à l'aide d'applications d'administration à distance (comme TeamViewer ou RemotelyAnywhere). La technologie remplit les fonctions suivantes :

- Protection contre la modification des paramètres de Kaspersky Endpoint Security.
- Protection contre la gestion des services de Kaspersky Endpoint Security (comme le service **AVP**).
- Protection contre l'arrêt des processus des applications.

La protection contre l'administration externe est disponible uniquement pour les ordinateurs utilisant des systèmes d'exploitation 32 bits. La technologie n'est pas disponible pour les ordinateurs utilisant des systèmes d'exploitation 64 bits.

Pour activer ou désactiver la protection contre l'administration externe :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .
2. Dans la fenêtre des propriétés de l'application, sélectionnez la section **Paramètres avancés** → **Général**.
3. Utilisez la case **Autoriser la gestion des paramètres de Kaspersky Endpoint Security via les applications de contrôle à distance** pour activer ou désactiver la protection contre les modifications des paramètres de Kaspersky Endpoint Security. Si vous utilisez des applications d'administration à distance, vous devez autoriser l'administration des paramètres de Kaspersky Endpoint Security et [ajouter les applications à la liste des applications de confiance](#). Les applications d'administration à distance non fiables ne sont pas autorisées à modifier les paramètres de Kaspersky Endpoint Security même si la case **Autoriser la gestion des paramètres de Kaspersky Endpoint Security via les applications de contrôle à distance** est cochée. Cette case est inaccessible si la case **Activer l'autodéfense** est cochée.
4. Utilisez la case **Activer le contrôle de service externe** pour activer ou désactiver la protection des services de Kaspersky Endpoint Security contre l'administration externe.

Pour quitter l'application à partir de la ligne de commande, désactivez la protection des services de Kaspersky Endpoint Security contre l'administration externe.


5. Enregistrez vos modifications.

Par conséquent, lorsque les mécanismes de l'autodéfense contre l'administration externe sont activés, Kaspersky Endpoint Security empêche le curseur de la souris de pointer sur l'icône de l'application. Lorsqu'un utilisateur distant tente de fermer un service d'application, une fenêtre système s'affiche avec un message d'erreur.

Assurance de fonctionnement des applications de l'administration à distance

Il arrive souvent que lors de l'utilisation de mécanismes de protection contre l'administration externe il soit nécessaire d'appliquer une application d'administration externe.

Pour garantir le fonctionnement des applications d'administration à distance, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Sélectionnez le fichier exécutable de l'application d'administration à distance.
Vous pouvez également saisir le chemin manuellement. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères et lors de la saisie d'un masque.
6. Cochez la case **Ne pas surveiller l'activité de l'application**.
7. Enregistrez vos modifications.

Performances de Kaspersky Endpoint Security et compatibilité avec d'autres applications

Performances de Kaspersky Endpoint Security

Les performances de Kaspersky Endpoint Security désignent le nombre de types d'objets nuisibles à l'ordinateur qui peuvent être détectés et la consommation en ressources et en énergie de l'ordinateur.

Sélection des types d'objets à détecter

Kaspersky Endpoint Security permet de configurer en souplesse la protection de l'ordinateur et de sélectionner les [types d'objets](#) que l'application va détecter durant son fonctionnement. Kaspersky Endpoint Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans le système d'exploitation. Vous ne pouvez pas désactiver l'analyse pour ces types d'objets. Ces programmes peuvent infliger des dégâts considérables à l'ordinateur de l'utilisateur. Pour élargir la protection offerte à l'ordinateur, vous pouvez enrichir la liste des types d'objets à détecter en activant le contrôle de l'activité des applications légitimes qui pourraient être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

Utilisation du mode d'économie d'énergie

Si vous utilisez un ordinateur portable, la consommation électrique qu'entraînent les applications revêt une certaine importance. Bien souvent, les tâches programmées de Kaspersky Endpoint Security sont très gourmandes en ressources. Quand l'ordinateur est alimenté par la batterie, pour économiser la charge vous pouvez utiliser le mode d'économie d'énergie.

Le mode d'économie d'énergie permet de reporter automatiquement l'exécution des tâches qui ont été programmées.

- tâche de mise à jour ;
- tâche d'analyse complète ;
- tâche d'analyse rapide ;
- tâche d'analyse personnalisée ;
- tâche d'analyse de l'intégrité.

Cliquez-droit pour ouvrir le menu contextuel de l'application Kaspersky Endpoint Security for Windows et choisissez l'option Propriétés ou cliquez sur le bouton Propriétés situé sous la liste des applications. La tâche de chiffrement reprend dès que l'ordinateur portable est rebranché sur le secteur.

Transfert des ressources de l'ordinateur à d'autres applications

L'utilisation des ressources de l'ordinateur par Kaspersky Endpoint Security peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés à l'utilisation conjointe d'applications en cas de surcharge du processeur et des sous-systèmes de disque, Kaspersky Endpoint Security peut suspendre l'exécution des tâches programmées et céder les ressources à d'autres applications.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas de l'exécution de ces applications, il ne faut pas leur céder les ressources du système d'exploitation.

Au besoin, vous pouvez lancer ces tâches manuellement.

Application de la technologie de désinfection avancée

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. Quand Kaspersky Endpoint Security a détecté une activité malveillante dans le système d'exploitation, il exécute une procédure de désinfection étendue en appliquant la technologie de désinfection avancée. La *technologie de désinfection avancée* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui empêchent Kaspersky Endpoint Security de les supprimer à l'aide d'autres méthodes. La menace est ainsi neutralisée. Pendant l'exécution de la désinfection de l'infection active, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registre du système d'exploitation. La technologie de désinfection avancée est gourmande en ressource et peut ralentir d'autres applications.



À l'issue de la désinfection de l'infection active sur un ordinateur tournant sous Microsoft Windows pour postes de travail, Kaspersky Endpoint Security demande à l'utilisateur de confirmer le redémarrage de l'ordinateur. Après le redémarrage de l'ordinateur, Kaspersky Endpoint Security supprime les fichiers de l'application malveillante et lance une analyse complète simplifiée de l'ordinateur.

Sous Microsoft Windows pour serveurs, il est impossible de demander à l'utilisateur de confirmer le redémarrage en raison des particularités de la version de Kaspersky Endpoint Security. Le redémarrage non prévu du serveur de fichiers peut entraîner des problèmes liés à l'accès temporairement refusé aux données du serveur de fichiers ou à la perte des données non enregistrées. Il est conseillé de redémarrer le serveur de fichiers strictement selon la planification prévue. Par défaut, la technologie de désinfection avancée pour les serveurs de fichiers est [désactivée](#).

En cas de détection d'une infection active sur un serveur de fichiers, un événement relatif à la nécessité de désinfecter l'infection active est envoyé au Kaspersky Security Center. Pour désinfecter l'infection active sur le serveur, il faut activer la technologie de désinfection avancée pour les serveurs de fichiers et lancer la tâche de groupe *Recherche de virus* à l'heure qui convient le mieux aux utilisateurs.

Sélection des types d'objets à détecter

Pour sélectionner les types d'objets à identifier, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans la section **Types d'objets détectés**, cochez les cases pour les types d'objets que Kaspersky Endpoint Security doit détecter :
 - [Virus, vers](#) 

Sous-catégorie : virus et vers (Viruses_and_Worms)

Niveau de la menace : élevé

Les virus et les vers classiques exécutent sur l'ordinateur des actions qui n'ont pas été autorisées par l'utilisateur. Ils peuvent créer leurs propres copies qui possèdent la capacité d'auto-reproduction.

Virus classique

Une fois que le virus classique s'est introduit dans un système, il infecte un fichier quelconque, s'y active, exécute son action malveillante, puis ajoute sa copie à d'autres fichiers.

Le virus classique se multiplie uniquement sur les ressources locales de l'ordinateur et il est incapable de s'introduire lui-même dans un autre ordinateur. Il peut pénétrer dans d'autres systèmes uniquement s'il ajoute sa copie dans un fichier enregistré dans un dossier partagé, sur un cédérom d'installation ou si l'utilisateur envoie un email avec le fichier infecté en pièce jointe.

Le code du virus classique peut s'introduire dans divers secteurs de l'ordinateur, du système d'exploitation ou de l'application. En fonction de l'environnement dans lequel ils évoluent, on parle de *virus de fichiers*, *virus de démarrage*, *virus de script* et *virus de macro*.

Les virus peuvent infecter des fichiers de diverses manières. Les virus *écraseurs* (overwriting) remplacent le code du fichier infecté par leur propre code et suppriment ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *parasites* (Parasitic) modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les *virus compagnons* (Companion) ne modifient pas les fichiers mais créent des copies. Lorsque le fichier infecté est exécuté, son double est lancé, à savoir le virus. Il existe également des *virus-liens* (Link), des virus *qui infectent les modules objets* (OBJ), des virus *qui infectent les bibliothèques de compilateur* (LIB), les virus *qui infectent les textes source des programmes* et d'autres.

Ver

Le code du ver, à l'instar de celui du virus classique, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Le ver doit son nom à sa capacité à "ramper" d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

La principale caractéristique qui distingue les vers entre eux est leur mode de diffusion. Le tableau suivant reprend une description des différents types de vers en fonction du mode de diffusion.

Mode de diffusion des vers

| Type | Nom | Description |
|------------|---------------|---|
| Email-Worm | Email-Worm | Ils se diffusent via email. L'email infecté contient un fichier joint avec la copie du ver ou un lien vers ce fichier sur un site compromis ou créé spécialement à cette fin. Lorsque vous ouvrez le fichier joint, le ver est activé. Lorsque vous cliquez sur le lien, téléchargez le fichier, puis ouvrez celui-ci, le ver commence également à exécuter ses actions malveillantes. Ensuite, il continue à diffuser ses copies après avoir trouvé d'autres adresses email auxquelles il envoie des messages infectés. |
| IRC-Worm | Clients IM | Ils se propagent via les clients IM. En règle générale, ce ver envoie aux contacts un message contenant un lien vers la copie du ver sur un site. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active. |
| IRC- | Vers de chats | Ils se diffusent via les canaux IRC (Internet Relay Chats), ces systèmes |

| | | |
|-----------------|--|--|
| Worm | | <p>qui permettent de discuter en temps réel avec d'autres personnes.</p> <p>Ce ver publie un fichier avec sa copie ou un lien vers celle-ci dans le chat. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.</p> |
| Net-Worm | Vers de réseau (vers de réseaux informatiques) | <p>Ils se diffusent via les réseaux informatiques.</p> <p>À la différence des autres types de vers, le ver de réseau se propage sans l'intervention de l'utilisateur. Il recherche une application vulnérable sur les ordinateurs du réseau local. Pour ce faire, il envoie un paquet réseau spécial (un exploit) qui contient le code du ver ou une partie de celui-ci. Si le réseau abrite un ordinateur "vulnérable", celui-ci acceptera le paquet. Une fois qu'il s'est complètement introduit dans cet ordinateur, le ver s'active.</p> |
| P2P-Worm | Vers de réseau d'échange de fichiers | <p>Ils se propagent via les réseaux d'échange de fichiers pair à pair.</p> <p>Afin d'infiltrer le réseau d'échange de fichiers, le ver se copie dans le dossier d'échange de fichiers qui se trouve normalement sur l'ordinateur de l'utilisateur. Le réseau d'échange de fichiers affiche les informations relatives à ce fichier et l'utilisateur peut "trouver" le fichier infecté comme n'importe quel autre fichier, le télécharger puis l'ouvrir.</p> <p>Les vers plus sophistiqués imitent le protocole d'un réseau d'échange de fichiers en particulier : ils répondent positivement aux recherches et proposent leur copie pour le téléchargement.</p> |
| Ver | Autres vers | <p>Parmi ces autres vers, citons :</p> <ul style="list-style-type: none"> • Les vers qui diffusent leur copie via les ressources réseau. À l'aide des fonctions du système d'exploitation, ils consultent les répertoires réseau accessibles, se connectent aux ordinateurs du réseau mondial et tentent d'ouvrir leur disque en libre accès. À la différence des types de vers décrits ci-dessus, ces autres vers ne peuvent pas s'activer de manière autonome, mais uniquement lorsque l'utilisateur ouvre le fichier contenant la copie du ver. • Les vers qui n'adoptent aucun des modes de diffusion décrits dans ce tableau (par exemple, ceux qui se propagent via les téléphones portables). |

- [Chevaux de Troie](#) ?

Sous-catégories : chevaux de Troie (Trojan_programs)

Niveau de la menace : élevé

À la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie. Ils s'infiltrent sur les ordinateurs via email ou via le navigateur lorsque l'internaute visite un site infecté. Les chevaux de Troie sont exécutés sur intervention de l'utilisateur. Ils entament leur action malveillante directement après l'exécution.

Le comportement des chevaux de Troie sur l'ordinateur infecté varie. Parmi les fonctions principales des chevaux de Troie, citons le blocage, la modification ou la suppression d'informations ainsi que la perturbation du fonctionnement des ordinateurs ou des réseaux. De plus, les chevaux de Troie peuvent recevoir ou envoyer des fichiers, les exécuter, afficher des messages, contacter des pages Internet, télécharger des applications et les installer et redémarrer l'ordinateur.

Les individus malintentionnés utilisent souvent des "sélections" composées de divers chevaux de Troie.

Les types de comportement des chevaux de Troie sont décrits dans le tableau suivant.

Types de comportement des chevaux de Troie sur l'ordinateur infecté

| Type | Nom | Description |
|-----------------------|---|--|
| Trojan-ArcBomb | Chevaux de Troie (bombes dans les archives) | <p>Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur.</p> <p>Lorsque l'utilisateur tente de décompresser une archive de ce genre, l'ordinateur peut commencer à ralentir, voire à s'arrêter et le disque peut se remplir de données "vides". Ces "bombes" sont particulièrement dangereuses pour les serveurs de fichiers et de messagerie. Si le serveur utilise un système de traitement automatique des données entrantes, ce genre de "bombe d'archive" peut entraîner l'arrêt du serveur.</p> |
| Backdoor | Chevaux de Troie pour l'administration à distance | <p>Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs.</p> <p>Ces programmes s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu malintentionné d'administrer l'ordinateur à distance.</p> |
| Trojan | Chevaux de Troie | <p>Cette catégorie reprend les programmes malveillants suivants :</p> <ul style="list-style-type: none">• Chevaux de Troie traditionnels. Ils exécutent uniquement les fonctions fondamentales des chevaux de Troie : le blocage, la modification ou la suppression d'informations, la perturbation du fonctionnement des ordinateurs ou des réseaux. Ils ne possèdent pas les fonctions complémentaires caractéristiques d'autres chevaux de Troie décrits dans ce tableau.• Chevaux de Troie "multicibles". Ils possèdent des fonctions complémentaires appartenant à divers types de chevaux de Troie. |
| Trojan-Ransom | Chevaux de Troie exigeant le versement d'une rançon | <p>Ces programmes "prennent en otage" les données de l'ordinateur après les avoir modifiées ou bloquées ou perturbent le fonctionnement de l'ordinateur de telle manière que l'utilisateur n'est plus en mesure d'exploiter les données.</p> |

| | | |
|--------------------------|--|--|
| | | L'individu malintentionné exige le versement d'une somme d'argent en échange de l'envoi d'un programme qui rétablira le fonctionnement de l'ordinateur et les données qu'il abrite. |
| Trojan-Clicker | Chevaux de Troie qui cliquent | Ils accèdent à des pages Internet depuis l'ordinateur de la victime : ils envoient des instructions au navigateur ou remplacent les adresses Internet conservées dans les fichiers système. Grâce à ces programmes malveillants, les individus malintentionnés organisent des attaques réseau ou augmentent le nombre de visites sur le site afin d'accroître le nombre d'affichages de bannières publicitaires. |
| Trojan-Downloader | Chevaux de Troie qui téléchargent | Ils accèdent à la page Internet de l'intrus, y téléchargent d'autres applications malveillantes et les installent sur l'ordinateur de l'utilisateur. Ils peuvent contenir le nom du fichier de l'application malveillante à télécharger ou le recevoir à partir de la page Internet consultée. |
| Trojan-Dropper | Chevaux de Troie qui procèdent à des installations | Ils enregistrent sur le disque, puis installent d'autres chevaux de Troie présents dans le corps de ces programmes. Les individus malintentionnés peuvent utiliser ce genre de chevaux de Troie pour : <ul style="list-style-type: none"> • Installer un programme malveillant à l'insu de l'utilisateur : ces chevaux de Troie n'affichent aucun message réel ou fictif (par exemple, messages relatifs à une erreur dans une archive ou à la version incorrecte du système d'exploitation) ; • Protéger un autre programme malveillant connu : tous les antivirus ne sont pas en mesure d'identifier un programme malveillant au sein d'un cheval de Troie qui réalise des installations. |
| Trojan-Notifier | Chevaux de Troie qui envoient des notifications | Ils signalent à l'individu malintentionné que la communication avec l'ordinateur infecté est établie et transmettent des informations relatives à l'ordinateur : adresse IP, numéro du port ouvert ou adresse email. Ils contactent l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. Ces programmes sont souvent utilisés dans les sélections de différents chevaux de Troie. Ils indiquent à l'individu malintentionné que les autres chevaux de Troie ont bien été installés sur l'ordinateur de l'utilisateur. |
| Trojan-Proxy | Chevaux de Troie faisant office de proxy | Ils permettent à l'individu malintentionné de contacter anonymement des pages Internet via l'ordinateur de la victime ; le plus souvent, ils sont utilisés pour diffuser du spam. |
| Trojan-SMS | Chevaux de Troie qui volent des mots de passe | Il s'agit de chevaux de Troie qui volent des mots de passe (Password Stealing Ware) ; ils volent les données des comptes des utilisateurs, les données d'enregistrement d'un logiciel. Ils recherchent les données confidentielles dans les fichiers système et dans la base de registre et les transmettent à leur "maître" via email ou via FTP sur la page Internet de l'individu malintentionné ou par d'autres méthodes. |

| | | |
|-------------------------|--|---|
| | | Certains de ces programmes appartiennent à des groupes particuliers décrits dans ce tableau. Il s'agit des chevaux de Troie qui volent les comptes bancaires (Trojan-Banker), des chevaux de Troie qui volent les données des utilisateurs des clients IM (Trojan-IM) et des chevaux de Troie qui volent les données des adeptes de jeux en ligne (Trojan-GameThief). |
| Trojan-Spy | Chevaux de Troie espions | Ils espionnent l'utilisateur et collectent des informations sur les actions qu'il effectue lorsqu'il travaille sur son ordinateur. Ils peuvent intercepter les données que l'utilisateur saisit au clavier, faire des captures d'écran ou collecter des listes d'applications actives. Une fois qu'ils ont obtenu ces informations, ils les transmettent à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. |
| Trojan-DDoS | Chevaux de Troie pour attaques réseau | Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). Ces programmes infectent généralement plusieurs ordinateurs pour attaquer simultanément un serveur. Les programmes de type DoS lancent l'attaque depuis un ordinateur avec l'accord de l'utilisateur. Les programmes de type DDoS (Distributed DoS) lancent des attaques distribuées depuis plusieurs ordinateurs, à l'insu de l'utilisateur de l'ordinateur infecté. |
| Trojan-IM | Chevaux de Troie qui volent les données des utilisateurs de clients IM | Ils volent les numéros et les mots de passe des utilisateurs des clients IM. Ils transmettent ces informations à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. |
| Rootkit | Rootkits | Ils masquent d'autres applications malveillantes et leur activité, et prolongent ainsi la persistance de ces applications dans le système d'exploitation. Ils peuvent également dissimuler des fichiers, des processus dans la mémoire d'un ordinateur infecté ou des clés de registre qui exécutent des applications malveillantes. Les rootkits peuvent masquer l'échange de données entre les applications sur l'ordinateur de l'utilisateur et les autres ordinateurs du réseau. |
| Trojan-SMS | Chevaux de Troie qui envoient des messages SMS | Ils infectent des téléphones mobiles et les utilisent pour envoyer des messages SMS vers des numéros payants. |
| Trojan-GameThief | Chevaux de Troie qui volent les données des adeptes de jeux en ligne | Ils volent les comptes des adeptes de jeux en ligne ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. |
| Trojan-Banker | Chevaux de Troie qui volent les données de comptes bancaires. | Ils volent les données des comptes bancaires ou les données des comptes de système de porte-monnaie électronique ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. |

| | | |
|---|---|---|
| Trojan-Mailfinder des adresses email | Chevaux de Troie qui récoltent des adresses email | Ils recueillent les adresses email sur l'ordinateur et les envoient à l'individu malintentionné par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. Les individus malintentionnés utilisent ensuite ces adresses pour diffuser du spam. |
|---|---|---|

- [Outils malveillants](#) 

Sous-catégories : outils malveillants (Malicious_tools)

Niveau de danger : moyen

Contrairement aux autres types de logiciels malveillants, les outils malveillants n'exécutent pas leurs actions immédiatement après leur démarrage. Elles peuvent être stockées et lancées en toute sécurité sur l'ordinateur de l'utilisateur. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants, s'introduire dans des ordinateurs ou exécuter d'autres actions malveillantes.

Les différentes fonctionnalités des outils malveillants sont regroupées en types présentés dans le tableau suivant.

Fonctionnalités des outils malveillants

| Type | Nom | Description |
|--------------------|-------------------------------------|--|
| Constructor | Constructeurs | Ils permettent de créer de nouveaux virus, vers ou chevaux de Troie. Certains constructeurs sont dotés d'une interface standard à base de fenêtres qui permet, à l'aide de menus, de sélectionner le type de programme malveillant à créer, son mode de résistance face aux débogueurs ainsi que d'autres propriétés. |
| Dos | Attaques réseau | Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). |
| Exploit | Exploits | <p>L'exploit est un ensemble de données ou de code qui exploite une vulnérabilité de l'application dans laquelle il est exécuté afin de réaliser une action malveillante quelconque sur l'ordinateur. Par exemple, un exploit peut écrire ou lire des fichiers ou contacter des pages Internet "infectées".</p> <p>Divers exploits exploitent les vulnérabilités de diverses applications et services réseau. L'exploit sous la forme d'un paquet réseau se transmet via le réseau vers de nombreux ordinateurs à la recherche d'ordinateurs possédant des services réseau vulnérables. L'exploit d'un fichier DOC utilise la vulnérabilité de l'éditeur de test. Il peut commencer à exécuter les fonctions intégrées par l'individu malintentionné lorsque l'utilisateur ouvre le fichier infecté. L'exploit intégré à un email recherche les vulnérabilités dans un client de messagerie quelconque. Il peut commencer à exécuter l'action malveillante dès que l'utilisateur ouvre le message infecté dans le client de messagerie.</p> <p>Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploits de type <i>Nuker</i> sont des paquets réseau qui mettent l'ordinateur hors service.</p> |
| FileCryptor | Encodeurs | Ils encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus. |
| Flooder | Programmes de "pollution" du réseau | Ils envoient une multitude de messages via les canaux réseau. Les programmes utilisés pour polluer les canaux IRC (Internet Relay Chats) appartiennent à cette catégorie. |

| | | |
|----------------------|--|--|
| | | La catégorie Flooder ne reprend pas les applications qui "polluent" l'email, les clients IM et les systèmes mobiles. Ces programmes sont regroupés dans des catégories distinctes décrites dans ce tableau (Email-Flooder, IM-Flooder et SMS-Flooder). |
| HackTool | Outils de piratage | Ils permettent de s'emparer de l'ordinateur sur lequel ils sont installés ou d'attaquer un autre ordinateur (par exemple, ajout d'autres utilisateurs au système sans l'autorisation de la victime ; purge des journaux du système afin de dissimuler les traces de leur présence dans le système). Il s'agit de quelques sniffers qui possèdent des fonctions malveillantes telles que l'interception des mots de passe. Les sniffers sont des programmes qui permettent de consulter le trafic réseau. |
| Hoax | Canulars | Ils effraient l'utilisateur à l'aide de messages semblables à ceux que pourrait produire un virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu. |
| Spoofers | Utilitaires d'imitation | Ils envoient des messages et des requêtes réseau au départ d'adresses fictives. Les individus malintentionnés les utilisent pour se faire passer pour l'expéditeur. |
| VirTool | Instruments pour la modification des programmes malveillants | Ils permettent de modifier d'autres programmes malveillants afin de les rendre invisibles pour les logiciels antivirus. |
| Email-Flooder | Programmes qui "inondent" l'email. | Ils envoient de nombreux messages aux adresses email du carnet d'adresses ("pollution du courrier"). Ce flux important de messages empêche l'utilisateur de lire le courrier utile. |
| SMS-Flooder | Programmes de "pollution" des clients IM | Ils envoient de nombreux messages aux utilisateurs de clients IM. Ce flux important de messages empêche l'utilisateur de lire les messages utiles. |
| SMS-Flooder | Programmes de "pollution" des messages SMS | Ils envoient de nombreux messages SMS vers les téléphones portables. |

- [Applications publicitaires](#) 

Sous-catégorie : applications publicitaires (Adware)

Niveau de la menace : moyen

Les applications publicitaires montrent des publicités à l'utilisateur. Elles affichent des bannières publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. Certaines d'entre elles recueillent également des informations marketing sur l'utilisateur qu'elles renvoient à l'auteur : par exemple, catégorie de sites Internet visités, mots clés utilisés dans les recherches. À la différence des chevaux de Troie espions, elles transmettent ces informations avec l'autorisation de l'utilisateur.

- [Numéroteurs automatiques](#) 

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

| Type | Nom | Description |
|----------------------|--|--|
| Client-IRC | Clients de chats | Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants. |
| Dialer | Numéroteurs automatiques | Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur. |
| Downloader | Programmes de téléchargement | Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché. |
| Monitor | Programmes de surveillance | Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs). |
| PSWTool | Récupérateur de mots de passe | Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs. |
| RemoteAdmin | Programmes d'administration à distance | Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer. Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions. |
| Server-FTP | Serveurs FTP | Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP. |
| Server-Proxy | Serveurs proxy | Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| Server-Telnet | Serveurs Telnet | Ils remplissent les fonctions d'un serveur Telnet. Les individus |

| | | |
|--------------------|--|---|
| | | malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet. |
| Server-Web | Serveurs Internet | Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP. |
| RiskTool | Outils utilisés sur l'ordinateur local | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs. |
| NetTool | Outils réseau | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs. |
| Client-P2P | Clients de réseaux d'échange de fichiers | Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants. |
| Client-SMTP | Clients SMTP | Envoient les emails en mode caché. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| WebToolbar | Barre d'outils Internet | Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche. |
| FraudTool | Pseudo-programmes | Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien. |

- [Autres logiciels que des criminels pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles](#) 

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

| Type | Nom | Description |
|----------------------|--|--|
| Client-IRC | Clients de chats | Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants. |
| Dialer | Numéroteurs automatiques | Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur. |
| Downloader | Programmes de téléchargement | Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché. |
| Monitor | Programmes de surveillance | Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs). |
| PSWTool | Récupérateur de mots de passe | Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs. |
| RemoteAdmin | Programmes d'administration à distance | Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer. Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions. |
| Server-FTP | Serveurs FTP | Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP. |
| Server-Proxy | Serveurs proxy | Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| Server-Telnet | Serveurs Telnet | Ils remplissent les fonctions d'un serveur Telnet. Les individus |

| | | |
|--------------------|--|---|
| | | malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet. |
| Server-Web | Serveurs Internet | Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP. |
| RiskTool | Outils utilisés sur l'ordinateur local | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs. |
| NetTool | Outils réseau | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs. |
| Client-P2P | Clients de réseaux d'échange de fichiers | Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants. |
| Client-SMTP | Clients SMTP | Envoient les emails en mode caché. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| WebToolbar | Barre d'outils Internet | Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche. |
| FraudTool | Pseudo-programmes | Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien. |

- [Fichiers compressés pouvant dissimuler un programme malveillant](#) 

Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX.

Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois.

Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Kaspersky Endpoint Security identifie les programmes suivants :

- *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie.
- *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.

- [Fichiers compressés à plusieurs reprises](#) ⓘ

Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX.

Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois.

Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Kaspersky Endpoint Security identifie les programmes suivants :

- *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie.
- *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.


4. Enregistrez vos modifications.

Activation et désactivation de la technologie de désinfection avancée

Si Kaspersky Endpoint Security ne peut pas arrêter l'exécution d'une application malveillante, vous pouvez utiliser la technologie de désinfection active. Par défaut, la désinfection active est désactivée, car cette technologie utilise une quantité importante de ressources informatiques. Par conséquent, vous pouvez activer la désinfection active uniquement lorsque vous [traitez des menaces actives](#).

La désinfection active fonctionne différemment pour les postes de travail et les serveurs. Pour utiliser cette technologie sur les serveurs, vous devez [activer la désinfection active immédiate](#) dans les propriétés de la tâche *Analyse antivirus*. Ce prérequis n'est pas nécessaire pour utiliser la technologie sur les postes de travail.


Pour activer ou désactiver la technologie de désinfection active, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Dans la section **Mode de protection**, cochez ou décochez la case **Appliquer la technologie de désinfection de l'infection active** pour activer ou désactiver la technologie de désinfection avancée.
4. Enregistrez vos modifications.

Il en résulte que l'utilisateur ne peut pas utiliser la plupart des fonctionnalités du système d'exploitation pendant que la désinfection active est en cours. Lorsque la désinfection est terminée, l'ordinateur redémarre.

Activation et désactivation du mode d'économie d'énergie

Pour activer ou désactiver le mode d'économie d'énergie, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Menaces et exclusions**.
3. Dans la section **Performances**, utilisez la case **Reporter les tâches planifiées en cas d'alimentation par batterie** pour activer ou désactiver le mode d'économie d'énergie.


Quand le mode d'économie d'énergie est activé, les tâches suivantes ne sont pas exécutées quand l'ordinateur est alimenté par la batterie, mais si elles sont programmées :

- tâche de mise à jour ;
- tâche d'analyse complète ;
- tâche d'analyse rapide ;
- tâche d'analyse personnalisée ;
- tâche d'analyse de l'intégrité.

4. Enregistrez vos modifications.

Activation et désactivation du mode de transfert des ressources vers d'autres applications

Pour activer ou désactiver le mode de transfert des ressources vers d'autres applications, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Dans la section **Performances**, utilisez la case **Céder les ressources aux autres applications** pour activer ou désactiver la cession de ressources à d'autres applications.

Si ce mode est activé, Kaspersky Endpoint Security reporte l'exécution des tâches si le lancement planifié a été défini pour ces tâches et que leur exécution ralentit le fonctionnement d'autres applications :

- tâche de mise à jour ;
- tâche d'analyse complète ;
- tâche d'analyse rapide ;
- tâche d'analyse personnalisée ;
- tâche d'analyse de l'intégrité.

Le mode de transfert des ressources vers d'autres applications est activé par défaut.


4. Enregistrez vos modifications.

Création et utilisation d'un fichier de configuration

Le fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Endpoint Security permet de réaliser les tâches suivantes :

- Exécuter l'installation locale de Kaspersky Endpoint Security via la ligne de commande selon des paramètres définis à l'avance.
Pour cela, il faut enregistrer le fichier de configuration dans le même dossier que celui où se trouve le paquet de distribution.
- Exécuter l'installation à distance de Kaspersky Endpoint Security via Kaspersky Security Center avec selon des paramètres définis à l'avance.
- Transférer les paramètres de fonctionnement de Kaspersky Endpoint Security d'un ordinateur à l'autre.


Pour créer un fichier de configuration, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Gestion des paramètres**.
3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin où vous voulez enregistrer le fichier de configuration et saisissez son nom.

Pour utiliser le fichier de configuration dans le cadre d'une installation locale ou à distance de Kaspersky Endpoint Security, il faut le nommer install.cfg.

5. Cliquez sur le bouton **Enregistrer**.

Pour importer les paramètres de fonctionnement de Kaspersky Endpoint Security depuis le fichier de configuration, procédez comme suit :


1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Gestion des paramètres**.
3. Cliquez sur le bouton **Importer**.
4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au fichier de configuration.
5. Cliquez sur le bouton **Ouvrir**.

Tous les paramètres de Kaspersky Endpoint Security prendront les valeurs définies dans le fichier de configuration choisi.

Restauration des paramètres par défaut de l'application

Vous pouvez à tout moment restaurer les paramètres recommandés de Kaspersky Endpoint Security. Lorsque les paramètres sont restaurés, le niveau de protection **Recommandé** sera sélectionné pour tous les modules de la protection.

Pour restaurer les paramètres par défaut de l'application, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Gestion des paramètres**.
3. Cliquez sur le bouton **Restaurer**.
4. Cliquez sur le bouton **Enregistrer**.

Échange de messages entre utilisateur et administrateur

Les modules [Contrôle des applications](#), [Contrôle des appareils](#), [Contrôle Internet](#) et [Contrôle évolutif des anomalies](#) permettent aux utilisateurs du réseau local de l'organisation dont les ordinateurs sont dotés de l'application Kaspersky Endpoint Security d'envoyer des messages à l'administrateur.

L'utilisateur peut être amené à envoyer un message à l'administrateur du réseau local de l'entreprise dans les cas suivants :

- Le Contrôle des appareils a bloqué l'accès à l'appareil.
Le modèle du message de demande d'accès à l'appareil bloqué est accessible dans l'interface de Kaspersky Endpoint Security dans la section [Contrôle des appareils](#).
- Le Contrôle des applications a interdit le lancement de l'application.
Le modèle du message de demande d'autorisation du lancement de l'application bloquée est accessible dans l'interface de Kaspersky Endpoint Security dans la section [Contrôle des applications](#).
- Le Contrôle Internet a bloqué l'accès à la ressource Internet.
Le modèle du message de demande d'accès à la ressource Internet bloquée est accessible dans l'interface de Kaspersky Endpoint Security dans la section [Contrôle Internet](#).

Le mode d'envoi des messages, ainsi que le choix du modèle utilisé, dépend de la présence ou non sur l'ordinateur doté de l'application Kaspersky Endpoint Security d'une stratégie active de Kaspersky Security Center et d'une communication avec le Serveur d'administration de Kaspersky Security Center. Les scénarios suivants sont envisageables :

- Si aucune stratégie de Kaspersky Security Center n'est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, le message de l'utilisateur est envoyé à l'administrateur du réseau local de l'organisation par email.
Les champs du message prennent les valeurs des champs du modèle défini dans l'interface locale de Kaspersky Endpoint Security.
- Si une stratégie Kaspersky Security Center est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, Kaspersky Endpoint Security envoie un message standard au Serveur d'administration de Kaspersky Security Center.
Dans ce cas, les messages des utilisateurs sont consultables dans le stockage des événements de Kaspersky Security Center (cf. instructions ci-dessous). Les champs du message prennent les valeurs des champs du modèle défini dans la stratégie de Kaspersky Security Center.
- Si une stratégie de Kaspersky Security Center pour les utilisateurs autonomes est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, le mode d'envoi du message dépendra de la connexion avec Kaspersky Security Center :
 - Si une connexion est établie avec Kaspersky Security Center, Kaspersky Endpoint Security envoie le message standard au Serveur d'administration de Kaspersky Security Center.
 - En l'absence de connexion avec Kaspersky Security Center, le message de l'utilisateur est envoyé à l'administrateur du réseau local de l'entreprise par email.

Dans les deux cas, les champs du message prennent les valeurs des champs du modèle défini dans la stratégie de Kaspersky Security Center.

Pour consulter le message de l'utilisateur dans le référentiel des événements de Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.

L'espace de travail de Kaspersky Security Center affichent tous les événements survenus pendant le fonctionnement de l'application Kaspersky Endpoint Security, y compris les messages envoyés à l'administrateur par les utilisateurs du réseau local de l'organisation.
3. Pour configurer le filtre des événements, il faut choisir l'option **Demandes des utilisateurs** dans la liste déroulante **Événements de la sélection**.
4. Choisissez le message pour l'administrateur.
5. Cliquez sur le bouton **Ouvrir la fenêtre des propriétés de l'événement** dans la partie droite de l'espace de travail de la Console d'administration.

Chiffrement des données

Kaspersky Endpoint Security permet de chiffrer les fichiers et les dossiers enregistrés sur les disques locaux de l'ordinateur et sur les disques amovibles, les disques amovibles et les disques durs en entier. Le chiffrement des données réduit le risque de fuites d'informations en cas de perte ou de vol d'un ordinateur portable, d'un disque amovible ou d'un disque dur ou en cas d'accès d'utilisateurs ou d'applications tierces à ces données. Kaspersky Endpoint Security utilise l'algorithme de chiffrement AES (Advanced Encryption Standard).

Si la licence a expiré, l'application ne chiffre pas les nouvelles données et les anciennes données chiffrées restent chiffrées et accessibles. Dans ce cas, le chiffrement de nouvelles données requiert l'activation de l'application selon une nouvelle licence qui autorise l'utilisation du chiffrement.

En cas d'expiration de la licence, de violation des conditions du Contrat de licence Utilisateur final, de suppression de la clé de licence ou de Kaspersky Endpoint Security ou de ses modules de chiffrement de l'ordinateur de l'utilisateur, il n'est pas garanti que les fichiers chiffrés antérieurement le resteront. Cela s'explique par le fait que certaines applications, comme Microsoft Office Word, créent une copie temporaire des fichiers pendant leur modification. Lorsque le fichier d'origine est enregistré, la copie temporaire remplace le fichier d'origine. Par conséquent, en l'absence de la fonction de chiffrement sur l'ordinateur ou en cas d'indisponibilité de celle-ci, le fichier reste non chiffré.

Kaspersky Endpoint Security protège les données de la manière suivante :

- **Chiffrement des fichiers sur les disques locaux de l'ordinateur.** Vous pouvez [former des listes à partir de fichiers](#) selon l'extension ou selon les groupes d'extensions ou de dossiers situés sur les disques locaux de l'ordinateur. Vous pouvez aussi créer des [règles de chiffrement de fichiers créés par des applications distinctes](#). Après l'application de la stratégie, l'application Kaspersky Endpoint Security chiffre et déchiffre les fichiers suivants :
 - les fichiers ajoutés séparément aux listes pour le chiffrement et le déchiffrement ;
 - les fichiers enregistrés dans les dossiers ajoutés aux listes pour le chiffrement et le déchiffrement ;
 - les fichiers créés des applications distinctes.
- **Chiffrement des disques amovibles.** Vous pouvez indiquer la règle de chiffrement par défaut conformément à laquelle l'application exécute la même action sur tous les disques amovibles ou indiquer des règles de chiffrement pour des disques amovibles distincts.

La priorité d'une règle de chiffrement par défaut est inférieure à celle d'une règle de chiffrement définie pour différents disques amovibles. La priorité des règles de chiffrement définies pour les disques amovibles du modèle d'appareil indiqué est inférieure à celle des règles de chiffrement définies pour les disques amovibles portant un identificateur d'appareil indiqué.

Afin de sélectionner la règle de chiffrement des fichiers sur le disque amovible, Kaspersky Endpoint Security vérifie si le modèle de l'appareil ou son identificateur sont connus. Ensuite, l'application réalise une des opérations suivantes :

- Si le seul le modèle de l'appareil est connu, l'application applique la règle de chiffrement définie pour les disques amovibles de ce modèle, si une telle règle existe.
- Si seul l'identificateur de l'appareil est connu, l'application utilise la règle de chiffrement définie pour les disques amovibles portant cet identificateur d'appareil, si une telle règle existe.
- Si le modèle de l'appareil et son identificateur sont connus, l'application utilise la règle de chiffrement définie pour les disques amovibles portant cet identificateur connu, si une telle règle existe. Si cette règle n'existe pas, mais qu'il existe une règle de chiffrement créée pour les disques amovibles de ce modèle d'appareil,

l'application l'applique. Si aucune règle de chiffrement n'est définie pour aucun identificateur d'appareil, ni pour aucun modèle d'appareil, l'application adopte la règle de chiffrement par défaut.

- Si le modèle et l'identificateur de l'appareil sont inconnus, l'application utilise la règle de chiffrement par défaut.

L'application permet de préparer le disque amovible pour travailler en mode portable avec les fichiers qui sont chiffrés sur ce dernier. Après l'activation du mode portable, l'utilisation des fichiers chiffrés devient accessible sur les disques amovibles connectés à l'ordinateur dont la fonction de chiffrement est inaccessible.

- **Administration des règles d'accès des applications aux fichiers chiffrés.** Vous pouvez créer pour n'importe quelle application une règle d'accès aux fichiers chiffrés qui interdira l'accès aux fichiers chiffrés ou qui l'autorisera uniquement sous la forme de texte chiffré, soit une séquence de caractères obtenues après l'application du chiffrement.
- **Création d'archives chiffrées.** Vous pouvez créer des archives chiffrées et les protéger par un mot de passe. Pour accéder au contenu de ces archives chiffrées, il faut saisir le mot de passe défini pour protéger l'accès à ces archives. Ces archives peuvent être envoyées en toute sécurité sur le réseau ou sur des disques amovibles.
- **Chiffrement du disque.** Vous pouvez choisir la technologie du chiffrement : Kaspersky Disk Encryption ou le Chiffrement de disque BitLocker (ci-après "BitLocker").

BitLocker est une technologie qui fait partie du système d'exploitation Windows. Si l'ordinateur est équipé d'un module Trusted Platform Module, BitLocker l'utilise pour conserver les clés de récupération qui permettent d'accéder au disque dur chiffré. Lors du chargement de l'ordinateur, BitLocker sollicite la clé de récupération du disque dur au module de plateforme sécurisée, puis débloque le disque. Vous pouvez configurer l'utilisation du mot de passe et/ou d'un code PIN pour accéder aux clés de restauration.

Vous pouvez désigner une règle de chiffrement du disque par défaut et composer une liste de disques à exclure du chiffrement. Kaspersky Endpoint Security chiffre le disque secteur par secteur après l'application de la stratégie de Kaspersky Security Center. L'application chiffre toutes les sections logiques des disques durs à la fois.

Une fois que les disques durs système auront été chiffrés, l'accès à ceux-ci et le chargement du système d'exploitation lors du prochain démarrage de l'ordinateur seront possibles uniquement après avoir suivi la procédure d'authentification à l'aide de l'[Agent d'authentification](#). Pour ce faire, il faut saisir le mot de passe du token ou de la carte à puce connecté à l'ordinateur, ou le nom et le mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur système du réseau local de l'organisation à l'aide de la tâche [Gérer les comptes de l'Agent d'authentification](#). Ces comptes utilisateur reposent sur les comptes utilisateur Microsoft Windows utilisés pour accéder au système d'exploitation. Vous pouvez également [utiliser la technologie d'authentification unique \(SSO, Single Sign-On\)](#), qui permet d'accéder automatiquement au système d'exploitation à l'aide du nom et du mot de passe du compte utilisateur de l'Agent d'Authentification.

Si une copie sauvegarde a été créée pour l'ordinateur puis que les données de celui-ci ont été chiffrées et que la copie de sauvegarde de l'ordinateur a été restaurée et les données à nouveau chiffrées, Kaspersky Security crée des doubles des comptes de l'Agent d'authentification. Pour supprimer les doublons, utilisez l'utilitaire klmover avec l'argument `dupfix`. L'utilitaire klmover est fourni avec la distribution de Kaspersky Security Center. Pour en savoir plus sur son fonctionnement, lisez l'aide de Kaspersky Security Center.

Les disques durs chiffrés sont accessibles uniquement depuis des ordinateurs équipés de l'application Kaspersky Endpoint Security avec la fonction de chiffrement du disque. Cette condition réduit au minimum le risque de fuite d'informations stockées sur le disque dur chiffré en cas d'utilisation de ce disque en dehors du réseau local de l'organisation.

Pour le chiffrement des disques durs et amovibles, vous pouvez utiliser la fonction **Chiffrer uniquement l'espace occupé**. Il est conseillé d'utiliser cette fonction seulement pour les nouveaux appareils qui n'ont jamais été utilisés. Si vous appliquez le chiffrement à un appareil déjà utilisé, il est recommandé de chiffrer tout l'appareil. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites.

Avant le chiffrement, Kaspersky Endpoint Security reçoit la carte des secteurs du système de fichiers. Lors du premier flux, ce sont les secteurs occupés par des fichiers au moment du lancement du chiffrement qui seront chiffrés. Dans le deuxième flux, les secteurs chiffrés sont les secteurs dans lesquels une écriture a eu lieu après le début du chiffrement. À la fin du chiffrement, tous les secteurs contenant des données sont chiffrés.

Si l'utilisateur, après le chiffrement, supprime un fichier, alors les secteurs dans lesquels se trouvait ce fichier deviennent disponibles pour d'autres écritures d'informations au niveau du système de fichiers, mais restent chiffrés. Ainsi, au fur et à mesure de l'enregistrement de fichiers sur un nouvel appareil, en cas de lancement régulier du chiffrement avec la fonction activée **Chiffrer uniquement l'espace occupé**, tous les secteurs de l'ordinateur seront chiffrés après un certain temps.

Les données indispensables au déchiffrement des objets sont offertes par le Serveur d'administration de Kaspersky Security Center qui gère l'ordinateur au moment du chiffrement. Si, pour une raison quelconque, un ordinateur avec des objets chiffrés se retrouve sous le contrôle d'un autre Serveur d'administration, vous pourrez accéder aux données chiffrées de l'une des manières suivantes :

- Serveurs d'administration dans une hiérarchie :
 - Il n'est pas nécessaire de prendre d'autres mesures. L'utilisateur aura toujours accès aux objets chiffrés. Les clés de chiffrement s'appliquent à tous les Serveurs d'administration.
- Les serveurs d'administration sont dispersés :
 - Demander l'accès aux objets chiffrés à l'administrateur du réseau local de l'organisation.
 - Restaurer les données sur les appareils chiffrés à l'aide de l'utilitaire de restauration.
 - Restaurer la configuration du Serveur d'administration de Kaspersky Security Center qui gérait l'ordinateur au moment du chiffrement à partir de la copie de sauvegarde. Utiliser cette configuration sur le Serveur d'administration qui gérait l'ordinateur avec les objets chiffrés.

En l'absence d'accès aux données chiffrées, suivez les instructions spéciales sur l'utilisation des données chiffrées ([Restauration de l'accès aux données chiffrées](#), [Utilisation des appareils chiffrés en l'absence d'accès à ceux-ci](#)).

Restrictions de la fonction de chiffrement

Le chiffrement des données possède les restrictions suivantes :

- L'application crée des fichiers de service pendant le chiffrement. Pour leur sauvegarde, il faut environ 0,5 % d'espace libre non fragmenté sur le disque dur de l'ordinateur. S'il n'y a pas assez d'espace libre non fragmenté sur le disque dur, le chiffrement n'est pas lancé tant que cette condition n'est pas remplie.
- Vous pouvez gérer l'ensemble des modules de chiffrement des données dans la Console d'administration de Kaspersky Security Center et dans Kaspersky Security Center 12 Web Console. Dans Kaspersky Security Center Cloud Console, vous pouvez administrer BitLocker uniquement.
- Le chiffrement des données n'est disponible que lors de l'utilisation de Kaspersky Endpoint Security avec le système d'administration Kaspersky Security Center ou Kaspersky Security Center Cloud Console (BitLocker uniquement). Le chiffrement des données lors de l'utilisation de Kaspersky Endpoint Security en mode hors connexion n'est pas possible car Kaspersky Endpoint Security enregistre les clés de chiffrement dans Kaspersky Security Center.
- Si l'application Kaspersky Endpoint Security est installée sur un ordinateur qui tourne sous un système d'exploitation [Microsoft Windows pour serveurs](#), seul le chiffrement du disque à l'aide de la technologie Chiffrement de disque BitLocker est accessible. Si Kaspersky Endpoint Security a été installé sur un ordinateur

s'exécutant sous un système d'exploitation Windows pour poste de travail, la fonction de chiffrement des données est entièrement disponible.

La fonction de chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption n'est pas accessible pour les disques durs qui ne sont pas conformes à la configuration matérielle et logicielle.

La compatibilité entre la fonction de chiffrement du disque de Kaspersky Endpoint Security et Kaspersky Anti-Virus for UEFI n'est pas prise en charge. Kaspersky Anti-Virus for UEFI se lance avant le chargement du système d'exploitation. Lors du chiffrement du disque, l'application découvre l'absence d'un système d'exploitation sur l'ordinateur. Cela entraîne l'arrêt sur échec de Kaspersky Anti-Virus for UEFI. Le chiffrement des fichiers n'influence pas le fonctionnement de Kaspersky Anti-Virus for UEFI.

Kaspersky Endpoint Security prend en charge les configurations suivantes :

- Disques durs, disques SSD et clés USB.

La technologie Kaspersky Disk Encryption (FDE) permet d'utiliser des disques SSD tout en préservant les performances et la durée de vie des disques SSD.

- Disques reliés par bus : SCSI, ATA, IEEE1394, USB, RAID, SAS, SATA, NVME.
- Disques non amovibles connectés par bus SD ou MMC.
- Disques avec des secteurs de 512 octets.
- Disques avec des secteurs de 4096 octets qui émulent 512 octets.
- Disques avec le type de partitions suivant : GPT, MBR et VBR (disques amovibles).
- Logiciel intégré de la norme UEFI 64 et Legacy BIOS.
- Logiciel intégré de la norme UEFI avec prise en charge de la technologie Secure Boot.

Secure Boot est une technologie conçue pour vérifier les signatures numériques des applications et des pilotes de chargeurs UEFI. Secure Boot bloque le démarrage des applications et des pilotes UEFI qui ne sont pas signés ou qui sont signés par des éditeurs inconnus. Kaspersky Disk Encryption (FDE) prend entièrement en charge la technologie Secure Boot. L'Agent d'authentification est signé par un certificat Microsoft Windows UEFI Driver Publisher.

Sur certains appareils (par exemple, Microsoft Surface Pro et Microsoft Surface Pro 2), il se peut qu'une liste obsolète de certificats de vérification de signature numérique soit installée par défaut. Avant de chiffrer le disque, vous devez mettre à jour la liste des certificats.

- Logiciel intégré de la norme UEFI avec prise en charge de la technologie Fast Boot.

Fast Boot est une technologie qui permet aux ordinateurs de démarrer plus rapidement. Lorsque la technologie Fast Boot est activée, l'ordinateur ne charge normalement que l'ensemble minimum de pilotes UEFI requis pour le démarrage du système d'exploitation. Lorsque la technologie Fast Boot est activée, il se peut que les claviers USB, les souris, les jetons USB, les pavés tactiles et les écrans tactiles ne pas fonctionnent pas lorsque l'Agent d'authentification est en cours d'exécution.

Pour utiliser la technologie Kaspersky Disk Encryption (FDE), il est recommandé de désactiver la technologie Fast Boot. Vous pouvez utiliser l'[utilitaire de test FDE](#) pour tester le fonctionnement de Kaspersky Disk Encryption (FDE).

Kaspersky Endpoint Security n'est pas compatible avec les configurations suivantes :

- schéma selon lequel le chargeur se trouve sur un disque et le système d'exploitation, sur un autre ;
- logiciel inséré standard UEFI 32 ;
- système avec technologie Intel® Rapid Start Technology et disques avec partition de mise en veille prolongée, même si l'utilisation d'Intel® Rapid Start Technology est désactivée ;
- disques au format MBR comptant plus de 10 partitions étendues ;
- système avec un fichier swap situé sur un disque non système ;
- système à démarrage multiple avec plusieurs systèmes d'exploitation installés simultanément ;
- sections dynamiques (seules les sections du type principal sont prises en charge) ;
- disques avec moins de 0,5 % d'espace disque libre non fragmenté ;
- disques dont la taille de secteur, différente de 512 ou 4 096 octets, émulent 512 octets ;
- disques hybrides.
- système avec des chargeurs tiers ;
- disques avec des répertoires NTFS compressés ;
- La technologie Kaspersky Disk Encryption (FDE) est incompatible avec d'autres technologies de chiffrement de disque complet (comme BitLocker, McAfee Drive Encryption et WinMagic SecureDoc).
- La technologie Kaspersky Disk Encryption (FDE) est incompatible avec la technologie Express Cache.
- La création, la suppression et la modification de partitions sur un disque chiffré ne sont pas prises en charge. Vous risquez de perdre des données.
- Le formatage des systèmes de fichiers n'est pas pris en charge. Vous risquez de perdre des données.
Si vous devez formater un disque qui a été chiffré au moyen de la technologie Kaspersky Disk Encryption (FDE), formatez le disque sur un ordinateur qui ne dispose pas de Kaspersky Endpoint Security for Windows et utilisez uniquement un chiffrement complet du disque.
Un disque dur chiffré qui a été formaté au moyen de l'option de formatage rapide peut être reconnu par erreur comme étant chiffré lors de la prochaine connexion à un ordinateur sur lequel est installé Kaspersky Endpoint Security for Windows. Les données des utilisateurs ne seront pas disponibles.
- L'Agent d'authentification ne prend pas en charge plus de 100 comptes.
- La technologie Single Sign-On est incompatible avec les autres technologies de concepteurs tiers.
- La technologie Kaspersky Disk Encryption (FDE) n'est pas prise en charge sur les modèles d'appareils suivants :
 - Dell Latitude E6410 (mode UEFI)
 - HP Compaq nc8430 (mode Legacy BIOS)
 - Lenovo Think Center 8811 (mode Legacy BIOS)
- L'Agent d'authentification ne permet pas de travailler avec des jetons USB lorsque la fonctionnalité Legacy USB Support est activée. Seule une authentification par mot de passe sera possible sur l'ordinateur.

- Lorsque vous chiffrez un disque en mode Legacy BIOS, il vous est conseillé d'activer la fonctionnalité Legacy USB Support sur les modèles d'appareils suivants :
 - Acer Aspire 5560G
 - Acer Aspire 6930
 - Acer TravelMate 8572T
 - Dell Inspiron 1420
 - Dell Inspiron 1545
 - Dell Inspiron 1750
 - Dell Inspiron N4110
 - Dell Latitude E4300
 - Dell Studio 1537
 - Dell Studio 1569
 - Dell Vostro 1310
 - Dell Vostro 1320
 - Dell Vostro 1510
 - Dell Vostro 1720
 - Dell Vostro V13
 - Dell XPS L502x
 - Fujitsu Celsius W370
 - Fujitsu LifeBook A555
 - HP Compaq dx2450 Microtower PC
 - Lenovo G550
 - Lenovo ThinkPad L530
 - Lenovo ThinkPad T510
 - Lenovo ThinkPad W540
 - Lenovo ThinkPad X121e
 - Lenovo ThinkPad X200s (74665YG)
 - Samsung R530
 - Toshiba Satellite A350

- Toshiba Satellite U400 100
- MSI 760GM-E51 (carte mère)

Modification de la longueur de la clé de chiffrement (AES56/AES256)

Kaspersky Endpoint Security utilise l'algorithme de chiffrement AES (Advanced Encryption Standard). Kaspersky Endpoint Security prend en charge l'algorithme de chiffrement AES avec une longueur de clé réelle de 256 et 56 bits. L'algorithme de chiffrement des données dépend de la bibliothèque de chiffrement AES incluse dans la distribution : *Strong encryption (AES256)* ou *Lite encryption (AES56)*. La bibliothèque de chiffrement AES est installée en même temps que l'application.

La modification de la longueur de la clé de chiffrement est uniquement possible avec Kaspersky Endpoint Security 11.2.0 et suivants.

La modification de la longueur d'une clé de chiffrement comprend les étapes suivantes :

1. Déchiffrez les objets que Kaspersky Endpoint Security avait chiffré avant de lancer la modification de la longueur de la clé de chiffrement.
 - a. [Déchiffrez les disques durs.](#)
 - b. [Déchiffrez les fichiers sur les disques locaux.](#)
 - c. [Déchiffrez les disques amovibles.](#)

Une fois que la longueur de la clé de chiffrement des objets a été modifiée, les objets chiffrés antérieurement ne sont plus disponibles.

2. [Supprimez Kaspersky Endpoint Security.](#)
3. [Installez Kaspersky Endpoint Security](#) à l'aide du paquet de distribution de Kaspersky Endpoint Security avec une autre bibliothèque de chiffrement.

Vous pouvez également modifier la longueur de la clé de chiffrement via une mise à jour de l'application. La modification de la longueur de la clé via une mise à jour de l'application est disponible dans les conditions suivantes :

- Kaspersky Endpoint Security version 10, Service Pack 2 et suivantes est installé sur l'ordinateur.
- Aucun module de chiffrement de données n'est installé sur l'ordinateur (Chiffrement des fichiers, Chiffrement du disque, Administration de BitLocker).

Par défaut, les modules de chiffrement des données ne sont pas inclus dans Kaspersky Endpoint Security. Le module d'administration BitLocker n'affecte pas la modification de la longueur de la clé de chiffrement.

Pour modifier la longueur de la clé de chiffrement, exécutez le fichier kes_win.msi ou setup_kes.exe à partir du paquet de distribution doté de la bibliothèque de chiffrement souhaitée. Vous pouvez également mettre à jour l'application à distance à l'aide du paquet d'installation.

Il est impossible de modifier la longueur de la clé de chiffrement à l'aide du paquet de distribution de la même version de l'application installée sur votre ordinateur sans désinstaller préalablement l'application.

Kaspersky Disk Encryption

La technologie Kaspersky Disk Encryption est disponible uniquement sur les ordinateurs tournant sous un système d'exploitation Windows pour postes de travail. Pour les ordinateurs tournant sous un système d'exploitation Windows pour serveurs, utilisez la technologie chiffrement de disque BitLocker.

Kaspersky Endpoint Security prend en charge le chiffrement du disque dans les systèmes de fichiers FAT32, NTFS et exFat.

Avant de lancer la tâche de chiffrement du disque, l'application exécute une série d'analyses visant à confirmer la possibilité d'appliquer le chiffrement à l'appareil, y compris une analyse de compatibilité du disque dur système avec l'Agent d'authentification ou avec les modules de chiffrement BitLocker. Pour vérifier la compatibilité, il faut redémarrer l'ordinateur. Après le redémarrage de l'ordinateur, l'application exécute toutes les analyses nécessaires en mode automatique. Si l'analyse de compatibilité réussit, la tâche de chiffrement du disque s'exécute après le démarrage du système d'exploitation et le lancement de l'application. Si durant le processus d'analyse, l'incompatibilité du disque dur système avec l'Agent d'authentification ou avec les modules de chiffrement BitLocker est détectée, il faut redémarrer l'ordinateur à l'aide du bouton (Reset). Kaspersky Endpoint Security consigne les informations relatives à cette incompatibilité. En fonction de ces informations, l'application ne lance pas le chiffrement complet du disque au démarrage du système d'exploitation. Les informations sur cet événement sont affichées dans les rapports de Kaspersky Security Center.

Si la configuration matérielle a été modifiée, l'analyse de la compatibilité du disque dur système avec l'Agent d'authentification ou les modules de chiffrement BitLocker doit être précédée de la suppression des informations sur les incompatibilités obtenues par l'application lors de l'analyse précédente. Pour ce faire, il faut saisir la commande `avp pbatestreset` dans la ligne de commande avant le chiffrement du disque. Si, suite à l'analyse de compatibilité du disque dur système avec l'Agent d'authentification, le système d'exploitation ne démarre pas, il est nécessaire de [supprimer les objets et données restants au terme du fonctionnement test de l'Agent d'authentification](#) à l'aide de l'utilitaire de restauration, puis de lancer Kaspersky Endpoint Security et d'exécuter à nouveau la commande `avp pbatestreset`.

Après le lancement du chiffrement du disque, Kaspersky Endpoint Security chiffre tout ce qui est enregistré sur les disques durs.

Si pendant le chiffrement du disque, l'utilisateur éteint ou redémarre l'ordinateur, l'Agent d'authentification est téléchargé avant le prochain démarrage du système d'exploitation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le chiffrement du disque.

Si le système d'exploitation passe en mode d'hibernation (hibernation mode) pendant le chiffrement du disque, l'Agent d'authentification est alors téléchargé lorsque le système d'exploitation sort du mode d'hibernation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le chiffrement du disque.

Si le système d'exploitation passe en mode veille pendant l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security reprend le chiffrement du disque, sans charger l'Agent d'authentification, lorsque le système d'exploitation sort du mode veille.

L'authentification de l'utilisateur dans l'Agent d'authentification peut s'exécuter par deux moyens :

- via la saisie du nom d'utilisateur et du mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur du réseau local de l'organisation via Kaspersky Security Center ;
- via la saisie du mot de passe du token ou de la carte à puce rattaché à l'ordinateur.

L'utilisation du token ou de la carte à puce est disponible uniquement si les disques durs de l'ordinateur sont chiffrés à l'aide d'un algorithme AES256. Si les disques durs de l'ordinateur ont été chiffrés à l'aide d'un algorithme de chiffrement AES56, le fichier de certificat électronique ne pourra pas être ajouté à la commande.

L'Agent d'authentification prend en charge les dispositions de clavier des langues suivantes :

- Anglais (Royaume-Uni) ;
- Anglais (E-U) ;
- Arabe (Algérie, Maroc, Tunisie, disposition AZERTY) ;
- Espagnol (Amérique latine) ;
- Italien ;
- Allemand (Allemagne et Autriche) ;
- Allemand (Suisse) ;
- Portugais (Brésil, disposition ABNT2) ;
- Russe (pour clavier IBM à 105 touches/Windows avec disposition ЙЦУКЕН) ;
- Turc (disposition QWERTY) ;
- Français (France) ;
- Français (Suisse) ;
- Français (Belgique, disposition AZERTY) ;
- Japonais (pour clavier à 106 touches, disposition QWERTY).

La disposition du clavier devient disponible dans l'Agent d'authentification si elle est ajoutée aux paramètres de langue et aux normes régionales du système d'exploitation. Elle est accessible via l'écran d'accueil de Microsoft Windows.

Si le nom du compte utilisateur de l'Agent d'authentification contient des caractères qui ne peuvent être saisis à l'aide des claviers disponibles dans l'Agent d'authentification, l'accès aux disques durs chiffrés est possible seulement après leur récupération à l'aide de l'utilitaire de restauration ou après [la restauration du nom et le mot de passe du compte utilisateur de l'Agent d'authentification](#).

Particularités du chiffrement des disques SSD

L'application permet de chiffrer les disques SSD, les disques hybrides SSHD et les disques dotés de la fonctionnalité Intel Smart Response. L'application ne prend pas en charge le chiffrement des disques avec la fonctionnalité Intel Rapid Start. Désactivez la fonctionnalité Intel Rapid Start avant de chiffrer un disque de ce type.

Le chiffrement des disques SSD présente les caractéristiques suivantes :

- Si un disque SSD est neuf et ne contient aucune donnée confidentielle, [activez le chiffrement de l'espace occupé uniquement](#). Cette action vous permet de remplacer les secteurs du disque appropriés.
- Si un disque SSD est utilisé et qu'il contient des données confidentielles, sélectionnez l'une des options suivantes :
 - Effacez complètement le disque SSD (Secure Erase), installez le système d'exploitation et [exécutez le chiffrement du disque SSD en activant l'option permettant de chiffrer uniquement l'espace occupé](#).
 - Exécutez le chiffrement du disque SSD en désactivant l'option permettant de chiffrer uniquement l'espace occupé.

Le chiffrement d'un disque SSD nécessite de 5 à 10 Go d'espace libre. Les exigences en matière d'espace libre pour le stockage des données d'administration de chiffrement sont indiquées dans le tableau ci-dessous.

Exigences en matière d'espace libre pour le stockage des données d'administration de chiffrement

| Taille du disque SSD (Go) | Espace libre sur la partition principale du disque SSD (Mo) | Espace libre sur la partition secondaire du disque SSD (Mo) |
|---------------------------|---|---|
| 128 | 250 | 64 |
| 256 | 250 | 640 |
| 512 | 300 | 128 |

Chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption

Avant de lancer le chiffrement du disque, il est recommandé de s'assurer que l'ordinateur n'est pas infecté. Pour ce faire, lancez une analyse complète ou une analyse des zones critiques de l'ordinateur. Le chiffrement du disque sur un ordinateur infecté par un rootkit peut provoquer le dysfonctionnement de l'ordinateur.

Pour réaliser le chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
6. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Kaspersky Disk Encryption**.

L'application de la technologie de chiffrement Kaspersky Disk Encryption est impossible si sur l'ordinateur possède des disques durs chiffrés à l'aide de BitLocker.

7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Chiffrer tous les disques durs**.

Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel l'application est installée peut être lancé après le chiffrement de l'ensemble des disques durs.

Si certains disques durs doivent être exclus du chiffrement, [consignez-les dans une liste](#).

8. Configurez les règles pour l'ajout de comptes d'Agent d'authentification pendant le chiffrement du disque. L'Agent permet à un utilisateur de s'authentifier pour accéder à des disques chiffrés et de charger le système d'exploitation. Pour ajouter automatiquement des comptes d'Agent d'authentification, configurez les paramètres suivants :

- **Pendant le chiffrement, créer automatiquement des comptes de l'Agent d'authentification pour les utilisateurs Windows.** Si cette case est cochée, l'application crée des comptes de l'Agent d'authentification en fonction de la liste des comptes d'utilisateurs Windows sur l'ordinateur. Par défaut, Kaspersky Endpoint Security utilise tous les comptes locaux et de domaine avec lesquels l'utilisateur s'est connecté au système d'exploitation au cours des 30 derniers jours.
- **Créer automatiquement des comptes de l'Agent d'authentification pour tous les utilisateurs de cet ordinateur lors de la connexion.** Si cette case est cochée, l'application vérifie les informations relatives aux comptes utilisateur Windows sur l'ordinateur avant de lancer l'Agent d'authentification. Si Kaspersky Endpoint Security détecte un compte utilisateur Windows qui ne dispose pas de compte d'Agent d'authentification, l'application créera un nouveau compte pour accéder aux disques chiffrés. Le nouveau compte de l'Agent d'authentification présentera les paramètres par défaut suivants : ouverture de session protégée par mot de passe uniquement et changement de mot de passe lors de la première authentification. Par conséquent, vous n'avez pas besoin d'[ajouter manuellement des comptes d'Agent d'authentification](#) en utilisant la tâche *Gérer les comptes de l'Agent d'authentification* pour les ordinateurs avec des disques déjà chiffrés.

Si vous avez désactivé la création automatique de comptes d'Agent d'authentification, vous pouvez [ajouter manuellement des comptes d'Agent d'authentification](#) en utilisant la tâche *Administrer les comptes*. Vous pouvez également utiliser cette tâche pour modifier les paramètres des comptes de l'Agent d'authentification qui ont été créés automatiquement.

9. Pour plus de facilité, vous pouvez enregistrer le nom utilisateur dans la mémoire de l'Agent d'authentification afin que l'utilisateur n'ait qu'à saisir un mot de passe lors de sa prochaine connexion au système. Pour ce faire, cochez la case **Enregistrer le nom d'utilisateur saisi dans l'Agent d'authentification**.

10. Choisissez un des modes de chiffrement suivants :

- Si vous voulez appliquer le chiffrement uniquement aux secteurs du disque dur qui sont occupés par des fichiers, cochez la case **Chiffrer uniquement l'espace occupé**.

Si vous appliquez le chiffrement à un disque déjà utilisé, il est recommandé de chiffrer tout le disque. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites. L'utilisation de la fonction **Chiffrer uniquement l'espace occupé** est recommandée pour les nouveaux disques jamais utilisés jusqu'à présent.

- Si vous voulez appliquer le chiffrement à tout le disque dur, décochez la case **Chiffrer uniquement l'espace occupé**.

Si l'appareil avait été chiffré à l'aide de la fonction **Chiffrer uniquement l'espace occupé**, après l'application de la stratégie en mode **Chiffrer tous les disques durs**, les secteurs qui n'hébergent pas de fichiers ne seront toujours pas chiffrés.

11. Si un problème d'incompatibilité matérielle se produit pendant le chiffrement de l'ordinateur, vous pouvez cocher la case **Utiliser Legacy USB Support**.

Legacy USB Support est une fonction BIOS/UEFI qui permet d'utiliser des appareils USB (comme un token) pendant la phase de démarrage d'un ordinateur avant le lancement du système d'exploitation (mode BIOS). La fonction Legacy USB Support n'a pas d'impact sur la prise en charge des appareils USB après le lancement du système d'exploitation.

Lorsque la fonction Legacy USB Support est activée, l'Agent d'authentification en mode BIOS ne prend pas en charge l'utilisation de jetons via USB. Il est recommandé d'utiliser la fonction uniquement en cas de problèmes d'incompatibilités avec le matériel et seulement sur les ordinateurs où le problème est apparu.

12. Enregistrez vos modifications.

Vous pouvez utiliser l'outil Surveillance du chiffrement pour contrôler le processus de chiffrement ou de déchiffrement du disque sur l'ordinateur d'un utilisateur. Vous pouvez exécuter l'outil Surveillance du chiffrement à partir de la [fenêtre principale de l'application](#).

Si les disques durs système sont chiffrés, l'Agent d'authentification est chargé avant le démarrage du système d'exploitation. L'Agent d'authentification permet de réaliser la procédure d'authentification pour obtenir l'accès aux disques durs système chiffrés et pour démarrer le système d'exploitation. Le système d'exploitation est chargé après la réussite de l'authentification. Lors des prochains redémarrages du système d'exploitation, il faudra suivre à nouveau la procédure d'authentification.

Composition de la liste des disques durs exclus du chiffrement

Vous pouvez composer la liste des exclusions du chiffrement seulement pour la technologie Kaspersky Disk Encryption.

Pour composer la liste des disques durs à exclure du chiffrement, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
6. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Kaspersky Disk Encryption**.

Le tableau **Ne pas chiffrer les disques durs suivants** reprend les enregistrements relatifs aux disques durs qui ne seront pas chiffrés par l'application. Ce tableau est vide si vous n'avez pas créé de liste de disques durs à exclure du chiffrement.

7. Si vous souhaitez ajouter des disques durs à la liste des disques durs qui ne seront pas chiffrés par l'application, procédez comme suit :

a. Cliquez sur le bouton **Ajouter**.

La fenêtre **Ajout d'appareils de la liste Kaspersky Security Center** s'ouvre.

b. Dans la fenêtre **Ajout d'appareils de la liste Kaspersky Security Center**, définissez les valeurs des paramètres **Nom**, **Ordinateur**, **Type de disque**, **Kaspersky Disk Encryption**.

c. Cliquez sur le bouton **Actualiser**.

d. Dans la colonne **Nom**, cochez les cases dans les lignes du tableau qui correspondent aux disques durs que vous souhaitez ajouter à la liste des disques durs exclus du chiffrement.

e. Cliquez sur le bouton **OK**.

Les disques durs sélectionnés sont repris dans le tableau **Ne pas chiffrer les disques durs suivants**.

8. Si vous souhaitez supprimer des disques durs du tableau des exclusions, sélectionnez une ou plusieurs lignes du tableau **Ne pas chiffrer les disques durs suivants**, puis cliquez sur **Supprimer**.

Pour sélectionner plusieurs lignes dans le tableau, sélectionnez-les en maintenant la touche **CTRL** enfoncée.

9. Enregistrez vos modifications.

Exportation et importation de la liste des disques durs à exclure du chiffrement

Vous pouvez exporter la liste des exclusions de chiffrement des disques durs dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'exclusions du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions ou pour procéder à la migration des exclusions vers un autre serveur.

[Comment exporter et importer une liste d'exclusions de chiffrement des disques durs dans la Console d'administration \(MMC\)](#)²

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
6. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Kaspersky Disk Encryption**.
Le tableau **Ne pas chiffrer les disques durs suivants** reprend les enregistrements relatifs aux disques durs qui ne seront pas chiffrés par l'application.
7. Pour exporter la liste des exclusions, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.
Si vous n'avez sélectionné aucune exclusion, Kaspersky Endpoint Security exportera toutes les exclusions.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
8. Pour importer la liste des règles, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
9. Enregistrez vos modifications.

[Comment exporter et importer une liste d'exclusions de chiffrement des disques durs dans Web Console ?](#)

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste d'exclusions.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Chiffrement des données** → **Chiffrement du disque**.
5. Sélectionnez la technologie **Kaspersky Disk Encryption** et suivez le lien pour configurer les paramètres.
Les paramètres de chiffrement s'affichent.
6. Cliquez sur le lien **Exclusions**.
7. Pour exporter la liste des règles, procédez comme suit :
 - a. Sélectionnez les exclusions que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.
 - d. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - e. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
8. Pour importer la liste des règles, procédez comme suit :
 - a. Cliquez sur le bouton **Importer**.
 - b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.
 - c. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
9. Enregistrez vos modifications.

Activation de l'utilisation de la technologie d'authentification unique (SSO)

La technologie d'authentification unique (SSO) vous permet de vous connecter automatiquement au système d'exploitation à l'aide des informations d'identification de l'Agent d'authentification.

Lors de l'utilisation de la technologie d'authentification unique, l'Agent d'authentification ignore les exigences de sécurité du mot de passe spécifiées dans Kaspersky Security Center. Vous pouvez définir les exigences de sécurité du mot de passe dans les paramètres du système d'exploitation.

La technologie d'authentification unique est incompatible avec les fournisseurs d'identifiants tiers.

Procédure d'activation de l'utilisation de la technologie d'authentification unique dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
6. Dans le groupe **Paramètres de mot de passe**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre qui s'ouvre, sous l'onglet **Agent d'authentification**, cochez la case **Utiliser la technologie d'authentification unique (SSO)**.
8. Enregistrez vos modifications.

L'utilisateur ne doit réaliser la procédure d'authentification qu'une seule fois à l'aide de l'agent.

L'authentification n'est pas requise pour charger le système d'exploitation. Le système d'exploitation se charge automatiquement.

Procédure d'activation de l'utilisation de la technologie d'authentification unique dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez activer l'utilisation de la technologie d'authentification unique.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à **Chiffrement des données** → **Chiffrement du disque**.
5. Sélectionnez la technologie **Kaspersky Disk Encryption** et suivez le lien pour configurer les paramètres.
Les paramètres de chiffrement s'affichent.
6. Dans la section **Paramètres de mot de passe**, cochez la case **Utiliser la technologie d'authentification unique (SSO)**.
7. Cliquez sur le bouton **OK**.

L'utilisateur ne doit réaliser la procédure d'authentification qu'une seule fois à l'aide de l'agent.
L'authentification n'est pas requise pour charger le système d'exploitation. Le système d'exploitation se charge automatiquement.

Pour que la technologie d'authentification unique fonctionne, le mot de passe du compte Windows et le mot de passe du compte utilisateur d'Agent d'authentification doivent correspondre. Si les mots de passe ne correspondent pas, l'utilisateur doit exécuter la procédure d'authentification deux fois : dans l'interface de l'Agent d'authentification et avant le chargement du système d'exploitation. Ensuite, Kaspersky Endpoint Security remplace le mot de passe du compte de l'Agent d'authentification par le mot de passe du compte Windows.

Administration des comptes utilisateur de l'Agent d'authentification

L'Agent d'authentification est nécessaire pour utiliser les disques protégés à l'aide de la technologie Kaspersky Disk Encryption (FDE). L'utilisateur doit s'authentifier à l'aide de l'agent avant le chargement du système d'exploitation. Pour configurer les paramètres d'authentification des utilisateurs, utilisez tâche *Gérer les comptes de l'Agent d'authentification*. Vous pouvez utiliser à la fois des tâches locales pour des ordinateurs individuels et des tâches de groupe pour des ordinateurs de groupes d'administration distincts ou une sélection d'ordinateurs.

Il n'est pas possible de planifier le lancement de la tâche *Gérer les comptes de l'Agent d'authentification*. Il est également impossible de forcer l'arrêt d'une tâche.

[Procédure d'ajout d'un compte utilisateur de l'Agent d'authentification via la Console d'administration \(MMC\)](#) 

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Sélection du type de tâche

Sélectionnez **Kaspersky Endpoint Security for Windows (11.6.0)** → **Gérer les comptes de l'Agent d'authentification**.

Étape 2. Sélection de la commande d'Administration des comptes utilisateur de l'Agent d'authentification

Composez la liste des commandes d'administration des comptes utilisateur de l'Agent d'authentification. Les commandes d'administration permettent d'ajouter, de modifier et de supprimer des comptes utilisateur de l'Agent d'authentification (cf. instructions ci-dessous). Seuls les utilisateurs disposant d'un compte utilisateur de l'Agent d'authentification peuvent réaliser la procédure d'authentification, charger le système d'exploitation et accéder au disque chiffré.

Étape 3. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 4. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple, **Comptes d'administrateur**.

Étape 5. Fin de la création de la tâche

Quittez l'assistant. Si nécessaire, cochez la case **Exécuter la tâche une fois l'assistant terminé**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Après avoir terminé la tâche, au prochain démarrage de l'ordinateur, le nouvel utilisateur peut alors suivre la procédure d'authentification, charger le système d'exploitation et accéder au disque chiffré.

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur le bouton **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows (11.6.0)**.

2. Dans la liste déroulante **Type de tâche**, sélectionnez **Gérer les comptes de l'Agent d'authentification**.

3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, **Comptes utilisateur d'administrateur**.

4. Dans le groupe **Sélection des appareils auxquels une tâche va être attribuée**, choisissez la zone d'action de la tâche.

Étape 2. Administration des comptes utilisateur de l'Agent d'authentification

Composez la liste des commandes d'administration des comptes utilisateur de l'Agent d'authentification. Les commandes d'administration permettent d'ajouter, de modifier et de supprimer des comptes utilisateur de l'Agent d'authentification (cf. instructions ci-dessous). Seuls les utilisateurs disposant d'un compte utilisateur de l'Agent d'authentification peuvent réaliser la procédure d'authentification, charger le système d'exploitation et accéder au disque chiffré.

Étape 3. Fin de la création de la tâche

Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches.

Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Après avoir terminé la tâche, au prochain démarrage de l'ordinateur, le nouvel utilisateur peut alors suivre la procédure d'authentification, charger le système d'exploitation et accéder au disque chiffré.

Pour ajouter un compte utilisateur de l'Agent d'authentification, vous devez ajouter une commande spéciale à la tâche *Gérer les comptes de l'Agent d'authentification*. Les tâches de groupe sont pratiques, par exemple, pour ajouter un compte administrateur à tous les ordinateurs.

Kaspersky Endpoint Security vous permet de créer automatiquement des comptes utilisateur d'Agent d'authentification avant de chiffrer un disque. Vous pouvez activer la création automatique de comptes utilisateur de l'Agent d'authentification dans les [paramètres de stratégie de chiffrement du disque](#). Vous pouvez également [utiliser la technologie d'authentification unique \(SSO\)](#).

1. Ouvrez la tâche de groupe *Administration des comptes utilisateur de l'Agent d'authentification*.

2. Dans les propriétés de la tâche, sélectionnez l'option **Paramètres**.

3. Cliquez sur le bouton **Ajouter** → **Commande d'ajout de compte**.

4. Dans le champ **Compte Windows** de la fenêtre qui s'ouvre, saisissez le nom du compte utilisateur Microsoft Windows sur la base duquel le compte utilisateur de l'Agent d'authentification va être créé.

5. Si vous avez saisi le nom de compte Windows manuellement, cliquez sur le bouton **Autoriser** pour définir l'identificateur de sécurité du compte (SID).

Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

La définition de l'identificateur de sécurité de compte Windows est nécessaire pour confirmer la saisie correcte du nom de compte Windows. Si le compte Windows n'existe pas sur l'ordinateur ou dans le domaine de confiance, la tâche *Administration des comptes utilisateur de l'Agent d'authentification* échouera.

6. Cochez la case **Remplacer le compte existant** si vous souhaitez qu'un compte utilisateur portant ce nom déjà saisi pour cet Agent de l'authentification soit remplacé par le compte ajouté.

Cette étape est accessible si vous ajoutez une commande de création d'un compte utilisateur de l'Agent d'authentification dans les propriétés de la tâche de groupe d'administration des comptes utilisateur de l'Agent d'authentification. Cette étape n'est pas disponible si vous ajoutez une commande de création d'un compte utilisateur de l'Agent d'authentification dans les propriétés de la tâche locale **Chiffrement du disque, administration des comptes utilisateur**.

7. Dans le champ **Nom d'utilisateur**, saisissez le nom du compte utilisateur de l'Agent d'authentification à saisir lors de la procédure d'authentification pour accéder aux disques durs chiffrés.

8. Cochez la case **Autoriser l'ouverture de session par mot de passe**, si vous souhaitez que l'application demande le mot de passe du compte utilisateur de l'Agent d'authentification lors de l'authentification pour l'accès aux disques durs chiffrés. Définissez le mot de passe du compte utilisateur de l'Agent d'authentification. Si nécessaire, vous pouvez demander à l'utilisateur de définir un nouveau mot de passe après la première authentification.

9. Cochez la case **Autoriser l'ouverture de session par certificat** si vous souhaitez que l'application exige la connexion du jeton ou de la carte à puce à l'ordinateur lors de l'authentification pour accéder aux disques durs chiffrés. Sélectionnez un fichier de certificat pour l'authentification avec une carte à puce ou un jeton.

10. Le cas échéant, saisissez dans le champ **Description de la commande** des informations sur le compte utilisateur de l'Agent d'authentification indispensables pour utiliser la commande.

11. Exécutez une des actions suivantes :

- Choisissez l'option **Autoriser l'authentification** si vous souhaitez que l'application autorise l'accès à l'authentification dans l'Agent d'authentification pour l'utilisateur qui travaille sous le compte utilisateur repris dans la commande.
- Choisissez l'option **Interdire l'authentification** si vous souhaitez que l'application interdise l'accès à l'authentification dans l'Agent d'authentification pour l'utilisateur qui travaille sous le compte utilisateur

repris dans la commande.

12. Enregistrez vos modifications.

[Procédure d'ajout d'un compte utilisateur de l'Agent d'authentification via Web Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** de Kaspersky Endpoint Security.

La fenêtre des propriétés de la tâche s'ouvre.

3. Choisissez l'onglet **Paramètres de l'application**.

4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter**.

L'Assistant d'administration des comptes utilisateurs de l'Agent d'authentification démarre.

5. Sélectionnez le type de la commande **Ajout d'un compte utilisateur**.

6. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement. Cliquez sur le bouton **Suivant**.

Kaspersky Endpoint Security définit un identificateur de sécurité du compte (SID). Ceci est nécessaire pour vérifier le compte utilisateur. En cas de saisie incorrecte du nom d'utilisateur, Kaspersky Endpoint Security arrête l'exécution de la tâche sur une erreur.

7. Configurez les paramètres du compte utilisateur de l'Agent d'authentification :

- **Créer un nouveau compte utilisateur de l'Agent d'authentification à la place du compte existant.** Kaspersky Endpoint Security analyse les comptes utilisateur existants sur l'ordinateur. Si l'identifiant de sécurité de l'utilisateur sur l'ordinateur et dans la tâche coïncide, Kaspersky Endpoint Security modifie les paramètres du compte utilisateur conformément à la tâche.
- **Nom d'utilisateur.** Le nom d'utilisateur du compte utilisateur de l'Agent d'authentification correspond par défaut au nom de domaine de l'utilisateur.
- **Autoriser l'ouverture de session par mot de passe.** Définissez le mot de passe du compte utilisateur de l'Agent d'authentification. Si nécessaire, vous pouvez demander à l'utilisateur de définir un nouveau mot de passe après la première authentification. Chaque utilisateur possède ainsi son propre mot de passe unique. Vous pouvez également définir des exigences quand à la sécurité du mot de passe pour le compte utilisateur de l'Agent d'authentification dans la stratégie.
- **Autoriser l'ouverture de session par certificat.** Sélectionnez un fichier de certificat pour l'authentification avec une carte à puce ou un jeton. L'utilisateur doit alors saisir le mot de passe de la carte à puce ou du jeton.
- **Accès du compte utilisateur aux données chiffrées.** Configurez l'accès d'utilisateur au disque chiffré. Vous pouvez, par exemple, désactiver temporairement l'authentification de l'utilisateur et ne pas supprimer le compte utilisateur de l'Agent d'authentification.
- **Commentaires.** Saisissez une description de compte utilisateur si nécessaire.

8. Enregistrez vos modifications.

9. Cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Après avoir terminé la tâche, au prochain démarrage de l'ordinateur, le nouvel utilisateur peut alors suivre la procédure d'authentification, charger le système d'exploitation et accéder au disque chiffré.

Pour modifier le mot de passe et d'autres paramètres du compte de l'Agent d'authentification, vous devez ajouter une commande spéciale à la tâche *Administration des comptes utilisateur de l'Agent d'authentification*. Les tâches de groupe sont pratiques, par exemple, pour remplacer le certificat d'un jeton d'administrateur sur tous les ordinateurs.

[Procédure de modification d'un compte utilisateur d'Agent d'authentification via la Console d'administration \(MMC\)](#) 

1. Ouvrez la tâche de groupe *Administration des comptes utilisateur de l'Agent d'authentification*.

2. Dans les propriétés de la tâche, sélectionnez l'option **Paramètres**.

3. Cliquez sur le bouton **Ajouter** → **Commande de modification de compte**.

4. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Compte Windows** le nom du compte d'utilisateur Microsoft Windows que vous souhaitez modifier.

5. Si vous avez saisi le nom de compte Windows manuellement, cliquez sur le bouton **Autoriser** pour définir l'identificateur de sécurité du compte (SID).

Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

La définition de l'identificateur de sécurité de compte Windows est nécessaire pour confirmer la saisie correcte du nom de compte Windows. Si le compte Windows n'existe pas sur l'ordinateur ou dans le domaine de confiance, la tâche *Administration des comptes utilisateur de l'Agent d'authentification* échouera.

6. Cochez la case **Modifier le nom d'utilisateur** et saisissez le nouveau nom pour le compte utilisateur de l'Agent d'authentification si vous souhaitez que l'application Kaspersky Endpoint Security remplace le nom de l'utilisateur par celui repris dans le champ ci-dessous pour tous les comptes utilisateur de l'Agent d'authentification créés sur la base du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

7. Cochez la case **Modifier les paramètres de l'ouverture de session par mot de passe** si vous souhaitez pouvoir modifier les paramètres d'entrée par mot de passe.

8. Cochez la case **Autoriser l'ouverture de session par mot de passe**, si vous souhaitez que l'application demande le mot de passe du compte utilisateur de l'Agent d'authentification lors de l'authentification pour l'accès aux disques durs chiffrés. Définissez le mot de passe du compte utilisateur de l'Agent d'authentification.

9. Cochez la case **Modifier la règle de changement du mot de passe lors de l'authentification dans l'Agent d'authentification** et saisissez le nouveau mot de passe pour le compte utilisateur de l'Agent d'authentification si vous souhaitez que l'application Kaspersky Endpoint Security remplace le mot de passe par celui repris dans le champ ci-dessous pour tous les comptes de l'Agent d'authentification créés à partir du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

10. Définissez la valeur du paramètre de modification du mot de passe lors de l'authentification dans l'Agent d'authentification.

11. Cochez la case **Modifier les paramètres de l'ouverture de session par certificat** si vous souhaitez pouvoir modifier les paramètres d'entrée par certificat électronique du token ou carte à puce.

12. Cochez la case **Autoriser l'ouverture de session par certificat**, si vous souhaitez que l'application demande de saisir le mot de passe du token ou de la carte à puce connecté à l'ordinateur lors de l'authentification pour l'accès aux disques durs chiffrés. Sélectionnez un fichier de certificat pour l'authentification avec une carte à puce ou un jeton.

13. Cochez la case **Modifier la description de la commande** et modifiez la description si vous souhaitez que l'application Kaspersky Endpoint Security modifie la description de la commande pour tous les comptes utilisateur de l'Agent d'authentification créés sur la base du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

14. Cochez la case **Modifier la règle d'accès à l'authentification dans l'Agent d'authentification** si vous souhaitez que l'application Kaspersky Endpoint Security remplace la règle d'accès de l'utilisateur à l'authentification dans l'Agent d'authentification par la valeur ci-dessous pour tous les comptes utilisateur de l'Agent d'authentification créés à partir du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.
15. Définissez la règle d'accès à l'authentification dans l'Agent d'authentification.
16. Enregistrez vos modifications.

[Procédure de modification d'un compte utilisateur d'Agent d'authentification via Web Console](#) 

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.
La liste des tâches s'ouvre.
2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** de Kaspersky Endpoint Security.
La fenêtre des propriétés de la tâche s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter**.
L'Assistant d'administration des comptes utilisateurs de l'Agent d'authentification démarre.
5. Sélectionnez le type de commande **Changement de compte utilisateur**.
6. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement. Cliquez sur le bouton **Suivant**.
Kaspersky Endpoint Security définit un identificateur de sécurité du compte (SID). Ceci est nécessaire pour vérifier le compte utilisateur. En cas de saisie incorrecte du nom d'utilisateur, Kaspersky Endpoint Security arrête l'exécution de la tâche sur une erreur.
7. Cochez les cases en regard des paramètres que vous souhaitez modifier.
8. Configurez les paramètres du compte utilisateur de l'Agent d'authentification :
 - **Créer un nouveau compte utilisateur de l'Agent d'authentification à la place du compte existant.** Kaspersky Endpoint Security analyse les comptes utilisateur existants sur l'ordinateur. Si l'identifiant de sécurité de l'utilisateur sur l'ordinateur et dans la tâche coïncide, Kaspersky Endpoint Security modifie les paramètres du compte utilisateur conformément à la tâche.
 - **Nom d'utilisateur.** Le nom d'utilisateur du compte utilisateur de l'Agent d'authentification correspond par défaut au nom de domaine de l'utilisateur.
 - **Autoriser l'ouverture de session par mot de passe.** Définissez le mot de passe du compte utilisateur de l'Agent d'authentification. Si nécessaire, vous pouvez demander à l'utilisateur de définir un nouveau mot de passe après la première authentification. Chaque utilisateur possède ainsi son propre mot de passe unique. Vous pouvez également définir des exigences quand à la sécurité du mot de passe pour le compte utilisateur de l'Agent d'authentification dans la stratégie.
 - **Autoriser l'ouverture de session par certificat.** Sélectionnez un fichier de certificat pour l'authentification avec une carte à puce ou un jeton. L'utilisateur doit alors saisir le mot de passe de la carte à puce ou du jeton.
 - **Accès du compte utilisateur aux données chiffrées.** Configurez l'accès d'utilisateur au disque chiffré. Vous pouvez, par exemple, désactiver temporairement l'authentification de l'utilisateur et ne pas supprimer le compte utilisateur de l'Agent d'authentification.
 - **Commentaires.** Saisissez une description de compte utilisateur si nécessaire.
9. Enregistrez vos modifications.
10. Cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Pour supprimer un compte utilisateur d'Agent d'authentification, vous devez ajouter une commande spéciale à la tâche *Administration des comptes utilisateur de l'Agent d'authentification*. Les tâches de groupe sont pratiques, par exemple, pour supprimer le compte utilisateur d'un employé licencié.

Procédure de suppression d'un compte utilisateur d'Agent d'authentification via la Console d'administration (MMC)

1. Ouvrez la tâche de groupe *Administration des comptes utilisateur de l'Agent d'authentification*.
2. Dans les propriétés de la tâche, sélectionnez l'option **Paramètres**.
3. Cliquez sur le bouton **Ajouter** → **Commande de suppression de compte**.
4. Dans la fenêtre qui s'ouvre, saisissez dans le champ **Compte Windows** le compte utilisateur Windows à partir duquel le compte utilisateur de l'Agent d'authentification que vous souhaitez supprimer a été créé.
5. Si vous avez saisi le nom de compte Windows manuellement, cliquez sur le bouton **Autoriser** pour définir l'identificateur de sécurité du compte (SID).

Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

La définition de l'identificateur de sécurité de compte Windows est nécessaire pour confirmer la saisie correcte du nom de compte Windows. Si le compte Windows n'existe pas sur l'ordinateur ou dans le domaine de confiance, la tâche *Administration des comptes utilisateur de l'Agent d'authentification* échouera.

6. Enregistrez vos modifications.

Procédure de suppression d'un compte utilisateur d'Agent d'authentification via Web Console

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Tâches**.

La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** de Kaspersky Endpoint Security.

La fenêtre des propriétés de la tâche s'ouvre.

3. Choisissez l'onglet **Paramètres de l'application**.

4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter**.

L'Assistant d'administration des comptes utilisateurs de l'Agent d'authentification démarre.

5. Sélectionnez le type de commande **Suppression d'un compte utilisateur**.

6. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement.

7. Enregistrez vos modifications.

8. Cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Suite à l'exécution de la tâche, l'utilisateur, lors du prochain démarrage de l'ordinateur, ne pourra pas réaliser la procédure d'authentification et charger le système d'exploitation. Kaspersky Endpoint Security interdira l'accès aux données chiffrées.

Pour afficher la liste des utilisateurs qui peuvent s'authentifier à l'aide de l'agent et charger le système d'exploitation, vous devez accéder aux propriétés de l'ordinateur administré.

[Procédure de consultation de la liste des comptes utilisateur d'Agent d'authentification via la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

4. Ouvrez les propriétés de l'ordinateur d'un double clic.

5. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Tâches**.

La liste des tâches locales s'ouvre.

6. Sélectionnez la tâche **Gérer les comptes de l'Agent d'authentification**.

7. Dans les propriétés de la tâche, sélectionnez l'option **Paramètres**.

Vous avez alors accès à la liste des comptes utilisateur d'Agent d'authentification sur cet ordinateur. Seuls les utilisateurs de la liste peuvent s'authentifier à l'aide de l'Agent et charger le système d'exploitation.

[Procédure de consultation de la liste des comptes utilisateur d'Agent d'authentification via Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez afficher la liste des comptes utilisateur d'Agent d'authentification.
Les propriétés de l'ordinateur s'ouvrent.
3. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Tâches**.
La liste des tâches locales s'ouvre.
4. Sélectionnez la tâche **Gérer les comptes de l'Agent d'authentification**.
5. Dans les propriétés de la tâche, sélectionnez l'onglet **Paramètres de l'application**.

Vous avez alors accès à la liste des comptes utilisateur d'Agent d'authentification sur cet ordinateur. Seuls les utilisateurs de la liste peuvent s'authentifier à l'aide de l'Agent et charger le système d'exploitation.

Utilisation du token et de la carte à puce lors de l'utilisation de l'Agent d'authentification

L'authentification en vue de l'accès aux disques durs cryptés peut être réalisée à l'aide d'un token ou d'une carte à puce. Il faut pour cela ajouter le fichier du certificat électronique du token ou de la carte à puce dans la tâche *Gérer les comptes de l'Agent d'authentification*.

L'utilisation du token ou de la carte à puce est disponible uniquement si les disques durs de l'ordinateur sont chiffrés à l'aide d'un algorithme AES256. Si les disques durs de l'ordinateur ont été chiffrés à l'aide d'un algorithme de chiffrement AES56, le fichier de certificat électronique ne pourra pas être ajouté à la commande.

Kaspersky Endpoint Security fonctionne avec les tokens liseurs de cartes à puces et avec les cartes à puce suivants :

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K (Java)
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511

- Rutoken ECP
- Rutoken ECP Flash
- Aladdin-RD JaCarta PKI
- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI

Pour ajouter le fichier de certificat électronique du token ou de la carte à puce à la commande de création d'un compte utilisateur de l'Agent d'authentification, il faut d'abord l'enregistrer à l'aide d'une application tierce prévue pour l'administration des certificats.

Le certificat du token ou de la carte à puce doit posséder les propriétés suivantes :

- Le certificat doit être conforme à la norme X.509, tandis que le fichier de certificat doit avoir le codage DER.
- Le certificat contient une clé RSA d'une longueur minimale de 1 024 bits.

Si le certificat électronique du token ou de la carte à puce ne remplit pas cette condition, il n'est pas possible de charger le fichier du certificat dans la commande de création d'un compte utilisateur d'Agent d'authentification.

De même, le paramètre `KeyUsage` doit avoir la valeur `keyEncipherment` ou `dataEncipherment`. Le paramètre `KeyUsage` détermine l'objectif du certificat. Si le paramètre a une valeur différente, Kaspersky Security Center télécharge le fichier de certificat, mais affiche un avertissement.

Si l'utilisateur perd le token ou la carte à puce, l'administrateur doit ajouter le fichier du certificat électronique du token ou de la carte à puce de remplacement à la commande de création d'un compte utilisateur d'Agent d'authentification. Ensuite, l'utilisateur doit suivre la procédure d'[obtention de l'accès aux appareils chiffrés ou de restauration des données sur les appareils chiffrés](#).

Déchiffrement des disques durs

Vous pouvez déchiffrer les disques durs même en l'absence d'une licence valide qui autorise le chiffrement des données.

Pour déchiffrer des disques durs, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.

6. Dans la liste déroulante **Technologie de chiffrement** choisissez la technologie à l'aide de laquelle les disques durs ont été chiffrés.

7. Exécutez une des actions suivantes :

- Dans la liste déroulante **Mode de chiffrement**, cochez la case **Déchiffrer tous les disques durs** si vous souhaitez déchiffrer tous les disques durs chiffrés.
- Ajoutez au tableau **Ne pas chiffrer les disques durs suivants** les disques durs chiffrés que vous souhaitez déchiffrer.

Cette option est accessible seulement pour la technologie de chiffrement Kaspersky Disk Encryption.

8. Enregistrez vos modifications.

Vous pouvez utiliser l'outil Surveillance du chiffrement pour contrôler le processus de chiffrement ou de déchiffrement du disque sur l'ordinateur d'un utilisateur. Vous pouvez exécuter l'outil Surveillance du chiffrement à partir de la [fenêtre principale de l'application](#).

Si, pendant le déchiffrement des disques durs chiffrés à l'aide de la technologie Kaspersky Disk Encryption, l'utilisateur éteint ou redémarre l'ordinateur, l'Agent d'authentification est chargé avant le prochain démarrage du système d'exploitation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le déchiffrement des disques durs.

Si, pendant le déchiffrement des disques durs chiffrés à l'aide de la technologie Kaspersky Disk Encryption, le système d'exploitation passe en mode d'hibernation (hibernation mode), lorsque le système d'exploitation sortira du mode veille, l'Agent d'authentification sera chargé. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le déchiffrement des disques durs. Après le déchiffrement des disques durs, le mode veille prolongée n'est pas accessible avant le premier redémarrage du système d'exploitation.

Si pendant le déchiffrement des disques durs, le système d'exploitation passe en mode veille, lorsque le système d'exploitation sortira du mode veille, Kaspersky Endpoint Security reprendra le déchiffrement des disques durs sans charger l'Agent d'authentification.

Restauration de l'accès à un disque protégé par la technologie Kaspersky Disk Encryption

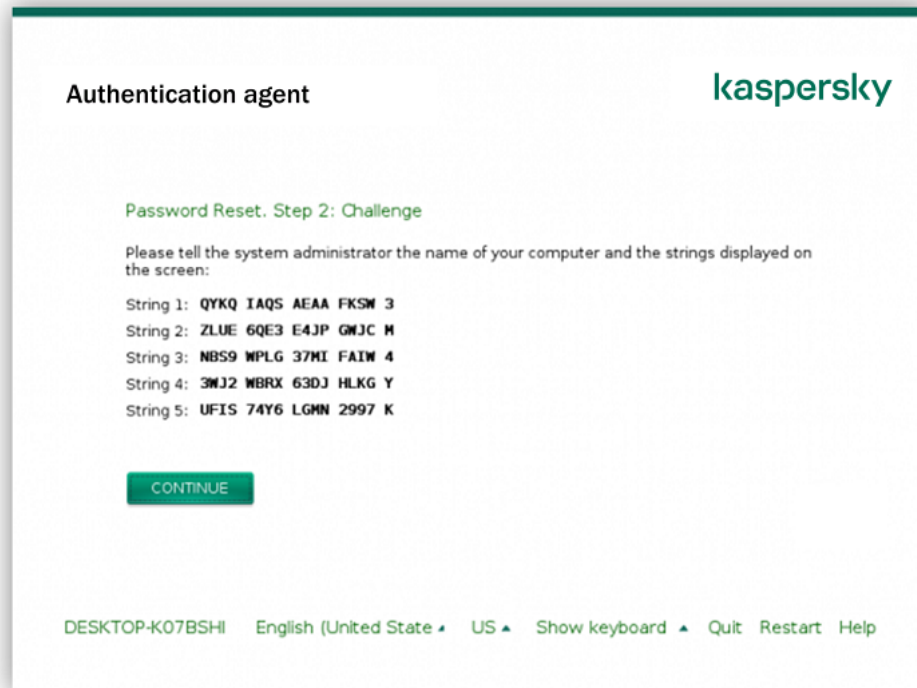
Si l'utilisateur a oublié le mot de passe d'accès au disque dur chiffré par la technologie Kaspersky Disk Encryption, il faut lancer la procédure de récupération (Requête-Réponse).

Restauration de l'accès au disque dur système

La restauration de l'accès à un disque dur système protégé par la technologie Kaspersky Disk Encryption comprend les étapes suivantes :

1. L'utilisateur communique à l'administrateur les groupes de demande (cf. ill. ci-dessous).
2. L'administrateur saisit les groupes de demande dans Kaspersky Security Center, reçoit les groupes de réponse et communique les groupes de réponse à l'utilisateur.

3. L'utilisateur saisit les groupes de réponse dans l'interface de l'Agent d'authentification et accède au disque dur.



Restauration de l'accès à un disque dur système protégé par la technologie Kaspersky Disk Encryption

Pour lancer la procédure de récupération, l'utilisateur doit cliquer sur le bouton **Forgot your password** (mot de passe oublié) dans l'interface de l'Agent d'authentification.

[Procédure d'obtention des groupes de réponse pour un disque dur système protégé par la technologie Kaspersky Disk Encryption dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a sollicité la restauration de l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Agent d'authentification**.
7. Dans la section **Algorithme de chiffrement utilisé**, sélectionnez l'algorithme de chiffrement : **AES56** ou **AES256**.

L'algorithme de chiffrement des données dépend de la bibliothèque de chiffrement AES incluse dans la distribution : *Strong encryption (AES256)* ou *Lite encryption (AES56)*. La bibliothèque de chiffrement AES est installée en même temps que l'application.
8. Dans la liste déroulante **Compte utilisateur**, sélectionnez le nom du compte d'Agent d'authentification de l'utilisateur qui a demandé la restauration de l'accès au disque.
9. Dans la liste déroulante **Disque dur**, choisissez le disque dur chiffré auquel il faut rétablir l'accès.
10. Dans le groupe **Codes de l'utilisateur**, saisissez les groupes de demande dictés par l'utilisateur.

Le contenu des groupes de réponse à la demande de l'utilisateur de restaurer le nom et le mot de passe du compte utilisateur de l'Agent d'authentification s'affiche alors dans le champ **Clé d'accès**. Transmettez le contenu des groupes de réponse à l'utilisateur.

[Procédure d'obtention des groupes de réponse pour un disque dur système protégé par la technologie Kaspersky Disk Encryption dans Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.
3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la section **Agent d'authentification**.
5. Sélectionnez le nom du compte utilisateur de l'Agent d'authentification, créé pour l'utilisateur à l'origine de la demande de récupération du nom et du mot de passe du compte utilisateur de l'Agent d'authentification, dans la liste déroulante **Compte utilisateur**.
6. Saisissez les groupes de demande dictés par l'utilisateur.

Le contenu des groupes de réponse à la demande de l'utilisateur portant sur la restauration du nom et du mot de passe du compte utilisateur de l'Agent d'authentification s'affiche dans le bas de la fenêtre. Transmettez le contenu des groupes de réponse à l'utilisateur.

Une fois la procédure de récupération terminée, l'Agent d'authentification invite à l'utilisateur à modifier le mot de passe.

Restauration de l'accès à un disque dur autre que le disque système

La restauration de l'accès à un disque dur autre que le disque système protégé par la technologie Kaspersky Disk Encryption comprend les étapes suivantes :

1. L'utilisateur envoie une requête d'accès au fichier à l'administrateur.
2. L'administrateur ajoute la requête d'accès au fichier à Kaspersky Security Center, crée le fichier de clé d'accès et l'envoie à l'utilisateur.
3. L'utilisateur ajoute le fichier de clé d'accès à Kaspersky Endpoint Security et accède au disque dur.

Pour lancer la procédure de récupération, l'utilisateur doit contacter le disque dur. Kaspersky Endpoint Security crée alors une requête d'accès au fichier (fichier avec l'extension kesdc), que l'utilisateur doit transmettre à l'administrateur, par exemple par email.

[Procédure d'obtention d'un fichier de clé d'accès à un disque dur chiffré autre que le disque système dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a sollicité la restauration de l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Chiffrement des données**.
7. Sous l'onglet **Chiffrement des données**, cliquez sur **Parcourir**.
8. Dans la fenêtre de sélection de la requête d'accès au fichier, indiquez le chemin d'accès au fichier reçu de l'utilisateur.

Les informations relatives à la requête de l'utilisateur s'affichent. Kaspersky Security Center crée le fichier clé d'accès. Envoyez à l'utilisateur un message électronique contenant le fichier clé d'accès aux données chiffrées. Ou enregistrez le fichier d'accès et transférez-le d'une manière quelconque.

[Procédure d'obtention d'un fichier de clé d'accès à un disque dur chiffré autre que le disque système dans Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
 2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.
 3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.
 4. Sélectionnez la section **Chiffrement des données**.
 5. Cliquez sur le bouton **Sélectionner un fichier** et sélectionnez la requête d'accès au fichier envoyée par l'utilisateur (fichier portant l'extension kesdc).
Web Console affiche les informations relatives à la requête. Notamment, le nom de l'ordinateur sur lequel l'utilisateur sollicite l'accès au fichier.
 6. Cliquez sur le bouton **Enregistrer la clé** et sélectionnez un dossier pour enregistrer le fichier clé d'accès aux données chiffrées (fichier portant l'extension kesdr).
- Vous aurez alors accès à une clé d'accès aux données chiffrées à remettre à l'utilisateur.

Mise à jour du système d'exploitation

La mise à jour du système d'exploitation d'un ordinateur protégé via le Chiffrement du disque (FDE) présente un certain nombre de particularités. Mettez à jour le système d'exploitation de manière progressive : commencez par mettre à jour le système d'exploitation sur un ordinateur, puis sur un nombre restreint d'ordinateurs, puis sur tous les ordinateurs du réseau.

Si vous utilisez la technologie de chiffrement du disque de Kaspersky, un agent d'authentification est chargé avant le lancement du système d'exploitation. L'Agent d'authentification permet à l'utilisateur de se connecter au système et d'accéder au disque chiffré. Le chargement du système d'exploitation débute ensuite.

Si vous lancez la mise à jour du système d'exploitation sur un ordinateur protégé par la technologie de chiffrement du disque de Kaspersky, l'Assistant de mise à jour du système d'exploitation supprime l'Agent d'authentification. Cela peut bloquer l'ordinateur car le module de démarrage du système d'exploitation ne pourra pas accéder au disque chiffré.

Pour en savoir plus sur la mise à jour sécurisée du système d'exploitation, veuillez consulter la [base des connaissances du Support Technique](#) ².

La mise à jour automatique du système d'exploitation est disponible dans les conditions suivantes :

1. Mise à jour du système d'exploitation via WSUS (Windows Server Update Services).
2. L'ordinateur tourne sous le système d'exploitation Windows 10 version 1607 (RS1) et versions ultérieures.
3. Kaspersky Endpoint Security version 11.2.0 et suivant est installé sur l'ordinateur.

Si toutes les conditions sont remplies, vous pouvez mettre à jour le système d'exploitation de la manière habituelle.

Si vous utilisez la technologie Kaspersky Disk Encryption (FDE) et que la version 11.1.0 ou 11.1.1 de Kaspersky Endpoint Security for Windows est installée sur l'ordinateur, vous n'avez pas besoin de chiffrer les disques durs pour mettre à jour Windows 10.

Pour mettre à jour le système d'exploitation, vous devez procéder comme suit :

1. Avant de mettre à jour le système, copiez les pilotes intitulés cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf et klfdefsf.sys dans un dossier local. Par exemple, dans C:\fde_drivers.
2. Lancez l'installation de la mise à jour du système à l'aide du commutateur `/ReflectDrivers` et indiquez le dossier contenant les pilotes enregistrés :
`setup.exe /ReflectDrivers C:\fde_drivers`

Si vous utilisez la technologie Chiffrement du disque BitLocker, vous n'avez pas besoin de déchiffrer les disques durs pour la mise à jour de Windows 10. Pour en savoir plus sur le fonctionnement BitLocker, consultez le [site de Microsoft](#).

Élimination des erreurs lors de la mise à jour de la fonctionnalité de chiffrement

Lors de la mise à jour depuis une version antérieure de l'application jusqu'à Kaspersky Endpoint Security for Windows 11.6.0, la fonctionnalité Chiffrement du disque est mise à niveau.

Les erreurs suivantes peuvent survenir lors du lancement de la mise à jour de la fonctionnalité de chiffrement du disque :

- Échec de l'initialisation de la mise à jour.
- L'appareil est incompatible avec l'Agent d'authentification.

Pour éliminer les erreurs qui surviennent au lancement de la mise à jour de la fonctionnalité de chiffrement du disque, réalisez les opérations suivantes dans la nouvelle version :

1. [Déchiffrez les disques durs.](#)
2. [Chiffrez à nouveau les disques durs.](#)

Lors de la mise à jour de la fonctionnalité de chiffrement du disque, les erreurs suivantes peuvent survenir :

- Échec de la mise à jour.
- Échec de la restauration de la mise à jour de la fonctionnalité de chiffrement.

Pour éliminer les erreurs survenues lors de la mise à jour de la fonctionnalité de chiffrement du disque,

[rétablissez l'accès à l'appareil chiffré à l'aide de l'utilitaire de restauration.](#)

Sélection du niveau de traçage de l'Agent d'authentification

L'application consigne dans le fichier de traçage les informations de service sur le fonctionnement de l'Agent d'authentification, ainsi que les informations relatives aux actions réalisées par l'utilisateur dans l'Agent d'authentification.

Pour modifier le niveau de traçage de l'Agent d'authentification, procédez comme suit :

1. Directement après le démarrage de l'ordinateur doté de disques durs chiffrés, appuyez sur la touche **F3** afin d'ouvrir la fenêtre de configuration de l'Agent d'authentification.

2. Sélectionnez le niveau de traçage souhaité dans la fenêtre de configuration des paramètres de l'Agent d'authentification :

- **Disable debug logging (default).** Si vous choisissez cette option, l'application ne consigne pas dans le fichier de traçage les informations relatives aux événements survenus pendant le fonctionnement de l'Agent d'authentification.
- **Enable debug logging.** Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification.
- **Enable verbose logging.** Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations détaillées relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification.

Le niveau de détail des entrées dans ce cas est plus élevé qu'au niveau **Enable debug logging**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

- **Enable debug logging and select serial port.** Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification et les transmet également via le port COM.

Si l'ordinateur avec les disques durs chiffrés est connecté à un autre ordinateur via le port COM, les événements survenus pendant le fonctionnement de l'Agent d'authentification peuvent être étudiés l'aide de cet ordinateur.

- **Enable verbose debug logging and select serial port.** Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations détaillées relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification et les transmet également via le port COM.

Le niveau de détails des entrées dans ce cas est plus élevé qu'au niveau **Enable debug logging and select serial port**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

L'écriture dans le fichier de traçage de l'Agent d'authentification a lieu si l'ordinateur est doté de disques durs chiffrés ou si le chiffrement du disque est en cours.

Le fichier de traçage de l'Agent d'authentification n'est pas transmis à Kaspersky comme les autres fichiers de traçage de l'application. Le cas échéant, vous pouvez envoyer le fichier de traçage de l'Agent d'authentification à Kaspersky pour analyse.

Modification des textes d'aide de l'Agent d'authentification

Avant de modifier les textes d'aide de l'Agent d'authentification, prenez connaissance de la liste des caractères autorisés dans l'environnement préalable au chargement (cf. ci-dessous).

Pour modifier les textes d'aide de l'Agent d'authentification, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
6. Cliquez sur le bouton **Aide** dans le groupe **Modèles**.
La fenêtre **Textes d'aide de l'Agent d'authentification** s'ouvre.
7. Procédez comme suit :
 - Sélectionnez l'onglet **Authentification** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de saisie des identifiants.
 - Sélectionnez l'onglet **Changer le mot de passe** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de modification du mot de passe du compte utilisateur de l'Agent d'authentification.
 - Sélectionnez l'onglet **Restauration du mot de passe** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de restauration du mot de passe du compte utilisateur de l'agent d'authentification.
8. Modifiez les textes d'aide.
Si vous voulez restaurer le texte original, cliquez sur le bouton **Par défaut**.

Vous pouvez saisir un texte d'aide qui contient 16 lignes maximum. Chaque ligne peut compter au maximum 64 caractères.

9. Enregistrez vos modifications.

Restrictions de prise en charge des caractères dans les textes d'aide de l'Agent d'authentification

L'environnement préalable au chargement prend en charge les caractères Unicode suivants :

- alphabet latin général (0000 - 007F) ;
- suppléments Latin-1 (0080 - 00FF) ;
- latin étendu A (0100 - 017F) ;
- latin étendu B (0180 - 024F) ;
- lettres modificatives avec chasse (02B0 - 02FF) ;
- diacritiques (0300 - 036F) ;

- grec et copte (0370 - 03FF) ;
- cyrillique (0400 - 04FF) ;
- hébreu (0590 - 05FF) ;
- arabe (0600 - 06FF) ;
- latin étendu additionnel (1E00 - 1EFF) ;
- caractères de ponctuation (2000 - 206F) ;
- symboles monétaires (20A0 - 20CF) ;
- symboles de type lettre (2100 - 214F) ;
- formes géométriques (25A0 - 25FF) ;
- formes B de présentation arabes (FE70 - FEFF).

Les caractères qui ne figurent pas dans cette liste ne sont pas pris en charge dans l'environnement préalable au démarrage. Il est déconseillé d'utiliser de tels caractères dans les textes d'aide de l'agent d'authentification.

Suppression des objets et données restants au terme du fonctionnement test de l'Agent d'authentification

Si, pendant le processus de suppression de l'application, Kaspersky Endpoint Security détecte des objets et données restés sur le disque dur système après le fonctionnement test de l'Agent d'authentification, la suppression de l'application est interrompue et ne reprendra que lorsque ces objets et données auront été supprimés.

Après le fonctionnement test de l'Agent d'authentification, les objets et données peuvent rester sur le disque dur système uniquement dans les situations d'exception. Par exemple, si après la mise en œuvre de la stratégie de Kaspersky Security Center selon les paramètres de chiffrement, l'ordinateur n'a jamais été redémarré ou encore après le fonctionnement test de l'Agent d'authentification.

Vous pouvez supprimer les objets et les données demeurés sur le disque dur système après le fonctionnement test de l'Agent d'authentification d'une des manières suivantes :

- avec la stratégie du Kaspersky Security Center ;
- [à l'aide de l'utilitaire de restauration](#).

Pour supprimer les objets et données restants au terme du fonctionnement test de l'Agent d'authentification à l'aide des stratégies de Kaspersky Security Center, procédez comme suit :

1. Appliquez à l'ordinateur la stratégie de Kaspersky Security Center avec les paramètres établis pour [déchiffrer](#) tous les disques durs de l'ordinateur.
2. Lancez Kaspersky Endpoint Security.

Pour supprimer les données sur l'incompatibilité de l'application avec l'Agent d'authentification,

saisissez la commande `avp pbatestreset` dans la ligne de commande.

Administration BitLocker

BitLocker est une technologie de chiffrement intégrée au système d'exploitation Windows. Kaspersky Endpoint Security vous permet de contrôler et de gérer BitLocker à l'aide de Kaspersky Security Center. BitLocker chiffre le volume logique. BitLocker ne permet pas de chiffrer les disques amovibles. Pour en savoir plus sur le fonctionnement de BitLocker, consultez la [documentation de Microsoft](#).

BitLocker fournit un stockage sécurisé des clés d'accès à l'aide d'un module de plateforme sécurisée. *Module de plateforme sécurisée (en anglais, Trusted Platform Module (TPM))*: puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Un module de plateforme sécurisée est généralement installé sur la carte mère de l'ordinateur et interagit avec tous les autres modules du système par le bus matériel. L'utilisation du module de plateforme sécurisée est le moyen le plus sûr de stocker des clés d'accès BitLocker, car ce module permet de vérifier l'intégrité du système avant le démarrage. Sur les ordinateurs sans TPM, vous pouvez également chiffrer des disques. Dans ce cas, la clé d'accès sera chiffrée à l'aide d'un mot de passe. Ainsi, BitLocker utilise les méthodes d'authentification suivantes :

- TPM.
- TPM et code PIN.
- Mot de passe.

Après avoir chiffré le disque, BitLocker crée une clé principale. Kaspersky Endpoint Security envoie la clé principale à Kaspersky Security Center afin que vous puissiez [restaurer l'accès au disque](#) si l'utilisateur a oublié le mot de passe, par exemple.

Si un utilisateur a chiffré un disque à l'aide de BitLocker, Kaspersky Endpoint Security envoie les [informations sur le chiffrement du disque à Kaspersky Security Center](#). Dans ce cas, Kaspersky Endpoint Security n'envoie pas la clé principale à Kaspersky Security Center et il est impossible de restaurer l'accès au disque à l'aide de Kaspersky Security Center. Pour que BitLocker fonctionne correctement avec Kaspersky Security Center, [déchiffrez le disque](#) et [chiffrez-le à nouveau](#) à l'aide d'une stratégie. Vous pouvez déchiffrer un disque localement ou à l'aide d'une stratégie.

Après avoir chiffré le disque dur du système, l'utilisateur doit passer par l'authentification BitLocker pour lancer le système d'exploitation. Une fois l'authentification réussie, BitLocker pourra se connecter. BitLocker n'est pas compatible avec la technologie d'authentification unique (SSO).

Si vous utilisez des stratégies de groupe pour Windows, désactivez l'administration de BitLocker dans les paramètres de la stratégie. Les paramètres de la stratégie Windows peuvent entrer en conflit avec les paramètres de la stratégie de Kaspersky Endpoint Security. Lors du chiffrement d'un disque, des erreurs peuvent se produire.

Lancement du chiffrement de disque BitLocker

Avant de lancer le chiffrement du disque, il est recommandé de s'assurer que l'ordinateur n'est pas infecté. Pour ce faire, lancez une analyse complète ou une analyse des zones critiques de l'ordinateur. Le chiffrement du disque sur un ordinateur infecté par un rootkit peut provoquer le dysfonctionnement de l'ordinateur.

Le fonctionnement de BitLocker sur des ordinateurs tournant sous un système d'exploitation Windows pour serveurs peut requérir l'installation du module BitLocker Drive Encryption. Installez le module à l'aide des outils du système d'exploitation (Assistant d'ajout de rôles et de fonctionnalités). Pour en savoir plus sur l'installation de Chiffrement de disque BitLocker, consultez la [documentation Microsoft](#).

Lancement du chiffrement de disque BitLocker via la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
6. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Chiffrement de disque BitLocker**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Chiffrer tous les disques durs**.

Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel le chiffrement a été réalisé peut être lancé après le chiffrement.

8. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).
9. Enregistrez vos modifications.

Lancement du chiffrement de disque BitLocker via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez lancer le chiffrement de disque BitLocker.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres des applications**.
4. Accédez à **Chiffrement des données** → **Chiffrement du disque**.
5. Dans la liste déroulante **Administration du chiffrement**, choisissez l'option **Chiffrement de disque BitLocker**.
6. Suivez le lien **Chiffrement de disque BitLocker**.
Une fenêtre contenant les options de chiffrement de lecteur BitLocker s'ouvre.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Chiffrer tous les disques durs**.

Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel le chiffrement a été réalisé peut être lancé après le chiffrement.

8. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).
9. Cliquez sur le bouton **OK**.

Vous pouvez utiliser l'outil Surveillance du chiffrement pour contrôler le processus de chiffrement ou de déchiffrement du disque sur l'ordinateur d'un utilisateur. Vous pouvez exécuter l'outil Surveillance du chiffrement à partir de la [fenêtre principale de l'application](#).

Une fois la stratégie est appliquée, l'application affichera les requêtes suivantes, en fonction des paramètres d'authentification :

- TPM uniquement. Aucune entrée d'utilisateur n'est requise. Le disque sera chiffré au redémarrage de l'ordinateur.
- TPM + PIN / Mot de passe. En présence d'un module TPM, une fenêtre de saisie d'un code PIN s'ouvre. En l'absence d'un module TPM, une fenêtre de saisie de mot de passe pour l'identification avant le chargement s'ouvre.
- Mot de passe uniquement. Vous verrez une fenêtre d'invite de saisie de mot de passe pour l'authentification avant le démarrage.

Si la compatibilité avec la norme FIPS (norme fédérale de traitement de l'information) est activée dans le système d'exploitation, une fenêtre de demande de connexion d'un appareil de stockage de masse pour l'enregistrement du fichier de clé de récupération s'ouvre dans les systèmes d'exploitation Windows 8 et dans les versions antérieures. Vous pouvez enregistrer plusieurs fichiers de clés de récupération sur un seul appareil de stockage.

Après avoir défini un mot de passe ou un code PIN, BitLocker vous demandera de redémarrer l'ordinateur pour terminer le chiffrement du disque. Ensuite, l'utilisateur doit passer par la procédure d'authentification BitLocker. Une fois la procédure d'authentification de BitLocker terminée, il faudra vous connecter. BitLocker terminera le chiffrement du disque une fois le système d'exploitation chargé.

En l'absence d'accès aux clés du chiffrement, l'utilisateur peut demander la [clé de récupération](#) à l'administrateur du réseau local de l'organisation (si la clé de la récupération n'avait pas été enregistrée sur l'appareil de stockage de masse ou si elle avait été perdue).

Paramètres du module Chiffrement de disque BitLocker

| Paramètre | Description |
|---|---|
| <p>Autoriser l'utilisation de l'authentification BitLocker qui requiert une saisie au clavier avant le démarrage sur les tablettes</p> | <p>La case active ou désactive l'utilisation de l'authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage, même si la plateforme ne dispose pas de cette possibilité (par exemple, claviers tactiles sur les tablettes).</p> <div data-bbox="464 656 1493 813" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Le clavier tactile des tablettes n'est pas accessible dans cet environnement. Pour réaliser une authentification BitLocker sur de telles tablettes, l'utilisateur doit absolument connecter un clavier USB par exemple.</p> </div> <p>Si la case est cochée, l'utilisation de l'authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage est autorisée. Il est recommandé d'utiliser ce paramètre uniquement pour les appareils qui, pendant le chargement préalable, disposent de modes alternatifs de saisie de données, par exemple un clavier USB en plus du clavier tactile.</p> <p>Si cette case est décochée, le chiffrement de disque BitLocker n'est pas possible sur les tablettes.</p> |
| <p>Utiliser le chiffrement au niveau matériel (Windows 8 et versions ultérieures)</p> | <p>Si la case est cochée, l'application adopte le chiffrement au niveau du matériel. Cela permet d'augmenter la vitesse du chiffrement et de réduire l'utilisation des ressources de l'ordinateur.</p> |
| <p>Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures)</p> | <p>La case active/désactive la fonction qui limite le secteur de chiffrement aux secteurs occupés du disque dur. Cette restriction permet de réduire la durée du chiffrement.</p> <div data-bbox="464 1485 1493 1682" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>L'activation ou la désactivation de la fonctionnalité Chiffrer uniquement l'espace occupé (réduit la durée du chiffrement) après le lancement du chiffrement ne modifie pas ce paramètre tant que les disques durs ne sont pas déchiffrés. Il faut cocher ou décocher la case avant le début du chiffrement.</p> </div> <p>Si la case est cochée, seule la partie du disque dur qui contient des fichiers est chiffrée. Kaspersky Endpoint Security chiffre les nouvelles données automatiquement au fur et à mesure qu'elles sont ajoutées.</p> <p>Si la case est décochée, tout le disque dur est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant.</p> |

Cette fonction est recommandée pour les nouveaux disques durs dont les données n'ont pas été modifiées ou supprimées. Si vous appliquez le chiffrement sur un disque dur déjà utilisé, il est conseillé de chiffrer tout le disque dur. Cela garantit la protection de toutes les données, même celles qui ont été supprimées mais qui pourraient être restaurées.

La case est décochée par défaut.

Paramètres d'authentification

Utiliser le mot de passe (Windows 8 et versions ultérieures)

Si vous avez choisi cette option, Kaspersky Endpoint Security demande le mot de passe à l'utilisateur lorsque celui-ci souhaite accéder au disque chiffré.

Cette option peut être choisie si la Trusted Platform Module (TPM) n'est pas utilisée.

Utiliser Trusted Platform Module (TPM)

Si vous avez choisi cette option, BitLocker utilise le Trusted Platform Module (TPM).

Module de plateforme sécurisée (en anglais, Trusted Platform Module (TPM)): puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Le Trusted Platform Module s'installe en général sur la carte mère de l'ordinateur et interagit avec les autres modules système via le bus matériel.

Pour les ordinateurs tournant sous les systèmes d'exploitation Windows 7 et Windows Server 2008 R2, seul le chiffrement à l'aide du module TPM est disponible. Si le module TPM n'est pas installé, le chiffrement BitLocker n'est pas possible. L'utilisation d'un mot de passe sur ces ordinateurs n'est pas prise en charge.

L'appareil équipé du Trusted Platform Module peut créer des clés de chiffrement qui peuvent être déchiffrées uniquement à l'aide de celui-ci. Le Trusted Platform Module chiffre les clés de chiffrement à l'aide de la clé racine de stockage correspondante. La clé racine de stockage se trouve à l'intérieur du Trusted Platform Module. Cela offre un niveau de sécurité complémentaire pour les clés de chiffrement contre les tentatives d'attaque.

Cette action est sélectionnée par défaut.

Vous pouvez définir une couche de protection supplémentaire pour l'accès à la clé de chiffrement, et chiffrer la clé à l'aide d'un mot de passe ou d'un code PIN :

- **Utiliser le code PIN pour le TPM.** Quand la case est cochée, l'utilisateur doit saisir un code PIN pour accéder à la clé de chiffrement conservée dans le module de plateforme sécurisée (TPM).
Si cette case n'est pas cochée, l'utilisateur n'est pas autorisé à utiliser le code PIN. Pour accéder à la clé de chiffrement, l'utilisateur utilise un mot de passe. Vous pouvez autoriser l'utilisateur à utiliser un code PIN amélioré. Le *code PIN renforcé* permet l'utilisation d'autres caractères en plus des caractères numériques : lettres latines majuscules et minuscules, caractères spéciaux et espaces.
- **Utiliser Trusted Platform Module (TPM) ; s'il n'est pas disponible, utiliser le mot de passe.** Si la case est cochée, l'utilisateur peut accéder aux clés de chiffrement à l'aide d'un mot de passe en l'absence du Trusted Platform Module (TPM).

Si la case n'est pas cochée et que le TPM n'est pas disponible, le chiffrement complet du disque ne démarre pas.

Déchiffrement d'un disque dur protégé par BitLocker

L'utilisateur peut déchiffrer indépendamment le disque à l'aide des outils du système d'exploitation (la fonction *Désactiver BitLocker*). Par la suite, Kaspersky Endpoint Security proposera de chiffrer à nouveau le disque. Kaspersky Endpoint Security proposera de chiffrer le disque jusqu'à ce que vous activiez le déchiffrement du disque dans la stratégie.

Déchiffrement d'un disque dur protégé par BitLocker via la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
6. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Chiffrement de disque BitLocker**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Déchiffrer tous les disques durs**.
8. Enregistrez vos modifications.

Procédure de déchiffrement d'un disque dur chiffré au moyen de BitLocker via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, choisissez l'onglet **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez déchiffrer les disques durs.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à **Chiffrement des données** → **Chiffrement du disque**.
5. Sélectionnez la technologie **Chiffrement de disque BitLocker** et suivez le lien pour configurer les paramètres.
Les paramètres de chiffrement s'affichent.
6. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Déchiffrer tous les disques durs**.
7. Cliquez sur le bouton **OK**.

Vous pouvez utiliser l'outil Surveillance du chiffrement pour contrôler le processus de chiffrement ou de déchiffrement du disque sur l'ordinateur d'un utilisateur. Vous pouvez exécuter l'outil Surveillance du chiffrement à partir de la [fenêtre principale de l'application](#).

Restauration de l'accès au disque protégé par BitLocker

Si l'utilisateur a oublié le mot de passe d'accès au disque dur chiffré par BitLocker, il faut lancer la procédure de récupération (Requête-Réponse).

Si le système d'exploitation prend en charge la norme FIPS (Federal Information Processing Standard), alors, dans les systèmes d'exploitation Windows 8 et antérieures, le fichier de clé de récupération aura été enregistré sur un disque amovible avant le chiffrement. Pour restaurer l'accès au disque, connectez le disque amovible et suivez les instructions à l'écran.

La restauration de l'accès au disque dur chiffré par BitLocker comprend les étapes suivantes :

1. L'utilisateur communique à l'administrateur l'identifiant de la clé de récupération (cf. figure ci-dessous).
2. L'administrateur vérifie l'identifiant de la clé de récupération dans les propriétés de l'ordinateur dans Kaspersky Security Center. L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant qui apparaît dans les propriétés de l'ordinateur.
3. Si les identifiants de la clé de récupération correspondent, l'administrateur fournit à l'utilisateur la clé de récupération ou transfère le fichier de la clé de récupération.

Le fichier de clé de récupération est utilisé pour les ordinateurs qui tournent sous les systèmes d'exploitation suivants :

- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2011
- Windows Server 2012

Pour les autres systèmes d'exploitation, la procédure recourt à la clé de récupération.

4. L'utilisateur saisit la clé de récupération et accède au disque dur.



Restauration de l'accès au disque dur chiffré à l'aide de BitLocker

Restauration de l'accès au disque système

Pour lancer la procédure de récupération, l'utilisateur doit appuyer sur la touche **Échap** lors de l'identification avant le chargement.

[Procédure de consultation de la clé de récupération pour un disque système chiffré à l'aide de BitLocker dans la console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a sollicité la restauration de l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Accès au disque système avec protection BitLocker**.
7. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération**.

Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

Vous avez alors accès à la clé de récupération ou au fichier de clé de récupération qu'il faudra transmettre à l'utilisateur.

[Procédure de consultation de la clé de récupération pour un disque système chiffré à l'aide de BitLocker dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.
3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la section **BitLocker**.
5. Vérifiez l'identifiant de la clé de récupération L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant repris dans les paramètres de l'ordinateur.

Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

6. Appuyez sur le bouton **Obtenir la clé**.

Vous avez alors accès à la clé de récupération ou au fichier de clé de récupération qu'il faudra transmettre à l'utilisateur.

Après le chargement du système d'exploitation, Kaspersky Endpoint Security invite l'utilisateur à modifier le mot de passe ou le code PIN. Une fois que vous avez défini un nouveau mot de passe ou code PIN, BitLocker crée une nouvelle clé principale et envoie la clé à Kaspersky Security Center. Par conséquent, la clé de récupération et le fichier de la clé de récupération seront mis à jour. Si l'utilisateur n'a pas modifié le mot de passe, vous pourrez utiliser l'ancienne clé de récupération lors du prochain démarrage du système d'exploitation.

Les ordinateurs Windows 7 ne permettent pas de modifier le mot de passe ni le code PIN. Une fois que la clé de récupération est saisie et que le système d'exploitation est chargé, Kaspersky Endpoint Security n'invite pas l'utilisateur à modifier le mot de passe ou le code PIN. Il est donc impossible de définir un nouveau mot de passe ou un nouveau code PIN. Ce problème provient des particularités du système d'exploitation. Pour continuer, vous devez de nouveau chiffrer le disque dur.

Restauration de l'accès à disque autre que le disque système

Pour lancer la procédure de récupération, l'utilisateur doit cliquer sur le lien **Mot de passe oublié** dans la fenêtre d'accès au disque. Une fois que l'utilisateur a obtenu l'accès au lecteur chiffré, il peut activer le déverrouillage automatique du disque lors de l'authentification Windows dans les paramètres de BitLocker.

[Procédure de consultation de la clé de récupération pour un disque autre que le disque système chiffré à l'aide de BitLocker dans la console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Chiffrement et protection des données** → **Appareils chiffrés**.
3. Dans l'espace de travail, choisissez l'appareil chiffré pour lequel vous voulez créer un fichier clé l'accès, puis, dans le menu contextuel de l'appareil, choisissez l'option **Obtenir l'accès à l'appareil dans Kaspersky Endpoint Security for Windows (11.6.0)**.
4. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération**.

Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

5. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

[Procédure de consultation de la clé de récupération pour un disque non-système chiffré à l'aide de BitLocker dans Web Console et Cloud Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Chiffrement et protection des données** → **Appareils chiffrés**.

2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.

3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.

L'assistant d'octroi de l'accès à l'appareil s'ouvre.

4. Suivez les instructions de l'assistant d'octroi de l'accès à l'appareil.

a. Sélectionnez le plug-in **Kaspersky Endpoint Security for Windows**.

b. Vérifiez l'identifiant de la clé de récupération L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant repris dans les paramètres de l'ordinateur.

Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

c. Appuyez sur le bouton **Obtenir la clé**.

Vous avez alors accès à la clé de récupération ou au fichier de clé de récupération qu'il faudra transmettre à l'utilisateur.

Chiffrement des fichiers sur les disques locaux de l'ordinateur

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le chiffrement des fichiers présente les caractéristiques suivantes :

- Kaspersky Endpoint Security (dé)chiffre les dossiers standards uniquement pour les profils utilisateur locaux du système d'exploitation. Kaspersky Endpoint Security ne (dé)chiffre pas les dossiers standard pour les profils utilisateur itinérant (roaming user profiles), les profils utilisateur obligatoire (mandatory user profiles), les profils utilisateur temporaires (temporary user profiles) et les redirections de dossiers.
- Kaspersky Endpoint Security ne chiffre pas les fichiers dont la modification peut nuire au fonctionnement du système d'exploitation et des programmes installés. Par exemple, la liste des exclusions du chiffrement inclut les fichiers et les dossiers suivants avec tous les dossiers qui y sont joints :
 - %WINDIR% ;
 - %PROGRAMFILES% et %PROGRAMFILES(X86)% ;
 - les fichiers du registre Windows.

La liste des exclusions du chiffrement ne peut pas être consultée et modifiée. Les fichiers et les dossiers de la liste des exclusions du chiffrement peuvent être ajoutés à la liste pour le chiffrement, mais ils ne seront pas chiffrés lors de l'exécution du chiffrement des fichiers.

Lancement du chiffrement des fichiers sur les disques locaux de l'ordinateur

Kaspersky Endpoint Security ne chiffre pas les fichiers dont le contenu se trouve dans le stockage Cloud OneDrive et bloque la copie des fichiers chiffrés dans le stockage Cloud OneDrive si ces fichiers n'ont pas été ajoutés à la [règle de déchiffrement](#).

Pour chiffrer des fichiers sur les disques locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
6. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Chiffrement**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Selon les règles**.
8. Sur l'onglet **Chiffrement**, appuyez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :
 - a. Choisissez l'option **Dossiers standards** pour ajouter à la règle de chiffrement des fichiers issus de dossiers de profils d'utilisateurs locaux proposés par les experts de Kaspersky.
 - **Documents**. Fichiers dans le dossier standard *Documents* du système d'exploitation, ainsi que dans ses sous-dossiers.
 - **Favoris**. Fichiers dans le dossier standard *Favoris* du système d'exploitation, ainsi que dans ses sous-dossiers.
 - **Bureau**. Fichiers dans le dossier standard *Bureau* du système d'exploitation, ainsi que dans ses sous-dossiers.
 - **Fichiers temporaires**. Fichiers temporaires associés au fonctionnement des applications installées sur l'ordinateur. Par exemple, les applications Microsoft Office créent des fichiers temporaires avec les copies de sauvegarde des documents.
 - **Fichiers Outlook**. Fichiers associés au fonctionnement du client de messagerie Outlook : fichiers de données (.pst), fichiers de données hors ligne (.ost), fichiers du carnet d'adresses en mode hors connexion (.ab) et fichiers du carnet d'adresses personnel (.pab).
 - b. Choisissez l'option **Dossier manuel** pour ajouter le chemin d'accès saisi manuellement à la règle du chiffrement du dossier.

Lors de l'ajout d'un chemin de dossier, les règles suivantes doivent être suivies :

- Utilisez une variable d'environnement (par exemple, %FOLDER%\UserFolder\). Vous ne pouvez utiliser la variable d'environnement qu'une seule fois et seulement au début du chemin.
- N'utilisez pas de chemins relatifs. Vous pouvez utiliser l'ensemble \..\ (par exemple, C:\Users\..\UserFolder\). L'ensemble \..\ indique la transition vers le dossier parent.
- N'utilisez pas * et ?.
- N'utilisez pas de chemins UNC.
- Utilisez ; ou , en guise de séparateur.

c. Choisissez l'option **Fichiers selon l'extension** pour ajouter des extensions de fichier distinctes à la règle de chiffrement. Kaspersky Endpoint Security chiffre les fichiers portant les extensions indiquées sur tous les disques locaux de l'ordinateur.

d. Choisissez l'option **Fichiers par groupes d'extensions** pour ajouter des groupes extensions de fichier à la règle de chiffrement (par exemple, le groupe *Documents Microsoft Office*). Kaspersky Endpoint Security chiffre les fichiers portant les extensions indiquées dans les groupes d'extensions sur tous les disques locaux de l'ordinateur.

9. Enregistrez vos modifications.

Directement après l'application de la stratégie, Kaspersky Endpoint Security chiffre les fichiers repris dans la règle de chiffrement et non repris [dans la règle de déchiffrement](#).

Le chiffrement des fichiers présente les caractéristiques suivantes :

- Si le même fichier est ajouté à la fois à la règle de chiffrement et à la règle de déchiffrement, Kaspersky Endpoint Security effectue les actions suivantes :
 - Si le fichier source n'est pas chiffré, Kaspersky Endpoint Security ne chiffre pas ce fichier.
 - Si le fichier source est chiffré, Kaspersky Endpoint Security le déchiffre.
- Kaspersky Endpoint Security continue de chiffrer les nouveaux fichiers s'ils répondent aux critères de la règle de chiffrement. Par exemple, vous avez modifié les propriétés d'un fichier non chiffré (chemin ou extension) et, par conséquent, le fichier répond aux critères de la règle de chiffrement. Kaspersky Endpoint Security chiffre ce fichier.
- Lorsque l'utilisateur crée un fichier dont les propriétés correspondent aux critères des règles de chiffrement, Kaspersky Endpoint Security le chiffre dès son ouverture.
- Kaspersky Endpoint Security attend que les fichiers soient fermés avant de les chiffrer.
- Si vous déplacez le fichier chiffré dans un autre dossier sur le disque local, le fichier reste chiffré que ce dossier soit couvert ou non par la règle de chiffrement.
- Si vous avez déchiffré un fichier, puis que vous l'avez copié dans un autre dossier sur le disque local qui n'est pas inclus dans la règle de déchiffrement, une copie du fichier peut être chiffrée. Pour exclure le chiffrement d'une copie d'un fichier, créez une règle de déchiffrement pour le dossier cible.

Composition des règles d'accès des applications aux fichiers chiffrés

Pour composer des règles d'accès des applications aux fichiers chiffrés, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
6. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Selon les règles**.

Les règles de l'accès fonctionnent uniquement selon le mode **Selon les règles**. Si après l'application des règles de l'accès en mode **Selon les règles** vous passez au mode **Laisser tel quel**, Kaspersky Endpoint Security ignorera toutes les règles d'accès. Toutes les applications auront l'accès à tous les fichiers chiffrés.

7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.
8. Si vous voulez choisir les applications exclusivement dans la liste Kaspersky Security Center, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications de la liste Kaspersky Security Center**.
 - a. Définissez les filtres pour afficher la liste des applications dans le tableau. Définissez pour cela les paramètres **Application**, **Éditeur**, **Période d'ajout**, ainsi que les cases du groupe **Groupe**.
 - b. Cliquez sur le bouton **Actualiser**.
 - c. Le tableau reprend les applications qui répondent aux filtres définis.
 - d. Dans la colonne **Applications**, cochez les cases en regard des applications pour lesquelles vous souhaitez créer des règles d'accès aux fichiers chiffrés.
 - e. Dans la liste déroulante **Règle pour les applications**, choisissez la règle qui définira l'accès des applications aux fichiers chiffrés.
 - f. Dans la liste déroulante **Action pour les applications sélectionnées auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les règles d'accès aux fichiers chiffrés définies pour les applications indiquées plus haut.
 - g. Cliquez sur le bouton **OK**.

Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

9. Si vous voulez choisir les applications manuellement, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications à la main**.

a. Dans le champ de saisie, saisissez le nom ou la liste de noms des fichiers exécutables des applications avec leur extension.

Vous pouvez également ajouter les noms des fichiers exécutables des applications de la liste de Kaspersky Security Center en cliquant sur le bouton **Ajouter depuis la liste de Kaspersky Security Center**.

b. Si vous le souhaitez, saisissez une description de la liste des applications dans le champ **Description**.

c. Dans la liste déroulante **Règle pour les applications**, choisissez la règle qui définira l'accès des applications aux fichiers chiffrés.

d. Cliquez sur le bouton **OK**.

Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

10. Enregistrez vos modifications.

Chiffrement des fichiers créés et modifiés par des applications distinctes

Vous pouvez créer une règle selon laquelle Kaspersky Endpoint Security chiffrera tous les fichiers créés et modifiés par les applications indiquées dans la règle.

Les fichiers créés ou modifiés par les applications indiquées avant l'application de la règle de chiffrement ne seront pas chiffrés.

Pour configurer le chiffrement des fichiers créés et modifiés par les applications distinctes, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
6. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Selon les règles**.

Les règles de chiffrement agissent seulement en mode **Selon les règles**. Si après l'application des règles de chiffrement en mode **Selon les règles** vous passez au mode **Laisser tel quel**, Kaspersky Endpoint Security ignorera toutes les règles du chiffrement. Les fichiers qui avaient été chiffrés auparavant resteront toujours chiffrés.

7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.
8. Si vous voulez choisir les applications exclusivement dans la liste Kaspersky Security Center, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications de la liste Kaspersky Security Center**.

La fenêtre **Ajout d'application depuis la liste Kaspersky Security Center** s'ouvre.

Procédez comme suit :

- a. Définissez les filtres pour afficher la liste des applications dans le tableau. Définissez pour cela les paramètres **Application**, **Éditeur**, **Période d'ajout**, ainsi que les cases du groupe **Groupe**.
- b. Cliquez sur le bouton **Actualiser**.
Le tableau reprend les applications qui répondent aux filtres définis.
- c. Dans la colonne **Applications**, cochez les cases en regard des applications du tableau dont vous souhaitez chiffrer les fichiers.
- d. Dans la liste déroulante **Règle pour les applications** choisissez l'option **Chiffrer tous les fichiers créés**.
- e. Dans la liste déroulante **Action pour les applications sélectionnées auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les règles de chiffrement des fichiers chiffrés définies pour les applications indiquées plus haut.
- f. Cliquez sur le bouton **OK**.

Les informations sur la règle de chiffrement des fichiers créés et modifiés par les applications choisies s'afficheront dans le tableau de l'onglet **Règles pour les applications**.

9. Si vous voulez choisir les applications manuellement, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications à la main**.

La fenêtre **Ajout/modification des noms des fichiers exécutables des applications** s'ouvre.

Procédez comme suit :

- a. Dans le champ de saisie, saisissez le nom ou la liste de noms des fichiers exécutables des applications avec leur extension.
Vous pouvez également ajouter les noms des fichiers exécutables des applications de la liste de Kaspersky Security Center en cliquant sur le bouton **Ajouter depuis la liste de Kaspersky Security Center**.
- b. Si vous le souhaitez, saisissez une description de la liste des applications dans le champ **Description**.
- c. Dans la liste déroulante **Règle pour les applications** choisissez l'option **Chiffrer tous les fichiers créés**.
- d. Cliquez sur le bouton **OK**.

Les informations sur la règle de chiffrement des fichiers créés et modifiés par les applications choisies s'afficheront dans le tableau de l'onglet **Règles pour les applications**.

10. Enregistrez vos modifications.

Composition de la règle de déchiffrement

Pour composer la règle de déchiffrement, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
6. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Déchiffrement**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Selon les règles**.
8. Sur l'onglet **Déchiffrement**, appuyez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :
 - a. Choisissez l'option **Dossiers standards** pour ajouter à la règle de déchiffrement des fichiers issus des dossiers des profils d'utilisateurs locaux proposés par les experts de Kaspersky.
 - b. Choisissez l'élément **Dossier manuel** pour ajouter à la règle de déchiffrement le dossier dont le chemin d'accès a été saisi manuellement.
 - c. Choisissez l'option **Fichiers selon l'extension** pour ajouter des extensions de fichier distinctes à la règle de déchiffrement. Kaspersky Endpoint Security ne chiffre pas les fichiers portant les extensions indiquées sur tous les disques locaux de l'ordinateur.
 - d. Choisissez l'option **Fichiers par groupes d'extensions** pour ajouter des groupes extensions de fichier à la règle de déchiffrement (par exemple, le groupe *Documents Microsoft Office*). Kaspersky Endpoint Security ne chiffre pas les fichiers portant les extensions indiquées dans les groupes d'extension sur tous les disques locaux de l'ordinateur.
9. Enregistrez vos modifications.

Si le même fichier est ajouté à la fois dans la règle de chiffrement et dans la règle de déchiffrement, Kaspersky Endpoint Security ne chiffre pas ce fichier si celui-ci n'est pas déchiffré et le déchiffre s'il est chiffré.

Déchiffrement des fichiers sur les disques locaux de l'ordinateur

Pour déchiffrer des fichiers sur les disques locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
6. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Chiffrement**.
7. Excluez de la liste de chiffrement les fichiers et les dossiers que vous ne souhaitez pas déchiffrer. Pour ce faire, sélectionnez les fichiers dans la liste et dans le menu contextuel du bouton **Supprimer**, choisissez l'option

Supprimer la règle et déchiffrer les fichiers.

Vous pouvez supprimer simultanément plusieurs éléments de la liste pour le chiffrement. Pour ce faire, maintenez la touche **CTRL** enfoncée et d'un clic gauche, sélectionnez les éléments, puis dans le menu contextuel du bouton **Supprimer**, choisissez l'option **Supprimer la règle et déchiffrer les fichiers**.

Les fichiers et dossiers supprimés de la liste de chiffrement sont ajoutés automatiquement à la liste de déchiffrement.

8. [Composez la liste des fichiers à déchiffrer.](#)

9. Enregistrez vos modifications.

Dès que la stratégie a été appliquée, Kaspersky Endpoint Security déchiffre les fichiers chiffrés ajoutés à la liste de déchiffrement.

Kaspersky Endpoint Security déchiffre les fichiers chiffrés si leurs paramètres (chemin d'accès au fichier, nom du fichier, extension du fichier) changent et répondent dès lors aux paramètres des objets ajoutés à la liste de déchiffrement.

Kaspersky Endpoint Security attend que les fichiers soient fermés avant de les déchiffrer.

Création d'archives chiffrées

Pour protéger les données lors du transfert de fichiers vers des utilisateurs en dehors du réseau de l'entreprise, vous pouvez utiliser des archives chiffrées. Les archives chiffrées sont un moyen simple pour transférer des fichiers volumineux à l'aide de lecteurs amovibles, vu que les clients de messagerie imposent des restrictions sur la taille des pièces jointes.

Avant de créer des archives chiffrées, Kaspersky Endpoint Security demande un mot de passe à l'utilisateur. Pour garantir une protection fiable des données, vous pouvez activer la vérification de la complexité du mot de passe et sélectionner des critères de complexité. Ainsi, vous pouvez interdire l'utilisation de mots de passe courts et simples, par exemple 1234.

[Comment activer la vérification de la complexité du mot de passe lors de la création d'archives chiffrées dans la console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
6. Dans le groupe **Paramètres de mot de passe**, cliquez sur le bouton **Paramètres**.
7. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Archives chiffrées**.
8. Configurez les paramètres de complexité du mot de passe lors de la création d'archives chiffrées.

Comment activer la vérification de la complexité du mot de passe lors de la création d'archives chiffrées dans Web Console


1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez activer la vérification de la complexité des mots de passe.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à **Chiffrement des données** → **Chiffrement des fichiers**.
5. Dans le groupe **Paramètres du mot de passe des archives chiffrées**, configurez les critères du niveau de sécurité du mot de passe exigés lors de la création de paquets chiffrés.

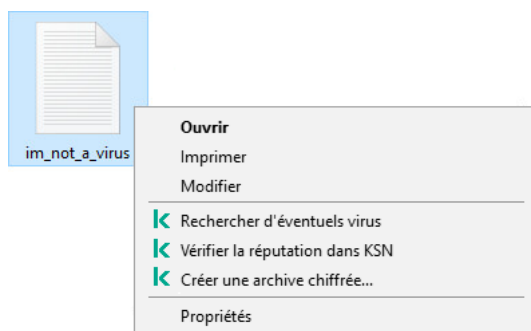
Vous pouvez créer des archives chiffrées sur des ordinateurs dotés de Kaspersky Endpoint Security avec la fonction de chiffrement de fichiers.

Lors de l'ajout à une archive chiffrée d'un fichier dont le contenu se trouve dans le stockage cloud OneDrive, Kaspersky Endpoint Security télécharge le contenu du fichier, puis le chiffre.

Pour créer une archive chiffrée, procédez comme suit :

1. Dans un gestionnaire de fichiers quelconques, sélectionnez les fichiers ou dossiers que vous souhaitez ajouter à l'archive chiffrée. Cliquez-droit pour ouvrir leur menu contextuel.
2. Sélectionnez l'option **Créer une archive chiffrée** dans le menu contextuel (cf. ill. ci-dessous).
3. Dans la fenêtre qui s'ouvre, sélectionnez un emplacement pour enregistrer l'archive chiffrée sur un disque amovible, spécifiez un nom et cliquez sur le bouton **Enregistrer**.
4. Dans la fenêtre qui s'ouvre, définissez le mot de passe et répétez-le.
Le mot de passe doit satisfaire aux critères de complexité définis dans la stratégie.
5. Cliquez sur le bouton **Générer**.

La création de l'archive chiffrée est lancée. Lors de la création d'archives chiffrées, Kaspersky Endpoint Security ne compresse pas les fichiers. À l'issue du processus, une archive chiffrée auto-extractible protégée par mot de passe est créée sur le disque amovible à l'emplacement indiqué (fichier exécutable portant l'extension exe) - .



Création d'une archive chiffrée

Pour accéder aux fichiers d'une archive chiffrée, vous devez lancer l'assistant de décompression de l'archive d'un double clic, puis saisir le mot de passe. Si vous oubliez le mot de passe, il sera impossible de rétablir l'accès aux fichiers dans l'archive chiffrée. Vous pouvez dans ce cas recréer l'archive chiffrée.

Restauration de l'accès aux fichiers chiffrés

Lors du chiffrement des fichiers, Kaspersky Endpoint Security reçoit la clé de chiffrement indispensable pour l'accès direct aux fichiers chiffrés. L'utilisateur, connecté sous n'importe quel compte utilisateur Windows actif au moment du chiffrement des fichiers, bénéficie, grâce à la clé de chiffrement, d'un accès direct aux fichiers chiffrés. L'utilisateur connecté sous un compte Windows inactif au moment du chiffrement des fichiers doit se connecter à Kaspersky Security Center pour pouvoir accéder aux fichiers chiffrés.

Les fichiers chiffrés peuvent être inaccessibles dans les cas suivants :

- Des clés de chiffrement existent sur l'ordinateur de l'utilisateur, mais il n'y a aucune connexion à Kaspersky Security Center pour pouvoir utiliser des clés. Dans ce cas, l'utilisateur doit solliciter l'accès aux fichiers chiffrés à l'administrateur du réseau local de l'organisation.

En l'absence de communication avec Kaspersky Security Center il faut :

- Demander une clé d'accès pour accéder aux fichiers chiffrés sur les disques durs de l'ordinateur ;
- Demander une clé d'accès aux fichiers chiffrés de chaque disque amovible pour accéder aux fichiers chiffrés sur les disques amovibles.
- Les modules de chiffrement ont été supprimés de l'ordinateur de l'utilisateur. Dans ce cas, l'utilisateur peut ouvrir les fichiers chiffrés sur les disques locaux et les disques amovibles, mais le contenu des fichiers s'affiche comme chiffré.

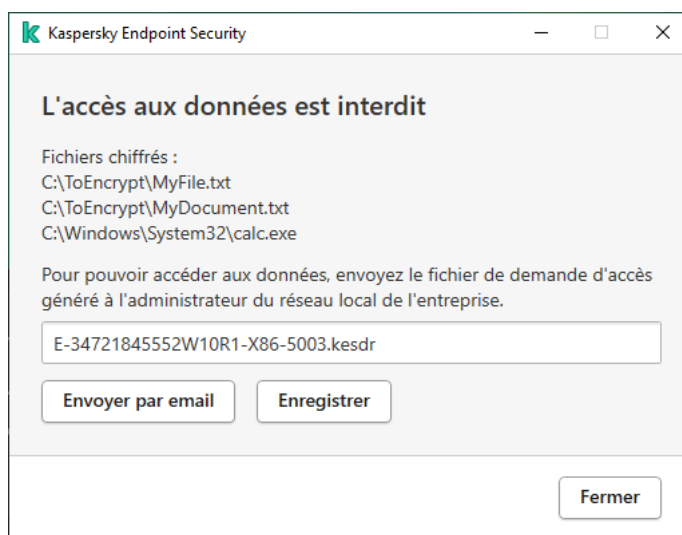
L'utilisateur peut travailler avec les fichiers chiffrés dans les conditions suivantes :

- Les fichiers se trouvent dans des [archives chiffrées](#) créées sur l'ordinateur à l'aide de l'application Kaspersky Endpoint Security installée.
- Les fichiers se trouvent sur des disques amovibles pour lesquels le fonctionnement en [mode portable](#) est autorisé.

Pour obtenir l'accès aux fichiers chiffrés, l'utilisateur doit lancer la procédure de restauration de l'accès (Requête-Réponse).

La restauration de l'accès aux fichiers chiffrés comprend les étapes suivantes :

1. L'utilisateur envoie une requête d'accès au fichier à l'administrateur (cf. ill. ci-dessous).
2. L'administrateur ajoute la requête d'accès au fichier à Kaspersky Security Center, crée le fichier de clé d'accès et l'envoie à l'utilisateur.
3. L'utilisateur ajoute le fichier de clé d'accès à Kaspersky Endpoint Security et accède aux fichiers.



Restauration de l'accès aux fichiers chiffrés

Pour lancer la procédure de restauration, l'utilisateur doit accéder au fichier. Kaspersky Endpoint Security crée alors une requête d'accès au fichier (fichier avec l'extension kesdc), que l'utilisateur doit transmettre à l'administrateur, par exemple par email.

Kaspersky Endpoint Security génère une requête d'accès au fichier pour tous les fichiers chiffrés stockés sur le disque de l'ordinateur (disque local ou disque amovible).

[Procédure du fichier de clé d'accès aux données chiffrées dans la Console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a sollicité la restauration de l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Chiffrement des données**.
7. Sous l'onglet **Chiffrement des données**, cliquez sur **Parcourir**.
8. Dans la fenêtre de sélection de la requête d'accès au fichier, indiquez le chemin d'accès au fichier reçu de l'utilisateur.

Les informations relatives à la requête de l'utilisateur s'affichent. Kaspersky Security Center crée le fichier clé d'accès. Envoyez à l'utilisateur un message électronique contenant le fichier clé d'accès aux données chiffrées. Ou enregistrez le fichier d'accès et transférez-le d'une manière quelconque.

[Procédure d'obtention du fichier de clé d'accès aux données chiffrées dans Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
 2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.
 3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.
 4. Sélectionnez la section **Chiffrement des données**.
 5. Cliquez sur le bouton **Sélectionner un fichier** et sélectionnez la requête d'accès au fichier envoyée par l'utilisateur (fichier portant l'extension kesdc).
Web Console affiche les informations relatives à la requête. Notamment, le nom de l'ordinateur sur lequel l'utilisateur sollicite l'accès au fichier.
 6. Cliquez sur le bouton **Enregistrer la clé** et sélectionnez un dossier pour enregistrer le fichier clé d'accès aux données chiffrées (fichier portant l'extension kesdr).
- Vous aurez alors accès à une clé d'accès aux données chiffrées à remettre à l'utilisateur.

Après avoir reçu le fichier de clé d'accès aux données chiffrées, l'utilisateur doit l'ouvrir d'un double clic. Kaspersky Endpoint Security octroie alors l'accès à tous les fichiers chiffrés stockés sur le disque. Pour pouvoir accéder aux fichiers chiffrés enregistrés sur d'autres disques, il faut obtenir les clés d'accès propres à ces disques.

Restauration de l'accès aux données chiffrées en cas de panne du système d'exploitation

La restauration de l'accès aux données en cas de panne du systèmes d'exploitation est disponible uniquement pour le chiffrement des fichiers (FLE). Il est impossible de restaurer l'accès aux données en cas de chiffrement du disque (FDE).

Pour restaurer l'accès aux données chiffrées en cas de panne du système d'exploitation, procédez comme suit :

1. Réinstallez le système d'exploitation sans formater le disque dur.
2. [Installez Kaspersky Endpoint Security](#).
3. Établissez la connexion entre l'ordinateur et le Serveur d'administration de Kaspersky Security Center qui gère l'ordinateur pendant le chiffrement des données.

L'accès aux données chiffrées sera octroyé sous les mêmes conditions que celles en vigueur avant la panne du système d'exploitation.

Modification des modèles de messages pour l'octroi de l'accès aux fichiers chiffrés

Pour modifier les modèles de messages pour l'octroi de l'accès aux fichiers chiffrés, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
6. Dans le groupe **Modèles**, cliquez sur le bouton **Modèles**.
La fenêtre **Modèles** s'ouvre.
7. Procédez comme suit :
 - Si vous souhaitez modifier le modèle du message de l'utilisateur, sélectionnez l'onglet **Message de l'utilisateur**. Lorsque l'utilisateur tente d'accéder au fichier chiffré alors que la clé d'accès à ceux-ci ne figure pas sur l'ordinateur, la fenêtre **L'accès aux données est interdit** s'ouvre. Quand vous cliquez sur le bouton **Envoyer par email** de la fenêtre **L'accès aux données est interdit**, le message de l'utilisateur se rédige automatiquement. Ce message est envoyé à l'administrateur du réseau local de l'entreprise avec un fichier de demande d'accès aux fichiers chiffrés.
 - Si vous souhaitez modifier le modèle du message pour l'administrateur, sélectionnez l'onglet **Message de l'administrateur**. Ce message est composé automatiquement lorsque vous cliquez sur le bouton **Envoyer par email** dans la fenêtre **Demande d'accès aux fichiers chiffrés**. L'utilisateur le reçoit une fois qu'il a obtenu l'accès aux fichiers chiffrés.
8. Modifiez le modèle de message.
Vous pouvez utiliser le bouton **Par défaut** et la liste déroulante **Variable**.
9. Enregistrez vos modifications.

Chiffrement des disques amovibles

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Kaspersky Endpoint Security prend en charge le chiffrement des fichiers dans les systèmes de fichiers FAT32 et NTFS. Si un disque amovible doté d'un système de fichiers non pris en charge est connecté à l'ordinateur, le chiffrement de ce disque amovible se solde sur une erreur et Kaspersky Endpoint Security lui attribue l'état d'accès "lecture seule".

Pour protéger les données sur des disques amovibles, vous pouvez utiliser les types de chiffrement suivants :

- Chiffrement de disque (FDE).
Chiffrement de l'intégralité du disque amovible, y compris du système de fichiers.

Il n'est pas possible d'accéder aux données chiffrées en dehors du réseau de l'entreprise. Il est également impossible d'accéder aux données chiffrées au sein du réseau de l'entreprise si l'ordinateur n'est pas connecté à Kaspersky Security Center (ordinateur invité).

- Chiffrement de fichiers (FLE).

Chiffrement uniquement des fichiers sur le disque amovible. Le système de fichiers reste inchangé.

Le chiffrement des fichiers sur des disques amovibles permet d'accéder aux données en dehors du réseau de l'entreprise à l'aide d'un mode spécial baptisé [mode portable](#).

Pendant le chiffrement, Kaspersky Endpoint Security crée une clé principale. Kaspersky Endpoint Security enregistre la clé principale dans les stockages suivants :

- Kaspersky Security Center.

- Ordinateur de l'utilisateur.

La clé principale est chiffrée à l'aide de la clé privée de l'utilisateur.

- Disque amovible.

La clé principale est chiffrée à l'aide de la clé publique de Kaspersky Security Center.

Une fois le chiffrement terminé, les données sur le disque amovible sont accessibles au sein du réseau d'entreprise comme si vous utilisiez un disque amovible classique sans chiffrement.

Obtention de l'accès aux données chiffrées

Lorsqu'un disque amovible contenant des données chiffrées est connecté, Kaspersky Endpoint Security exécute les actions suivantes :

1. Recherche la présence éventuelle d'une clé principale dans le stockage local sur l'ordinateur de l'utilisateur.

Si la clé principale existe, l'utilisateur peut accéder aux données sur le disque amovible.

Si la clé principale est introuvable, Kaspersky Endpoint Security exécute les actions suivantes :

- a. Il envoie une demande à Kaspersky Security Center.

Après avoir reçu la demande, Kaspersky Security Center envoie une réponse contenant la clé principale.

- b. Kaspersky Endpoint Security enregistre la clé principale dans le stockage local sur l'ordinateur de l'utilisateur pour pouvoir ensuite utiliser le disque amovible chiffré.

2. Il déchiffre les données.

Particularités du chiffrement des disques amovibles

Le chiffrement des disques amovibles présente les caractéristiques suivantes :

- Une stratégie avec les paramètres définis de chiffrement des disques amovibles est composée pour un groupe défini d'ordinateurs administrés. Par conséquent, le résultat de l'application de la stratégie de Kaspersky Security Center avec chiffrement/déchiffrement des disques amovibles dépend de l'ordinateur auquel le disque amovible a été connecté.

- Kaspersky Endpoint Security ne (dé)chiffre pas les fichiers avec l'état d'accès "lecture seule" qui sont enregistrés sur les disques amovibles.
- Les types d'appareils suivants sont pris en charge en guise de disques amovibles :
 - supports branchés via le port USB ;
 - disques durs branchés via le port USB ou FireWire ;
 - disques SSD branchés via le port USB ou FireWire.

Lancement du chiffrement des disques amovibles

Vous pouvez déchiffrer un disque amovible à l'aide d'une stratégie. Une stratégie avec les paramètres définis de chiffrement des disques amovibles est composée pour un groupe d'administration défini. Par conséquent, le résultat du déchiffrement des données sur les disques amovibles dépend de l'ordinateur auquel le disque amovible est connecté.

Kaspersky Endpoint Security prend en charge le chiffrement des systèmes de fichiers FAT32 et NTFS. Si le système de fichiers d'un disque amovible connecté à un ordinateur n'est pas pris en charge, le chiffrement du disque amovible échouera et Kaspersky Endpoint Security définira l'autorisation "lecture seule" pour ce disque amovible.

Pour chiffrer des disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
6. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'action exécutée par défaut par Kaspersky Endpoint Security sur tous les disques amovibles :
 - **Chiffrer tout le disque amovible** (FDE). Kaspersky Endpoint Security chiffre le contenu du disque amovible secteur par secteur. De cette façon, le chiffrement porte non seulement sur les fichiers stockés sur le disque local, mais aussi sur les systèmes fichiers, y compris les noms des fichiers et les structures des dossiers sur le disque amovible.
 - **Chiffrer tous les fichiers** (FLE). Kaspersky Endpoint Security chiffre tous les fichiers stockés sur les disques amovibles. L'application ne chiffre pas les systèmes fichiers des disques amovibles, y compris les noms des fichiers et les structures des dossiers.
 - **Chiffrer uniquement les nouveaux fichiers** (FLE). Kaspersky Endpoint Security chiffre uniquement les fichiers ajoutés aux disques amovibles ou stockés sur des disques amovibles et modifiés après la dernière application de la stratégie de Kaspersky Security Center.

Kaspersky Endpoint Security ne chiffre pas à nouveau un disque amovible déjà chiffré.

7. Si vous souhaitez [utiliser le mode portable](#) pour chiffrer les disques amovibles, cochez la case **Mode portable**.

Le *mode portable* est un mode de chiffrement des fichiers (FLE) sur les disques amovibles qui permet d'accéder aux données en dehors du réseau de l'entreprise. Le mode portable permet également de travailler avec des données chiffrées sur des ordinateurs qui ne sont pas dotés de Kaspersky Endpoint Security.

8. Si vous souhaitez chiffrer un nouveau disque amovible, il est conseillé de cocher la case **Chiffrer uniquement l'espace occupé**. Si cette case n'est pas cochée, Kaspersky Endpoint Security chiffrera tous les fichiers, y compris les restes de fichiers supprimés ou modifiés.

9. Si vous souhaitez configurer le chiffrement pour des disques amovibles individuels, [définissez les règles de chiffrement](#).

10. Si vous souhaitez utiliser le chiffrement complet des disques amovibles en mode hors connexion, cochez la case **Autoriser le chiffrement des disques amovibles en mode hors ligne**.

Le *mode de chiffrement hors ligne* désigne le chiffrement des disques amovibles en l'absence de communication avec Kaspersky Security Center. Lors du chiffrement, Kaspersky Endpoint Security enregistre la clé maîtresse uniquement sur l'ordinateur de l'utilisateur. Kaspersky Endpoint Security envoie la clé maîtresse à Kaspersky Security Center à la synchronisation suivante.

Si l'ordinateur sur lequel la clé maîtresse est enregistrée est endommagé et que les données n'ont pas été envoyées à Kaspersky Security Center, il est impossible d'accéder au disque amovible.

Si l'option **Autoriser le chiffrement des disques amovibles en mode hors ligne** est désactivée et qu'il n'y a pas de connexion à Kaspersky Security Center, le chiffrement du lecteur amovible n'est pas possible.

11. Enregistrez vos modifications.

Suite à l'application de la stratégie, si un utilisateur connecte un disque amovible ou si un disque amovible est déjà connecté, Kaspersky Endpoint Security demande une confirmation avant d'exécuter le chiffrement (cf. fig. ci-dessous).

L'application permet d'effectuer les opérations suivantes :

- Si l'utilisateur confirme la demande de chiffrement, Kaspersky Endpoint Security chiffre les données.
- Si l'utilisateur rejette la demande de chiffrement, Kaspersky Endpoint Security laisse les données inchangées et définit le droit d'accès "lecture seule" pour ce lecteur amovible.
- Si l'utilisateur ne répond pas à la demande de chiffrement, Kaspersky Endpoint Security laisse les données inchangées et définit le droit d'accès "lecture seule" pour ce disque amovible. L'application demande à nouveau la confirmation lors de l'application suivante de la stratégie ou lors de la connexion suivante de ce disque amovible.

Si l'utilisateur tente de retirer le disque amovible pendant le chiffrement des données, Kaspersky Endpoint Security interrompt le chiffrement et permet le retrait du disque amovible avant la fin du chiffrement. Le chiffrement des données se poursuivra à la prochaine connexion du disque amovible à cet ordinateur.

En cas d'échec du chiffrement du disque amovible, consultez le rapport **Chiffrement des données** dans l'interface de Kaspersky Endpoint Security. L'accès aux fichiers peut être bloqué par une autre application. Dans ce cas, essayez d'éjecter le disque amovible et de le connecter à nouveau à l'ordinateur.



Demande de chiffrement du disque amovible

Ajout d'une règle de chiffrement pour les disques amovibles

Pour ajouter une règle de chiffrement pour les disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
6. Cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :
 - Si vous voulez ajouter des règles de chiffrement pour les disques amovibles qui se trouvent dans la liste des appareils de confiance du module Contrôle des appareils, choisissez l'option **De la liste des appareils de confiance de cette stratégie**.
 - Si vous voulez ajouter des règles de chiffrement pour les disques amovibles qui se trouvent dans la liste de Kaspersky Security Center, choisissez l'option **Depuis la liste des appareils de Kaspersky Security Center**.
7. Dans la liste déroulante **Mode de chiffrement des appareils sélectionnés**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les fichiers stockés sur les disques amovibles sélectionnés.
8. Cochez la case **Mode portable** si vous souhaitez que Kaspersky Endpoint Security prépare les disques amovibles avant le chiffrement en vue de pouvoir manipuler les fichiers chiffrés qu'ils renferment en cas de connexion en mode portable.

Le mode portable permet d'utiliser les fichiers chiffrés des disques amovibles sur les ordinateurs lorsque la [fonction de chiffrement est inaccessible](#).

9. Cochez la case **Chiffrer uniquement l'espace occupé** si vous voulez que Kaspersky Endpoint Security chiffre uniquement les secteurs du disque qui sont occupés par des fichiers.

Si vous appliquez le chiffrement à un disque déjà utilisé, il est recommandé de chiffrer tout le disque. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites. L'utilisation de la fonction **Chiffrer uniquement l'espace occupé** est recommandée pour les nouveaux disques jamais utilisés jusqu'à présent.

Si l'appareil avait été chiffré à l'aide de la fonction **Chiffrer uniquement l'espace occupé**, après l'application de la stratégie en mode **Chiffrer tout le disque amovible**, les secteurs qui n'hébergent pas de fichiers ne seront toujours pas chiffrés.

10. Dans la liste déroulante **Action pour les appareils sélectionnés auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va effectuer sur les règles de chiffrement définies antérieurement pour les disques amovibles :

- Si vous voulez que la règle de chiffrement du disque amovible créée auparavant reste sans inchangée, choisissez l'option **Ignorer**.
- Si vous voulez que la règle de chiffrement du disque amovible créée auparavant soit remplacée par une nouvelle règle, choisissez l'option **Mise à jour**.

11. Enregistrez vos modifications.

Les règles ajoutées pour le chiffrement des disques amovibles seront appliquées aux lecteurs amovibles connectés à n'importe quel ordinateur de l'organisation.

Exportation et importation d'une liste de règles de chiffrement pour les disques amovibles

Vous pouvez exporter la liste des règles de chiffrement des disques amovibles dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre de règles pour le même type de disques amovibles. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles ou pour procéder à la migration des règles vers un autre serveur.

[Comment exporter et importer une liste de règles de chiffrement des disques amovibles dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
6. Pour exporter la liste des règles de chiffrement pour les disques amovibles, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter. Pour sélectionner plusieurs ports, utilisez les touches **CTRL** ou **MAJ**.
Si vous n'avez sélectionné aucune règle, Kaspersky Endpoint Security exportera toutes les règles.
 - b. Cliquez sur le lien **Exporter**.
 - c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des règles et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.
 - d. Cliquez sur le bouton **Enregistrer**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.
7. Pour importer une liste de règles de chiffrement pour les disques amovibles, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

[Comment exporter et importer une liste de règles de chiffrement des disques amovibles dans Web Console](#) 

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez exporter ou importer une liste de règles de chiffrement des disques amovibles.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Chiffrement des données** → **Chiffrement des disques amovibles**.
5. Dans le groupe **Règles de chiffrement des appareils sélectionnés**, cliquez sur le lien **Règles de chiffrement**.
Cette action permet d'ouvrir une liste de règles de chiffrement pour les disques amovibles.
6. Pour exporter la liste des règles de chiffrement pour les disques amovibles, procédez comme suit :
 - a. Sélectionnez les règles que vous souhaitez exporter.
 - b. Cliquez sur le bouton **Exporter**.
 - c. Confirmez que vous souhaitez exporter uniquement les règles sélectionnées ou exporter la liste complète.
 - d. Cliquez sur le bouton **Exporter**.
Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML dans le dossier des téléchargements par défaut.
7. Pour importer la liste des règles, procédez comme suit :
 - a. Cliquez sur le lien **Importer**.
Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.
 - b. Cliquez sur le bouton **Ouvrir**.
Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

Mode portable pour utiliser les fichiers chiffrés sur les disques amovibles

Le *mode portable* est un mode de chiffrement des fichiers (FLE) sur les disques amovibles qui permet d'accéder aux données en dehors du réseau de l'entreprise. Le mode portable permet également de travailler avec des données chiffrées sur des ordinateurs qui ne sont pas dotés de Kaspersky Endpoint Security.

L'utilisation du mode portable peut être pratique dans les cas suivants :

- Il n'y a pas de connexion entre l'ordinateur et le Serveur d'administration de Kaspersky Security Center.
- L'infrastructure a changé avec la modification du Serveur d'administration de Kaspersky Security Center.

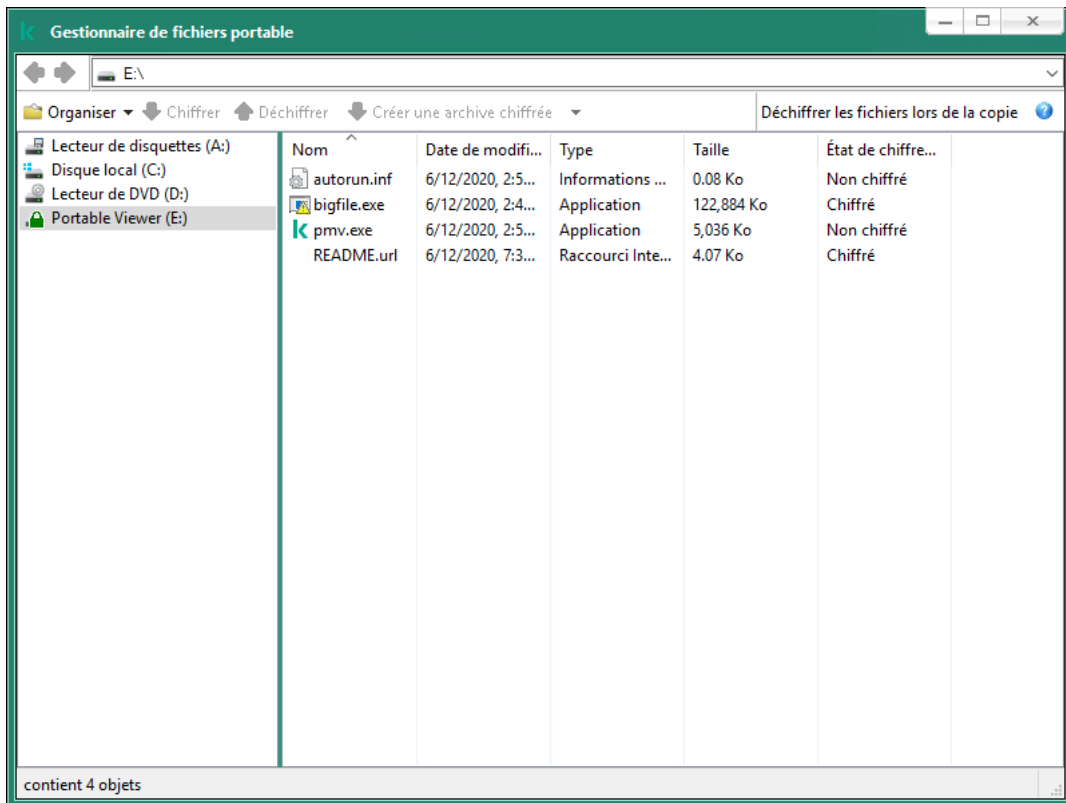
- Kaspersky Endpoint Security n'est pas installé sur l'ordinateur.

Gestionnaire de fichiers portable

Pour permettre le fonctionnement du mode portable, Kaspersky Endpoint Security installe un module de chiffrement spécial sur un disque amovible : le *gestionnaire de fichiers portable*. Le gestionnaire de fichiers portable fournit une interface pour utiliser les données chiffrées si Kaspersky Endpoint Security n'est pas installé sur l'ordinateur (cf. ill. ci-dessous). Si Kaspersky Endpoint Security est installé sur votre ordinateur, vous pouvez travailler avec des disques amovibles chiffrés à l'aide du gestionnaire de fichiers habituel (par exemple, Explorer).

Le gestionnaire de fichiers portable conserve la clé de chiffrement des fichiers sur le disque amovible. La clé est chiffrée à l'aide du mot de passe de l'utilisateur. L'utilisateur définit un mot de passe avant de chiffrer les fichiers sur le disque amovible.

Le gestionnaire de fichiers portable démarre automatiquement lorsqu'un disque amovible est connecté à un ordinateur sur lequel Kaspersky Endpoint Security n'est pas installé. Si le lancement automatique des applications n'est pas activé sur l'ordinateur, lancez le gestionnaire de fichiers portable manuellement. Pour ce faire, exécutez le fichier pmv.exe, stocké sur le disque amovible.



Gestionnaire de fichiers portable

Prise en charge du mode portable pour travailler avec des fichiers chiffrés

[Comment activer la prise en charge du mode portable pour travailler avec des fichiers chiffrés sur des lecteurs amovibles dans la console d'administration \(MMC\)](#)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
6. Sélectionnez l'option **Chiffrer tous les fichiers** ou **Chiffrer uniquement les nouveaux fichiers** dans la liste **Mode de chiffrement des appareils sélectionnés**.

Le mode portable est disponible avec le chiffrement des fichiers (FLE). Il n'est pas possible d'activer la prise en charge du mode portable pour le chiffrement du disque (FDE).

7. Cochez la case **Mode portable**.
8. Si nécessaire, [ajoutez des règles de chiffrement pour chaque disque amovible](#).
9. Enregistrez vos modifications.
10. Après avoir appliqué la stratégie, connectez le disque amovible à l'ordinateur.
11. Confirmez l'opération de chiffrement du disque amovible.
La fenêtre de création du mot de passe pour le gestionnaire de fichiers portable s'ouvre.
12. Définissez un mot de passe qui respecte les exigences en matière de complexité et confirmez-le.
13. Cliquez sur le bouton **OK**.

Kaspersky Endpoint Security chiffre les fichiers sur le disque amovible. Le gestionnaire de fichiers portable pour la manipulation des fichiers chiffrés sera lui aussi ajouté sur le disque amovible. S'il y a déjà des fichiers chiffrés sur le disque amovible, Kaspersky Endpoint Security les chiffre à nouveau à l'aide de sa propre clé. Cela permet à l'utilisateur d'accéder à tous les fichiers du disque amovible en mode portable.

[Comment activer le mode portable pour utiliser les fichiers chiffrés sur les disques amovibles dans Web Console](#) ?

1. Dans la fenêtre principale de Web Console, sélectionnez la section **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez activer l'utilisation du mode portable.
La fenêtre des propriétés de la stratégie s'ouvre.
3. Choisissez l'onglet **Paramètres de l'application**.
4. Accédez à la section **Chiffrement des données** → **Chiffrement des disques amovibles**.
5. Dans le groupe **Administration du chiffrement**, sélectionnez l'option **Chiffrer tous les fichiers** ou **Chiffrer uniquement les nouveaux fichiers**.

Le mode portable est disponible avec le chiffrement des fichiers (FLE). Il n'est pas possible d'activer la prise en charge du mode portable pour le chiffrement du disque (FDE).

6. Cochez la case **Mode portable**.
7. Si nécessaire, [ajoutez des règles de chiffrement pour chaque disque amovible](#).
8. Enregistrez vos modifications.
9. Après avoir appliqué la stratégie, connectez le disque amovible à l'ordinateur.
10. Confirmez l'opération de chiffrement du disque amovible.
La fenêtre de création du mot de passe pour le gestionnaire de fichiers portable s'ouvre.
11. Définissez un mot de passe qui respecte les exigences en matière de complexité et confirmez-le.
12. Cliquez sur le bouton **OK**.

Kaspersky Endpoint Security chiffre les fichiers sur le disque amovible. Le gestionnaire de fichiers portable pour la manipulation des fichiers chiffrés sera lui aussi ajouté sur le disque amovible. S'il y a déjà des fichiers chiffrés sur le disque amovible, Kaspersky Endpoint Security les chiffre à nouveau à l'aide de sa propre clé. Cela permet à l'utilisateur d'accéder à tous les fichiers du disque amovible en mode portable.

Obtention de l'accès aux fichiers chiffrés sur le disque amovible

Une fois que les fichiers ont été chiffrés sur un disque amovible prenant en charge le mode portable, vous pouvez y accéder d'une des manières suivantes :

- Si Kaspersky Endpoint Security n'est pas installé sur l'ordinateur, le gestionnaire de fichiers portable vous invite à saisir un mot de passe. Vous devrez saisir le mot de passe à chaque redémarrage de l'ordinateur ou reconnexion du disque amovible.
- Si l'ordinateur se trouve hors du réseau de l'entreprise et que Kaspersky Endpoint Security est installé sur l'ordinateur, l'application vous invite à saisir le mot de passe ou à envoyer à l'administrateur une demande d'accès aux fichiers. Après avoir obtenu l'accès aux fichiers sur le disque amovible, Kaspersky Endpoint Security enregistre la clé secrète dans le stockage de clés de l'ordinateur. Cela permettra d'accéder plus tard aux fichiers sans saisir le mot de passe, ni envoyer une demande à l'administrateur.

- Si l'ordinateur se trouve à l'intérieur du réseau de l'entreprise et que Kaspersky Endpoint Security est installé sur l'ordinateur, vous aurez accès à l'appareil sans devoir saisir le mot de passe. Kaspersky Endpoint Security reçoit alors la clé privée depuis le Serveur d'administration de Kaspersky Security Center auquel l'ordinateur est connecté.

Récupération du mot de passe en vue d'une utilisation en mode portable

Si vous avez oublié le mot de passe pour pouvoir utiliser le mode portable, vous devez connecter le disque amovible à un ordinateur doté de Kaspersky Endpoint Security et se trouvant à l'intérieur du réseau de l'entreprise. Vous aurez accès aux fichiers car la clé privée se trouve dans le stockage de clés de l'ordinateur ou sur le Serveur d'administration. Déchiffrez et chiffrez à nouveau les fichiers avec un nouveau mot de passe.

Particularités du mode portable en cas de connexion du disque amovible à un ordinateur d'un autre réseau

Si l'ordinateur se trouve hors du réseau de l'entreprise et qu'il est doté de Kaspersky Endpoint Security, vous pouvez accéder aux fichiers de la manière suivante :

- **Accès par mot de passe**

Après avoir saisi le mot de passe, vous pouvez visualiser, modifier et enregistrer les fichiers sur le disque amovible (*accès transparent*). Kaspersky Endpoint Security peut définir l'accès en lecture seule pour le disque amovible si les paramètres suivants de la stratégie de chiffrement des disques amovibles ont été configurés :

- La prise en charge du mode portable est désactivée.
- Le mode **Chiffrer tous les fichiers** ou **Chiffrer uniquement les nouveaux fichiers** est sélectionné.

Dans les autres cas, vous aurez un accès complet au disque amovible (autorisation de lecture et d'écriture). Vous pourrez ajouter et supprimer des fichiers.

Vous pouvez modifier les autorisations d'accès au disque amovible, même si le disque amovible est connecté à l'ordinateur. Si les autorisations d'accès au disque amovible ont été modifiées, Kaspersky Endpoint Security bloque l'accès aux fichiers et requiert à nouveau le mot de passe.

Une fois que le mot de passe a été saisi, il est impossible d'appliquer les paramètres de stratégie de chiffrement pour le disque amovible. Par conséquent, il est impossible de chiffrer ou de déchiffrer les fichiers sur le disque amovible.

- **Requête l'accès aux fichiers adressée à l'administrateur**

Si vous avez oublié le mot de passe pour pouvoir utiliser le mode portable, sollicitez l'accès aux fichiers à l'administrateur. Pour accéder aux fichiers, l'utilisateur doit envoyer une requête d'accès au fichier (fichier avec l'extension kesdc) à l'administrateur. L'utilisateur peut envoyer la requête d'accès au fichier par e-mail par exemple. L'administrateur envoie le fichier d'accès aux données chiffrées (fichier portant l'extension kesdr).

Après avoir suivi la procédure de récupération de mot de passe (Requête- Réponse), vous obtiendrez un accès transparent aux fichiers sur le disque amovible et un accès complet au disque amovible (accès écriture et lecture).

Vous pouvez appliquer une stratégie pour chiffrer les lecteurs amovibles et, par exemple, déchiffrer les fichiers. Après la récupération du mot de passe ou lors de la mise à jour de la stratégie, Kaspersky Endpoint Security propose de confirmer les modifications.

[Comment obtenir un fichier d'accès aux données chiffrées dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a sollicité la restauration de l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Chiffrement des données**.
7. Sous l'onglet **Chiffrement des données**, cliquez sur **Parcourir**.
8. Dans la fenêtre de sélection de la requête d'accès au fichier, indiquez le chemin d'accès au fichier reçu de l'utilisateur.

Les informations relatives à la requête de l'utilisateur s'affichent. Kaspersky Security Center crée le fichier clé d'accès. Envoyez à l'utilisateur un message électronique contenant le fichier clé d'accès aux données chiffrées. Ou enregistrez le fichier d'accès et transférez-le d'une manière quelconque.

[Comment obtenir le fichier d'accès aux données chiffrées dans Web Console](#)

1. Dans la fenêtre principale de Web Console, choisissez **Appareils** → **Appareils administrés**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.
3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.
4. Sélectionnez la section **Chiffrement des données**.
5. Cliquez sur le bouton **Sélectionner un fichier** et sélectionnez la requête d'accès au fichier envoyée par l'utilisateur (fichier portant l'extension kesdc).
Web Console affiche les informations relatives à la requête. Notamment, le nom de l'ordinateur sur lequel l'utilisateur sollicite l'accès au fichier.
6. Cliquez sur le bouton **Enregistrer la clé** et sélectionnez un dossier pour enregistrer le fichier clé d'accès aux données chiffrées (fichier portant l'extension kesdr).

Vous aurez alors accès à une clé d'accès aux données chiffrées à remettre à l'utilisateur.

Déchiffrement des disques amovibles

Vous pouvez déchiffrer un disque amovible à l'aide d'une stratégie. Une stratégie avec les paramètres définis de chiffrement des disques amovibles est composée pour un groupe d'administration défini. Par conséquent, le résultat du déchiffrement des données sur les disques amovibles dépend de l'ordinateur auquel le disque amovible est connecté.

Pour déchiffrer des disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
6. Si vous souhaitez déchiffrer tous les fichiers chiffrés présents sur les disques amovibles, sélectionnez, dans la liste déroulante **Mode de chiffrement**, l'action **Déchiffrer tout le disque amovible**.
7. Si vous souhaitez déchiffrer des données enregistrées sur différents disques amovibles, modifiez les règles de chiffrement des disques amovibles dont vous souhaitez déchiffrer les données. Pour ce faire, procédez comme suit :
 - a. Sélectionnez l'entrée de disque amovible qui vous intéresse dans la liste des disques amovibles pour lesquels des règles de chiffrement ont été définies.
 - b. Cliquez sur le bouton **Définir la règle** pour modifier la règle de chiffrement pour ce disque amovible. Le menu contextuel du bouton **Définir la règle** s'ouvre.
 - c. Dans le menu contextuel du bouton **Définir la règle**, sélectionnez l'option **Déchiffrer tous les fichiers**.
8. Enregistrez vos modifications.

Par conséquent, si un utilisateur connecte un disque amovible ou s'il est déjà connecté, Kaspersky Endpoint Security déchiffre le disque amovible. L'application signale à l'utilisateur que le déchiffrement peut durer un certain temps. Si l'utilisateur tente de retirer le disque amovible pendant le déchiffrement des données, Kaspersky Endpoint Security interrompt le déchiffrement des données et permet le retrait du disque amovible avant la fin du déchiffrement. Le déchiffrement des données se poursuivra à la prochaine connexion du disque amovible à l'ordinateur.

En cas d'échec du déchiffrement du disque amovible, consultez le rapport de **Chiffrement des données** dans l'interface de Kaspersky Endpoint Security. L'accès aux fichiers peut être bloqué par une autre application. Dans ce cas, essayez d'éjecter le disque amovible et de le connecter à nouveau à l'ordinateur.

Consultation des informations relatives au chiffrement des données

Pendant le chiffrement et le déchiffrement des données, Kaspersky Security Center reçoit de Kaspersky Endpoint Security des informations sur l'application des paramètres de chiffrement sur les postes clients.

Chaque ordinateur peut avoir un des états de chiffrement suivants :

- *Aucune stratégie de chiffrement définie.* Aucune stratégie de chiffrement de Kaspersky Security Center n'a été attribuée à l'ordinateur.

- *En cours d'application d'une stratégie.* Le chiffrement et/ou le déchiffrement des données est en cours sur l'ordinateur.
- *Erreur.* Une erreur s'est produite lors du chiffrement et/ou du déchiffrement des données sur l'ordinateur.
- *Redémarrage requis.* Pour initialiser ou terminer le chiffrement ou le déchiffrement des données sur l'ordinateur, il faut redémarrer le système d'exploitation.
- *Conforme à la stratégie.* Le chiffrement des données sur l'ordinateur est exécuté conformément aux paramètres de chiffrement indiqués dans la stratégie de Kaspersky Security Center appliquée à l'ordinateur.
- *Annulé par l'utilisateur.* L'utilisateur n'a pas confirmé l'exécution de l'opération de chiffrement des fichiers sur le disque amovible.

Consultation des états du chiffrement

Pour consulter les états de chiffrement des données de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
L'onglet **Appareils** dans l'espace de travail reprend les propriétés des ordinateurs du groupe d'administration sélectionné.
4. Sous l'onglet **Appareils** de l'espace de travail, déplacez le curseur au maximum à droite.
5. Si la colonne **État de chiffrement** ne s'affiche pas, procédez comme suit :
 - a. Cliquez-droit pour ouvrir le menu contextuel des titres du tableau.
 - b. Dans le menu contextuel, ouvrez la liste déroulante **Apparence** et choisissez **Ajouter ou supprimer des colonnes**.
La fenêtre **Ajout ou suppression de colonnes** s'ouvre.
 - c. Dans la fenêtre **Ajout ou suppression de colonnes**, cochez la case **État de chiffrement**.
 - d. Cliquez sur le bouton **OK**.

La colonne **État de chiffrement** reprend les états de chiffrement des données pour les ordinateurs du groupe d'administration sélectionné. Cet état est obtenu sur la base des informations relatives au chiffrement des fichiers sur les disques locaux de l'ordinateur et au chiffrement du disque.

Consultation des statistiques de chiffrement sur les volets d'informations de Kaspersky Security Center

Pour consulter les états de chiffrement sur les barres d'informations de Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, choisissez l'entrée **Serveur d'administration – <Nom de l'ordinateur>**.
3. Dans l'espace de travail situé à droite de l'arborescence de la Console de l'administration, choisissez l'onglet **Statistiques**.
4. Créez une page avec les volets d'informations contenant les statistiques du chiffrement des données. Pour ce faire, procédez comme suit :
 - a. Sous l'onglet **Statistiques**, cliquez sur le bouton **Configurer l'apparence**.
La fenêtre **Propriétés : Statistiques** s'ouvre.
 - b. Dans la fenêtre **Propriétés : Statistiques** qui s'ouvre, cliquez sur **Ajouter**.
La fenêtre **Propriétés : Nouvelle page** s'ouvre.
 - c. Saisissez le nom de la page dans la section **Général** de la fenêtre **Propriétés : Nouvelle page**.
 - d. Dans la section **Volets d'informations**, cliquez sur **Ajouter**.
La fenêtre **Nouveau panneau d'informations** s'ouvre.
 - e. Dans le groupe **État de la protection** de la fenêtre **Nouveau panneau d'informations**, choisissez l'option **Chiffrement des périphériques**.
 - f. Cliquez sur le bouton **OK**.
La fenêtre **Propriétés : Chiffrement des appareils** s'ouvre.
 - g. Modifiez les paramètres de la barre d'informations en fonction de besoins. Utilisez pour ce faire les options des sections **Apparence** et **Appareils** de la fenêtre **Propriétés : Chiffrement des appareils**.
 - h. Cliquez sur le bouton **OK**.
 - i. Répétez les étapes d à h des instructions et dans la section **État de la protection** de la fenêtre **Nouveau panneau d'informations**, sélectionnez l'option **Chiffrement des disques amovibles**.
Les barres d'informations ajoutées figurent dans la liste **Barres d'informations** de la fenêtre **Propriétés : Nouvelle page**.
 - j. Dans la fenêtre **Propriétés : Nouvelle page**, cliquez sur **OK**.
Le nom des pages contenant les barres d'informations créées aux étapes antérieures apparaît dans la liste **Pages** de la fenêtre **Propriétés : Statistiques**.
 - k. Dans la fenêtre **Propriétés : Statistiques**, cliquez sur **Fermer**.
5. Sous l'onglet **Statistiques**, ouvrez la page créée aux étapes antérieures des instructions.

Les barres d'informations qui reprennent les états de chiffrement des ordinateurs et des disques amovibles s'affichent.

Consultation des erreurs de chiffrement des fichiers sur les disques locaux de l'ordinateur

Pour consulter les erreurs de chiffrement des fichiers sur les disques durs locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration où se trouve l'ordinateur de l'utilisateur pour lequel vous souhaitez consulter la liste des erreurs de chiffrement des fichiers.
3. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur dans la liste et ouvrez le menu contextuel d'un clic droit.
5. Dans le menu contextuel de l'ordinateur, sélectionnez l'option **Propriétés**. Dans la fenêtre **Propriétés: <nom de l'ordinateur>** qui s'ouvre, sélectionnez la section **Endpoint Protection**.
6. Dans la section **Endpoint Protection** de la fenêtre **Propriétés: <nom de l'ordinateur>** à l'aide du lien **Consulter les erreurs de chiffrement des données**, ouvrez la fenêtre **Erreurs de chiffrement des données**.

Celle-ci reprend les informations relatives aux erreurs de chiffrement des fichiers sur les disques durs locaux de l'ordinateur. Si l'erreur a été corrigée, Kaspersky Security Center supprime les informations qui la concernent dans la fenêtre **Erreurs de chiffrement des données**.

Consultation du rapport sur le chiffrement des données

Pour consulter le rapport sur le chiffrement des données, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.
L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. Dans la section **Autre** de la fenêtre **Sélection du type de modèle du rapport**, sélectionnez une des options suivantes :
 - **Rapport de l'état de chiffrement des appareils administrés.**
 - **Rapport de l'état de chiffrement des appareils mémorisés.**
 - **Rapport sur les erreurs de chiffrement de fichiers.**
 - **Rapport sur le blocage de l'accès aux fichiers chiffrés.**

Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.

5. Choisissez le modèle de rapport créé aux étapes précédentes.
6. Dans le menu contextuel du modèle, sélectionnez l'option **Afficher le rapport**.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Utilisation des appareils chiffrés en l'absence d'accès à ceux-ci.

Obtention de l'accès à l'appareil chiffrés

L'utilisateur peut devoir solliciter l'accès aux appareils chiffrés dans les cas suivants :

- Le disque dur a été chiffré sur un autre ordinateur.
- L'ordinateur est privé de la clé de chiffrement pour l'appareil (par exemple, lors de la première sollicitation d'un disque amovible chiffré sur cet ordinateur) et il n'y a pas de communication avec Kaspersky Security Center.
Après que l'utilisateur a activé la clé d'accès à l'appareil chiffré, Kaspersky Endpoint Security enregistre la clé de chiffrement sur l'ordinateur de l'utilisateur et octroie l'accès à cet appareil pour les requêtes suivantes, même en l'absence de communication avec Kaspersky Security Center.

L'obtention de l'accès aux appareils chiffrés s'opère de la manière suivante :

1. L'utilisateur crée via l'interface de l'application Kaspersky Endpoint Security la requête d'accès au fichier avec l'extension kesdc et la transmet à son administrateur du réseau local de l'organisation.
2. L'administrateur crée le fichier clé d'accès dans la Console d'administration de Kaspersky Security Center avec l'extension kesdr et la transmet à l'utilisateur.
3. L'utilisateur applique la clé d'accès.

Restauration des données sur les appareils chiffrés.

Pour utiliser les appareils chiffrés, l'utilisateur peut utiliser l'[utilitaire de restauration des appareils chiffrés](#) (ci-après, l'utilitaire de restauration). Ce besoin peut se présenter dans les situations suivantes :

- Échec de la procédure d'obtention de l'accès à l'aide de la clé d'accès
- Absence des modules de chiffrement sur l'ordinateur avec l'appareil chiffré

Les données nécessaires à la restauration de l'accès aux appareils à l'aide de l'utilitaire de restauration se trouvent pendant quelque temps dans la mémoire de l'ordinateur de l'utilisateur en clair. Pour réduire la probabilité d'un accès non autorisé à ces données, il est conseillé d'exécuter la restauration de l'accès aux appareils chiffrés sur des ordinateurs de confiance.

La restauration des données sur les appareils chiffrés s'opère de la manière suivante :

1. L'utilisateur crée une requête d'accès au fichier à l'aide de l'utilitaire de restauration et transmet ce fichier portant l'extension fdertc à l'administrateur du réseau local de l'organisation.
2. L'administrateur crée le fichier clé d'accès dans la Console d'administration de Kaspersky Security Center avec l'extension fdertr et la transmet à l'utilisateur.
3. L'utilisateur applique la clé d'accès.

Pour restaurer les données sur les disques durs système chiffrés, l'utilisateur peut également indiquer les identifiants de l'Agent d'authentification dans l'utilitaire de restauration. Si les métadonnées du compte utilisateur de l'Agent d'authentification sont endommagées, l'utilisateur devra réaliser la procédure de restauration à l'aide de la requête d'accès au fichier.

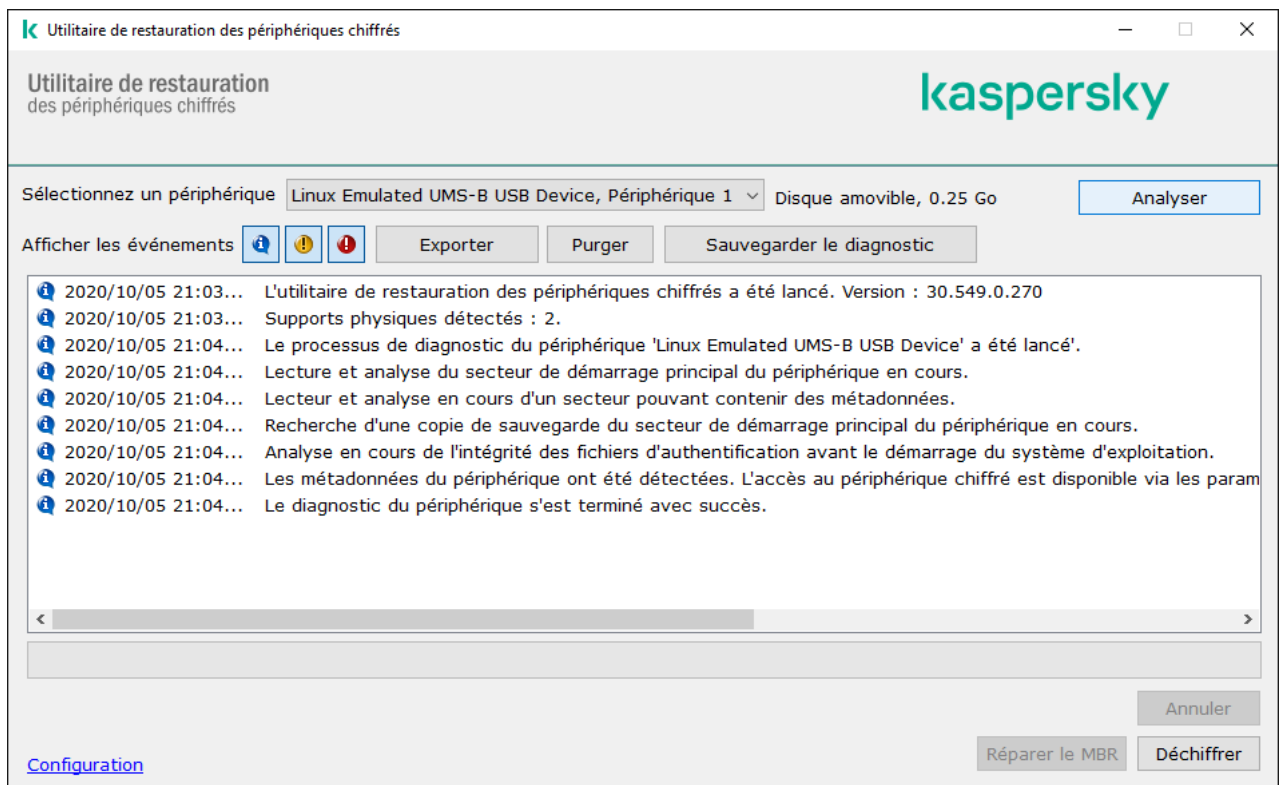
Avant de restaurer les données sur les appareils chiffrés, il est conseillé d'annuler l'application de la stratégie de Kaspersky Security Center ou de désactiver le chiffrement dans les paramètres de la stratégie de Kaspersky Security Center sur l'ordinateur sur lequel la procédure va être exécutée. Ceci permet d'éviter un nouveau chiffrement de l'appareil.

Récupération de données à l'aide de l'utilitaire de restauration FDERT

Le système de fichiers peut s'endommager en cas de dysfonctionnement du disque dur. Dans ce cas, les données protégées par la technologie Kaspersky Disk Encryption ne seraient plus accessibles. Vous pouvez déchiffrer les données et les copier sur un nouveau disque.

La récupération de données sur un disque protégé par la technologie Kaspersky Disk Encryption comprend les étapes suivantes :

1. Création d'un utilitaire de restauration portable (cf. ill. ci-dessous).
2. Connexion d'un disque à l'ordinateur qui n'est pas doté des modules de chiffrement de Kaspersky Endpoint Security.
3. Lancement de l'utilitaire de restauration et diagnostic du disque dur.
4. Accès aux données sur le disque. Pour ce faire, il faut saisir les informations d'identification de l'Agent d'authentification ou lancez la procédure de récupération (Requête-Réponse).



Utilitaire de restauration FDERT

Création d'un utilitaire de restauration portable

Pour créer un fichier exécutable de l'utilitaire de restauration, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Assistance**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Restauration d'un appareil chiffré**.
L'utilitaire de restauration des appareils chiffrés est lancé.
3. Dans la fenêtre de l'utilitaire de restauration, cliquez sur le bouton **Créer un utilitaire de restauration portable**.
4. Enregistrez l'utilitaire de restauration portable dans la mémoire de l'ordinateur.

Le fichier exécutable de l'utilitaire de restauration fdert.exe est enregistré dans le dossier indiqué. Copiez l'utilitaire de restauration sur l'ordinateur dépourvu des modules de chiffrement de Kaspersky Endpoint Security. Ceci permet d'éviter un nouveau chiffrement du disque.

Les données nécessaires à la restauration de l'accès aux appareils à l'aide de l'utilitaire de restauration se trouvent pendant quelque temps dans la mémoire de l'ordinateur de l'utilisateur en clair. Pour réduire la probabilité d'un accès non autorisé à ces données, il est conseillé d'exécuter la restauration de l'accès aux appareils chiffrés sur des ordinateurs de confiance.

Récupération des données du disque dur

Pour restaurer l'accès à l'appareil chiffré à l'aide de l'utilitaire de restauration, procédez comme suit :

1. Exécutez le fichier intitulé fdert.exe, qui est le fichier exécutable de l'Utilitaire de restauration. Ce fichier est créé par Kaspersky Endpoint Security.
2. Dans la fenêtre de l'utilitaire de restauration dans la liste déroulante **Sélectionnez un appareil**, sélectionnez l'appareil chiffré auquel vous souhaitez restaurer l'accès.
3. Cliquez sur le bouton **Analyser** pour que l'utilitaire puisse définir l'action à exécuter sur l'appareil chiffré : débloquer ou déchiffrer.
Si la fonction de chiffrement de Kaspersky Endpoint Security est disponible sur l'ordinateur, l'utilitaire de restauration propose de débloquer l'appareil. Lors du déblocage, l'appareil n'est pas déchiffré. Il est simplement possible d'y accéder directement. Si la fonction de chiffrement de Kaspersky Endpoint Security n'est pas disponible sur l'ordinateur, l'utilitaire de restauration propose de déchiffrer l'appareil.
4. Si vous souhaitez importer des informations de diagnostic, cliquez sur le bouton **Sauvegarder le diagnostic**.
L'utilitaire enregistre une archive avec des fichiers contenant les informations de diagnostic.
5. Cliquez sur le bouton **Réparer le MBR** si le diagnostic du système du disque dur chiffré a généré un message qui vous signale des problèmes liés au secteur de démarrage principal (MBR) de l'appareil.
La réparation du secteur de démarrage principal peut accélérer la récupération d'informations indispensables au déblocage ou au déchiffrement de l'appareil.
6. Appuyez sur le bouton **Débloquer** ou **Déchiffrer** en fonction des résultats du diagnostic.
7. Si vous souhaitez récupérer les données à l'aide d'un compte d'Agent d'authentification, sélectionnez l'option **Utiliser les paramètres du compte de l'Agent d'authentification** et saisissez les informations d'identification de l'Agent d'authentification.

Cette méthode est disponible uniquement en cas de restauration des données sur le disque dur système. Si le disque dur système ont été endommagées ou si vous avez oublié les données du compte utilisateur de l'Agent d'authentification, il faudra obtenir une clé d'accès auprès de l'administrateur du réseau local de l'organisation pour restaurer les données sur l'appareil chiffré.

8. Si vous souhaitez lancer la procédure de récupération, procédez comme suit :

- a. Choisissez l'option **Désigner manuellement la clé d'accès à l'appareil**.
- b. Cliquez sur le bouton **Obtenir la clé d'accès** et enregistrez la requête d'accès au fichier dans la mémoire de l'ordinateur (fichier portant l'extension fdertc).
- c. Transmettez la requête d'accès au fichier à l'administrateur du réseau local de l'organisation.

Ne fermez pas la fenêtre **Obtenir la clé d'accès à l'appareil** tant que vous n'aurez pas reçu la clé d'accès. Si vous ouvrez à nouveau cette fenêtre, la clé d'accès créée antérieurement par l'administrateur ne pourra pas être appliquée.

- d. Recevez et enregistrez le fichier d'accès (fichier avec l'extension fdertr) créé et transmis par l'administrateur du réseau local de l'organisation (cf. instructions ci-dessous).
 - e. Téléchargez le fichier d'accès dans la fenêtre **Obtenir la clé d'accès à l'appareil**.
9. Si vous déchiffrez un appareil, vous devez configurer des paramètres complémentaires de déchiffrement :

- Indiquez la zone du déchiffrement :
 - Si vous voulez déchiffrer tout l'appareil, choisissez l'option **Déchiffrer tout l'appareil**.
 - Si vous voulez déchiffrer une partie des données sur l'appareil, choisissez l'option **Déchiffrer certains secteurs de l'appareil** et définissez les limites de la zone de déchiffrement.
- Choisissez l'emplacement de l'enregistrement des données déchiffrées :
 - Si vous voulez que les données de l'appareil original soient écrasées par les données déchiffrées, décochez la case **Déchiffrement dans le fichier d'image de disque**.
 - Si vous voulez enregistrer les données déchiffrées séparément des données originales chiffrées, cochez la case **Déchiffrement dans le fichier d'image de disque** et à l'aide du bouton **Parcourir**, indiquez le chemin de l'emplacement où il faudra enregistrer le fichier au format VHD.

10. Cliquez sur le bouton **OK**.

Le déblocage/le déchiffrement de l'appareil est lancé.

[Procédure de création de fichier d'accès pour les données chiffrées dans la Console d'administration \(MMC\)](#) 

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Chiffrement et protection des données** → **Appareils chiffrés**.
3. Dans l'espace de travail, choisissez l'appareil chiffré pour lequel vous voulez créer un fichier clé l'accès, puis, dans le menu contextuel de l'appareil, choisissez l'option **Obtenir l'accès à l'appareil dans Kaspersky Endpoint Security for Windows (11.6.0)**.

Si vous n'êtes pas certain de connaître l'ordinateur pour lequel la requête d'accès au fichier a été créée, choisissez dans l'arborescence de la Console d'administration le dossier **Avancé** → **Chiffrement et protection des données**, puis, dans l'espace de travail, cliquez sur le lien **Obtenir la clé de chiffrement de l'appareil dans Kaspersky Endpoint Security for Windows (11.6.0)**.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'algorithme de chiffrement à utiliser : **AES256** ou **AES56**.
L'algorithme de chiffrement des données dépend de la bibliothèque de chiffrement AES incluse dans la distribution : *Strong encryption (AES256)* ou *Lite encryption (AES56)*. La bibliothèque de chiffrement AES est installée en même temps que l'application.
5. Cliquez sur le bouton **Parcourir**. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès à la requête d'accès au fichier envoyée par l'utilisateur avec l'extension fdertc.
6. Cliquez sur le bouton **Ouvrir**.

Les informations relatives à la requête de l'utilisateur s'affichent. Kaspersky Security Center crée le fichier clé d'accès. Envoyez à l'utilisateur un message électronique contenant le fichier clé d'accès aux données chiffrées. Ou enregistrez le fichier d'accès et transférez-le d'une manière quelconque.

[Procédure de création du fichier d'accès aux données chiffrées dans Web Console](#)

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Chiffrement et protection des données** → **Appareils chiffrés**.

2. Cochez la case en regard du nom de l'ordinateur sur lequel vous souhaitez récupérer les données.

3. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode autonome**.

L'assistant d'octroi de l'accès à l'appareil s'ouvre.

4. Suivez les instructions de l'assistant d'octroi de l'accès à l'appareil.

a. Sélectionnez le plug-in **Kaspersky Endpoint Security for Windows**.

b. Sélectionnez l'algorithme de chiffrement à utiliser : **AES256** ou **AES56**.

L'algorithme de chiffrement des données dépend de la bibliothèque de chiffrement AES incluse dans la distribution : *Strong encryption (AES256)* ou *Lite encryption (AES56)*. La bibliothèque de chiffrement AES est installée en même temps que l'application.

c. Cliquez sur le bouton **Sélectionner un fichier** et sélectionnez la requête d'accès au fichier reçue de l'utilisateur (fichier avec l'extension fdertc).

d. Cliquez sur le bouton **Enregistrer la clé** et sélectionnez un dossier pour enregistrer le fichier de clé d'accès aux données chiffrées (fichier avec l'extension fdertr).

Vous aurez alors accès à une clé d'accès aux données chiffrées à remettre à l'utilisateur.

Création d'un disque de dépannage du système d'exploitation

Un disque de dépannage peut être utile quand, pour une raison quelconque, l'accès au disque dur système chiffré n'est pas possible et que le système d'exploitation ne peut être chargé.

Vous pouvez charger une image du système d'exploitation Windows à l'aide du disque de dépannage et restaurer l'accès au disque dur système chiffré à l'aide de l'utilitaire de restauration repris dans l'image du système d'exploitation.

Pour créer un disque de dépannage du système d'exploitation, procédez comme suit :

1. [Créez le fichier exécutable de l'utilitaire de restauration des appareils chiffrés](#).

2. Créez l'image utilisateur de l'environnement de pré-installation Windows. Pendant cette procédure, ajoutez l'image du fichier exécutable de l'utilitaire de restauration des appareils chiffrés.

3. Placez l'image utilisateur de l'environnement de pré-installation Windows sur un support amovible tel qu'un CD ou d'un disque amovible.

Les instructions relatives à la création de l'image utilisateur de l'environnement de pré-installation Microsoft figurent dans l'aide de Microsoft (par exemple, sur le [site de Microsoft TechNet](#) ²).

Administration de l'application via la ligne de commande

Vous pouvez administrer Kaspersky Endpoint Security via la ligne de commande. Vous pouvez consulter la liste des commandes d'administration de l'application à l'aide de la commande `HELP`. Pour obtenir de l'aide sur la syntaxe d'une commande en particulier, saisissez `HELP <commande>`.

Les caractères spéciaux doivent être escamotés dans la commande. Pour escamoter les caractères `&`, `|`, `(`, `)`, `<`, `>`, `^`, utilisez le caractère `^` (par exemple, pour utiliser le caractère `&`, saisissez `^&`). Pour escamoter le caractère `%`, saisissez `%%`.

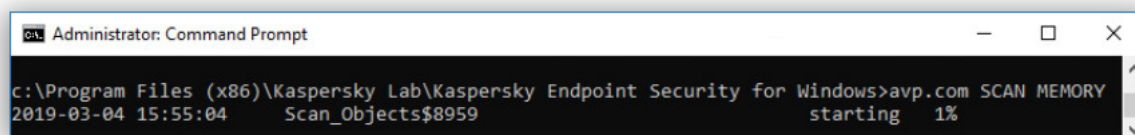
Commandes AVP

Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande `cmd` au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.
3. Utilisez le modèle suivant pour exécuter la commande :

```
avp.com <commande> [paramètres]
```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



Administration de l'application via la ligne de commande

SCAN. Recherche de virus

Lancer la tâche de recherche de virus.

Syntaxe de la commande

```
SCAN [<zone d'analyse>] [<action lorsqu'une menace est détectée>] [<types de fichiers>] [<exclusion de l'analyse>] [/ R [A]: <fichier de rapport>] [<technologie d'analyse>] [/C: <fichier avec paramètres de recherche de virus>]
```

| Zone d'analyse | |
|----------------|---|
| <fichiers à | Liste de fichiers et de dossiers séparés par un espace. Les longs chemins d'accès |

| | |
|-----------------------------|--|
| analyser> | doivent être saisis entre guillemets. Les raccourcis (format MS-DOS) n'ont pas besoin d'être placés entre guillemets. Par exemple : <ul style="list-style-type: none"> • "C:\Program Files (x86)\Example Folder" : long chemin d'accès. • C:\PROGRA~2\EXAMPL~1 : chemin court. |
| /ALL | Lancer la tâche <i>Analyse complète</i> . Kaspersky Internet Endpoint analyse les objets suivants : <ul style="list-style-type: none"> • Mémoire du noyau • Objets chargés au lancement du système d'exploitation • Secteurs d'amorçage • Sauvegarde du système d'exploitation • Tous les disques durs et amovibles |
| /MEMORY | Analyser la mémoire du noyau |
| /STARTUP | Analyser les objets chargés au lancement du système d'exploitation |
| /MAIL | Analyser la boîte aux lettres Outlook |
| /REMDRIVES | Analyser les disques amovibles. |
| /FIXDRIVES | Analyser les disques durs. |
| /NETDRIVES | Analyser les disques réseau. |
| /QUARANTINE | Analyser les fichiers dans la quarantaine de Kaspersky Endpoint Security. |
| /@:<liste des fichiers.lst> | Analyser les fichiers et les dossiers de la liste. Chaque fichier de la liste doit être saisi sur une nouvelle ligne. Les longs chemins d'accès doivent être saisis entre guillemets. Les raccourcis (format MS-DOS) n'ont pas besoin d'être placés entre guillemets. Par exemple : <ul style="list-style-type: none"> • "C:\Program Files (x86)\Example Folder" : long chemin d'accès. • C:\PROGRA~2\EXAMPL~1 : chemin court. |

| Action en cas de détection d'une menace | |
|---|--|
| /i0 | Notifier. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives. |
| /i1 | Désinfecter ; bloquer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives. |
| /i2 | Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, |

| | |
|-----|--|
| | <p>Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.</p> <p>Cette action est sélectionnée par défaut.</p> |
| /i3 | Désinfecter les fichiers infectés détectés. Si la désinfection est impossible, supprimer les fichiers infectés. Supprimer également les fichiers composés (par exemple, les archives) s'il est impossible de désinfecter ou de supprimer le fichier infecté. |
| /i4 | Supprimer les fichiers infectés. Supprimer également les fichiers composés (par exemple, les archives) s'il est impossible de supprimer le fichier infecté. |
| /i8 | Demander à l'utilisateur de confirmer l'action immédiatement après la détection d'une menace. |
| /i9 | Demander à l'utilisateur de confirmer l'action après l'analyse. |

| | |
|--------------------------|--|
| Types de fichiers | |
| /fe | Fichiers analysés par extension. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables . Le format du fichier sera déterminé sur la base de son extension. |
| /fi | Fichiers analysés par format. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables . Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte. |
| /fa | Tous les fichiers. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension). Le paramètre est sélectionné par défaut. |

| | |
|--------------------------------|---|
| Exclusions de l'analyse | |
| -e:a | Exclusion de l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE. |
| -e:b | Exclusion de l'analyse des bases de messagerie et des messages électroniques entrants et sortants. |
| -E:<masque de fichier> | Exclusion de l'analyse des fichiers sur la base d'un masque. Par exemple : <ul style="list-style-type: none"> Le masque *.exe reprend tous les chemins d'accès aux fichiers portant l'extension exe. Le masque example reprend tous les chemins d'accès aux fichiers dont le nom est EXAMPLE. |
| -e: <secondes> | Exclusion de l'analyse des fichiers dont la durée d'analyse dépasse la valeur spécifiée en secondes. |
| -es:<mégaoctets> | Exclusion de l'analyse des fichiers dont la taille dépasse la valeur spécifiée en mégaoctets. |

| | |
|--|---|
| Mode de sauvegarde des événements dans le fichier de rapport. | |
| /R:<fichier de rapport> | Enregistrer uniquement les événements critiques dans le fichier de rapport. |

| | |
|--------------------------|---|
| /RA:<fichier de rapport> | Enregistrer tous les événements dans le fichier de rapport. |
|--------------------------|---|

| Technologies d'analyse | |
|------------------------|---|
| /iChecker=on off | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |
| /iSwift=on off | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS. |

| Paramètres avancés | |
|--|---|
| /C: <fichier avec paramètres de recherche de virus> | Fichier avec les paramètres de la tâche de recherche de virus. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : [<zone d'analyse>] [<action en cas de détection d'une menace>] [<types de fichiers>] [<exclusions de l'analyse>] [/R[A]:<fichier de rapport>] [<technologies d'analyse>]. |

Exemple :

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Mise à jour des bases de données et des modules de l'application

Lancer la tâche *Mise à jour*.

Syntaxe de la commande

```
UPDATE [local]["<source de la mise à jour>"] [/R[A]:<fichier de rapport>] [/C:<fichier avec les paramètres de mise à jour>]
```

| Paramètres de la tâche de mise à jour | |
|---------------------------------------|---|
| local | Démarrage de la tâche de <i>mise à jour</i> qui a été créée automatiquement après l'installation de l'application. Vous pouvez modifier les paramètres de la tâche de <i>mise à jour</i> dans l'interface |

de l'application locale ou dans la console de Kaspersky Security Center. Si ce paramètre n'est pas configuré, Kaspersky Endpoint Security lance la tâche de *mise à jour* avec les paramètres par défaut ou avec les paramètres indiqués dans la commande. Vous pouvez configurer les paramètres de la tâche de mise à jour comme suit :

- UPDATE lance la tâche de *mise à jour* avec les paramètres par défaut : la source de mise à jour correspond aux serveurs de mise à jour de Kaspersky, le compte est System et d'autres paramètres par défaut.
- UPDATE local lance la tâche de *mise à jour* qui a été créée automatiquement après l'installation (tâche prédéfinie).
- UPDATE <paramètres de mise à jour> lance la tâche de *mise à jour* avec des paramètres définis manuellement (voir ci-dessous).

| Source des mises à jour | |
|----------------------------------|---|
| " <source de la mise à jour>" | Adresse du serveur HTTP ou FTP ou du dossier partagé contenant le paquet de mises à jour. Vous ne pouvez indiquer qu'une seule source de mise à jour. Si la source de mise à jour n'est pas précisée, Kaspersky Endpoint Security utilise la source par défaut, c'est-à-dire les serveurs de mises à jour de Kaspersky. |

| Mode de sauvegarde des événements dans le fichier de rapport. | |
|---|---|
| /R:<fichier de rapport> | Enregistrer uniquement les événements critiques dans le fichier de rapport. |
| /RA:<fichier de rapport> | Enregistrer tous les événements dans le fichier de rapport. |

| Paramètres avancés | |
|--|--|
| /C:<fichier avec les options de mise à jour> | Fichier avec les paramètres de la tâche <i>Mise à jour</i> . Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : ["<source de mise à jour>"] [/R[A]: <fichier de rapport>]. |

Exemple :

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://mon_serveur/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Restauration de la dernière mise à jour

Annuler les dernières mises à jour des bases antivirus. Cela permet de revenir le cas échéant à l'utilisation de la version antérieure des bases et des modules de l'application, par exemple si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sûre.

Syntaxe de la commande

```
ROLLBACK [/R[A]:<fichier de rapport>]
```

| Mode de sauvegarde des événements dans le fichier de rapport. | |
|---|---|
| /R:<fichier de rapport> | Enregistrer uniquement les événements critiques dans le fichier de rapport. |
| /RA:<fichier de rapport> | Enregistrer tous les événements dans le fichier de rapport. |

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Traces

Activer/désactiver le traçage. [Les fichiers de traçage](#) sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application. Les fichiers de traçage, à l'exception des fichiers de traçage de l'Agent d'authentification, sont stockés dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces. Par défaut, le traçage est désactivé.

Syntaxe de la commande

```
TRACES on|off [<niveau de traçage>] [<paramètres complémentaires>]
```

| Niveau de traçage | |
|---------------------|---|
| <niveau de traçage> | <p>Niveau de détail du traçage Valeurs possibles :</p> <ul style="list-style-type: none">• 100 (critique). Uniquement les messages relatifs aux erreurs irrémédiables.• 200 (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables.• 300 (diagnostique). Messages relatifs à toutes les erreurs et messages d'avertissement.• 400 (important). Messages relatifs à l'ensemble des erreurs, des avertissements, ainsi que des informations supplémentaires.• 500 (ordinaire). Messages relatifs à l'ensemble des erreurs, avertissements, ainsi que des informations détaillées sur le fonctionnement de l'application en mode normal (valeur par défaut).• 600 (bas). Tous les messages. |

| Paramètres avancés | |
|--------------------|---|
| all | Exécuter la commande avec les paramètres <code>dbg</code> , <code>file</code> et <code>mem</code> . |

| | |
|------|--|
| dbg | Utiliser la fonction OutputDebugString et enregistrer le fichier de traçage. La fonction OutputDebugString envoie une chaîne de caractères au débogueur de l'application pour l'afficher. Pour en savoir plus, consulter le site de MSDN . |
| file | Enregistrer un fichier de traçage (sans limite de taille). |
| rot | Enregistrer les résultats du traçage dans un nombre limité de fichiers de taille limitée et écraser les anciens fichiers quand la limite est atteinte. |
| mem | Écrire les résultats du traçage dans les fichiers dump. |

Exemples :

- avp.com TRACES on 500
- avp.com TRACES on 500 dbg
- avp.com TRACES off
- avp.com TRACES on 500 dbg mem
- avp.com TRACES off file

START. Activation du profil

Lancer l'exécution du profil (par exemple, lancer la mise à jour des bases ou activer le module de la protection).

Syntaxe de la commande

```
START <profil> [/R[A]:<fichier de rapport>]
```

| Profil | |
|----------|--|
| <profil> | Nom du profil. Un <i>profil</i> désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande <code>HELP START</code> . |

| Mode de sauvegarde des événements dans le fichier de rapport. | |
|---|---|
| /R:<fichier de rapport> | Enregistrer uniquement les événements critiques dans le fichier de rapport. |
| /RA:<fichier de rapport> | Enregistrer tous les événements dans le fichier de rapport. |

Exemple :

```
avp.com START Scan_Objects
```

STOP. Désactivation du profil

Arrêter le profil en cours d'exécution (par exemple, arrêter l'analyse des disques amovibles ou désactiver le module de la protection).

L'exécution de la commande requiert l'[activation de la Protection par mot de passe](#). L'utilisateur doit disposer des autorisations **Désactivation des modules de la protection, Désactivation des modules de contrôle**.

Syntaxe de la commande

```
STOP <profil> /login=<nom d'utilisateur> /password=<mot de passe>
```

| Profil | |
|----------|---|
| <profil> | Nom du profil. Un <i>profil</i> désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande <code>HELP STOP</code> . |

| Autorisation | |
|--|--|
| /login=<nom d'utilisateur> /password=<mot de passe> | Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe . |

STATUS. État du profil

Afficher les informations sur l'état des [profils de l'application](#) (par exemple, `running` ou `completed`). Pour connaître la liste des profils disponibles, utilisez la commande `HELP STATUS`.

Kaspersky Endpoint Security affiche également les informations sur l'état des profils de service. Les profils de service peuvent être utiles lors de l'interaction avec le Support Technique de Kaspersky.

Syntaxe de la commande

```
STATUS [<profil>]
```

STATISTICS. Statistiques de l'exécution du profil

Afficher les statistiques sur le [profil de l'application](#) (par exemple, heure de l'analyse ou nombre de menaces détectées). Pour connaître la liste des profils disponibles, utilisez la commande `HELP STATISTICS`.

Syntaxe de la commande

```
STATISTICS <profils>
```

RESTORE. Restauration des fichiers

Restaurer un fichier depuis la Sauvegarde vers son emplacement d'origine. Si un fichier portant le même nom se trouve déjà à cet emplacement, le suffixe "-copy" est ajouté au nom du fichier. Le fichier restauré conserve son nom d'origine.

L'exécution de la commande requiert l'[activation de la Protection par mot de passe](#). L'utilisateur doit posséder l'autorisation **Restauration depuis la sauvegarde**.

La *Sauvegarde* est le stockage qui contient les copies de sauvegarde des objets qui ont été modifiés ou supprimés lors de la désinfection. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier C:\ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès total à ce dossier sont accordées aux utilisateurs du groupe Administrateurs. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Kaspersky Endpoint Security n'offre pas la possibilité de configurer les autorisations d'accès des utilisateurs aux copies de sauvegarde des fichiers.

Syntaxe de la commande

```
RESTORE [/REPLACE] <nom du fichier> /login=<nom d'utilisateur> /password=<mot de passe>
```

| Paramètres avancés | |
|--------------------|------------------------------|
| /REPLACE | Écraser le fichier existant. |
| <nom du fichier> | Nom du fichier à restaurer. |

| Autorisation | |
|--|--|
| /login=<nom d'utilisateur> /password=<mot de passe> | Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe . |

Exemple :

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Exportation des paramètres de l'application

Exporter les paramètres de Kaspersky Endpoint Security dans un fichier. Le fichier est enregistré dans C:\Windows\SysWOW64.

Syntaxe de la commande

```
EXPORT <profil> <nom du fichier>
```

| | |
|---------------------------|---|
| Profil | |
| <profil> | Nom du profil. Un <i>profil</i> désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande <code>HELP EXPORT</code> . |
| Fichier à exporter | |
| <nom du fichier> | Nom dans lequel les paramètres de l'application vont être exportés. Vous pouvez exporter les paramètres du profil dans un fichier de configuration au format DAT ou CFG, un fichier au format TXT ou un document au format XML. |

Exemples :

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importation des paramètres de l'application

Importer les paramètres de Kaspersky Endpoint Security depuis un fichier créé à l'aide de la commande `EXPORT`.

L'exécution de la commande requiert l'[activation de la Protection par mot de passe](#). L'utilisateur doit avoir l'autorisation **Configuration des paramètres de l'application**.

Syntaxe de la commande

```
IMPORT <nom du fichier> /login=<nom d'utilisateur> /password=<mot de passe>
```

| | |
|---------------------------|---|
| Fichier à importer | |
| <nom du fichier> | Nom du fichier depuis lequel il faut importer les paramètres de l'application. Vous pouvez importer les paramètres de Kaspersky Endpoint Security depuis un fichier de configuration au format DAT ou CFG, un fichier au format TXT ou un document au format XML. |

| | |
|--|--|
| Autorisation | |
| <code>/login=<nom d'utilisateur></code> <code>/password=<mot de passe></code> | Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe . |

Exemple :

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Application du fichier clé

Appliquer un fichier clé pour activer Kaspersky Endpoint Security. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve.

Syntaxe de la commande

```
ADDKEY <nom du fichier> [/login=<nom d'utilisateur> /password=<mot de passe>]
```

| | |
|--------------------|---------------------------|
| Fichier clé | |
| <nom du fichier> | Nom du fichier de licence |

| | |
|---|---|
| Autorisation | |
| /login=<nom d'utilisateur> /password=<mot de passe> | Données du compte utilisateur Les données du compte utilisateur doivent être saisies uniquement si la Protection par mot de passe est activée . |

Exemple :

```
avp.com ADDKEY file.key
```

LICENSE. Licence

Exécuter les opérations liées aux clés de l'application Kaspersky Endpoint Security.

Pour pouvoir exécuter la commande de suppression de clé de licence, la [Protection par mot de passe](#) doit être activée. L'utilisateur doit posséder l'autorisation **Suppression de la clé**.

Syntaxe de la commande

```
LICENSE <opération> [/login=<nom d'utilisateur> /password=<mot de passe>]
```

| Opération | |
|--|--|
| /ADD <nom du fichier> | Appliquer un fichier clé pour activer Kaspersky Endpoint Security. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve. |
| /ADD <code d'activation> | Activer Kaspersky Endpoint Security à l'aide d'un code d'activation. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve. |
| /REFRESH <nom du fichier> | Renouveler la durée de validité de la licence à l'aide d'un fichier clé. Ceci a pour effet d'ajouter une clé de réserve. Elle est activée à l'expiration de la licence. Il est impossible d'ajouter une clé active à l'aide de cette commande. |
| /REFRESH <code d'activation> | Renouveler la durée de validité de la licence à l'aide d'un code d'activation. Ceci a pour effet d'ajouter une clé de réserve. Elle est activée à l'expiration de la licence. Il est impossible d'ajouter une clé active à l'aide de cette commande. |
| /DEL /login=<nom d'utilisateur> /password=<mot de passe> | Supprimer la clé de licence La clé de licence de réserve est également supprimée. |

| | |
|--|--|
| Autorisation | |
| <code>/login=<nom d'utilisateur> /password=<mot de passe></code> | Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe . |

Exemple :

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Achat d'une licence

Accéder au site de Kaspersky pour acheter une licence ou la renouveler.

PBATESTRESET. Réinitialiser les résultats de l'analyse avant le chiffrement du disque

Réinitialisez les résultats de l'analyse de la prise en charge du chiffrement du disque (FDE) à l'aide des technologies de Kaspersky Disk Encryption et BitLocker.

Avant de lancer le chiffrement du disque, l'application réalise une série de vérifications pour voir s'il est possible de chiffrer l'ordinateur. Si le chiffrement du disque est impossible, Kaspersky Endpoint Security enregistre les informations relatives à l'incompatibilité. Lors de la tentative de chiffrement suivante, l'application ne procède pas à la vérification mais signale que le chiffrement est impossible. Si la configuration matérielle a été modifiée, la vérification de la compatibilité du disque dur système avec la technologie Kaspersky Disk Encryption ou de la prise en charge de la technologie BitLocker doit être précédée de la suppression des informations sur les incompatibilités obtenues par l'application lors de la vérification précédente.

EXIT. Quitter l'application

Arrêter Kaspersky Endpoint Security. L'application est déchargée de la mémoire vive de l'ordinateur.

L'exécution de la commande requiert l'[activation de la Protection par mot de passe](#). L'utilisateur doit avoir l'autorisation **Quitter l'application**.

Syntaxe de la commande

```
EXIT /login=<nom d'utilisateur> /password=<mot de passe>
```

EXITPOLICY. Désactiver la stratégie

Désactive la stratégie de Kaspersky Security Center sur l'ordinateur. Tous les paramètres de Kaspersky Endpoint Security peuvent être configurés, même les paramètres accompagnés d'un cadenas dans la stratégie (🔒).

L'exécution de la commande requiert l'[activation de la Protection par mot de passe](#). L'utilisateur doit posséder l'autorisation **Désactivation de la stratégie de Kaspersky Security Center**.

Syntaxe de la commande

```
EXITPOLICY /login=<nom d'utilisateur> /password=<mot de passe>
```

STARTPOLICY. Activation de la stratégie

Activer la stratégie de Kaspersky Security Center sur l'ordinateur. Les paramètres de l'application sont alors configurés conformément à la stratégie.

DISABLE. Désactivation de la protection

Désactiver la Protection contre les fichiers malicieux sur un ordinateur doté d'une licence pour Kaspersky Endpoint Security expirée. Il est impossible d'exécuter la commande sur un ordinateur sur lequel l'application n'a pas été activée ou qui ne possède pas une licence active.

SPYWARE. Détection de logiciels espion

Activer/désactiver la détection de logiciels espion. La détection de logiciels espion est activée par défaut.

Syntaxe de la commande

```
SPYWARE on|off
```

MDRLICENSE. Activation MDR

Effectuez des opérations avec le fichier de configuration BLOB pour activer le module Managed Detection and Response. Le fichier BLOB contient l'identifiant du client ainsi que des informations à propos de la licence pour Kaspersky Managed Detection and Response. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR. Vous pouvez obtenir l'archive ZIP dans le module Kaspersky Managed Detection and Response Console. Pour en savoir plus à propos d'un fichier BLOB, *veuillez consulter le [guide d'aide de Kaspersky Managed Detection and Response](#)*.

Des privilèges d'administrateur sont requis pour utiliser un fichier BLOB. Les paramètres du module Managed Detection and Response dans la stratégie doivent également être modifiables (🔒).

Syntaxe de la commande

```
MDRLICENSE <opération> [/login=<nom d'utilisateur> /password=<mot de passe>]
```

| Opération | |
|--------------------------|--|
| /ADD <nom du fichier> | Appliquez le fichier de configuration BLOB pour assurer l'intégration avec Kaspersky Managed Detection and Response (format de fichier P7). Vous ne pouvez appliquer qu'un seul fichier BLOB. Si un fichier BLOB a déjà été ajouté à l'ordinateur, le fichier sera remplacé. |
| /DEL | Supprimez le fichier de configuration BLOB. |

| Autorisation | |
|--|--|
| /login=<nom d'utilisateur> /password=<mot de passe> | Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe . |

Exemple :

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

KSN. Transition Global/Private KSN

Sélection d'une solution Kaspersky Security Network pour déterminer la réputation de fichiers ou de sites Web. Kaspersky Endpoint Security prend en charge les infrastructures KSN suivantes :

- Le *KSN global* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky Security Network et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques de Kaspersky.
- Le *KSN privé* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Endpoint Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KSN privé a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :
 - absence de connexion des postes de travail locaux à Internet ;
 - interdiction législative ou restriction imposée par la sécurité de l'entreprise sur l'envoi de données hors du pays ou hors du réseau local de l'organisation.

Syntaxe de la commande

```
KSN /global | /private <nom du fichier>
```

| Fichier de configuration du KSN privé | |
|---------------------------------------|--|
| <nom du fichier> | Nom du fichier de configuration contenant les paramètres du serveur proxy KSN. |

Ce fichier présente l'extension PKCS7 ou PEM.

Exemple :

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

Commandes KESCLI

Les commandes KESCLI vous permettent de recevoir des informations à propos de l'état de la protection de l'ordinateur à l'aide du module OPSWAT, et d'effectuer des tâches standards, comme l'analyse des virus et la mise à jour des bases de données.

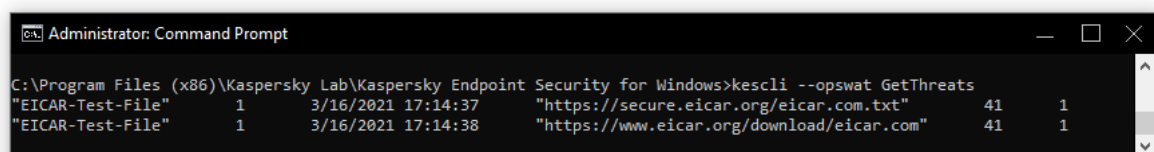
Vous pouvez consulter la liste des commandes KESCLI à l'aide de la commande `--help` ou en utilisant la commande abrégée `-h`.

Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.
3. Utilisez le modèle suivant pour exécuter la commande :

```
kescli <commande> [paramètres]
```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Administration de l'application via la ligne de commande

Analyse. Recherche de virus

Lancer la tâche de recherche de virus.

Syntaxe de la commande

```
--opswat Scan <zone d'analyse> <action en cas de détection d'une menace>
```

Vous pouvez vérifier l'état d'achèvement de la tâche *Analyse complète* à l'aide de la [commande `GetScanState`](#) et afficher la date et l'heure de la dernière analyse à l'aide de la [commande `GetLastScanTime`](#).

| Zone d'analyse | |
|-----------------------|--|
| <fichiers à analyser> | Liste de fichiers et de dossiers séparés par le symbole <code>;</code> . Par exemple, <code>C:\Program Files (x86)\Exemple de dossier</code> . |

| Action en cas de détection d'une menace | |
|---|---|
| 0 | Notifier. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives. |
| 1 | Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. Cette action est sélectionnée par défaut. |

Exemple :

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. État d'achèvement de l'analyse

Recevez des informations à propos de l'état d'achèvement de la tâche *Analyse complète* :

- 1 : l'analyse est en cours.
- 0 : l'analyse n'est pas en cours.

Syntaxe de la commande

```
--opswat GetScanState
```

Exemple :

```
kescli --opswat GetScanState
```

GetLastScanTime. Calcul du temps requis pour l'analyse

Recevez des informations à propos de la date et de l'heure d'achèvement de la dernière tâche *Analyse complète*.

Syntaxe de la commande

```
--opswat GetLastScanTime
```

Exemple :

```
kescli --opswat GetLastScanTime
```

GetThreats. Collecte de données à propos des menaces détectées

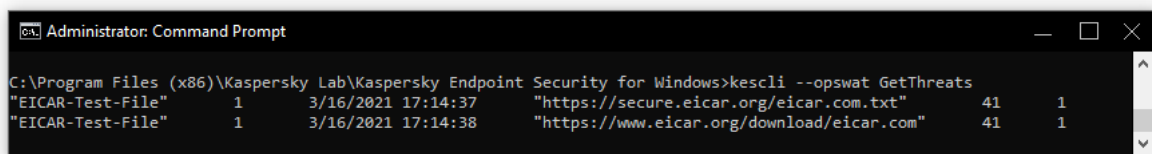
Recevez une liste des menaces détectées (*rapport sur les menaces*). Ce rapport contient des informations à propos des menaces et de l'activité des virus au cours des 30 derniers jours précédant la création du rapport.

Syntaxe de la commande

```
--opswat GetThreats
```

Lorsque cette commande est exécutée, Kaspersky Endpoint Security envoie une réponse au format suivant :

```
<nom de l'objet détecté> <type d'objet> <date et heure de détection> <chemin d'accès au  
fichier> <action en cas de détection d'une menace> <niveau de danger de la menace>
```



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Administration de l'application via la ligne de commande

| Type d'objet | |
|--------------|---|
| 0 | Inconnu (Inconnu). |
| 1 | Virus (Virware). |
| 2 | Chevaux de Troie (Trojware). |
| 3 | Programmes malveillants (Programme malveillant). |
| 4 | Programmes publicitaires (Programme publicitaire). |
| 5 | Numéroteurs automatiques (Programme pornographique). |
| 6 | Applications qui pourraient être utilisées par un cybercriminel pour nuire à l'ordinateur ou aux données de l'utilisateur (Programme à risque). |
| 7 | Objets compressés dont la méthode d'emballage peut être utilisée pour protéger du code malveillant (Compressé) |
| 20 | Objets inconnus (Xfiles). |
| 21 | Applications connues (Logiciel). |
| 22 | Fichiers cachés (Masqué). |
| 23 | Application nécessitant une attention particulière (Pupware). |
| | |

| | |
|-----|--|
| 24 | Comportement anormal (Anomalie). |
| 30 | Non déterminé (Non détecté). |
| 40 | Bannières publicitaires (Bannière). |
| 50 | Attaque réseau (Attaque). |
| 51 | Accès au registre (Registre). |
| 52 | Activité suspecte (Soupçon). |
| 60 | Vulnérabilités (Vulnérabilité). |
| 70 | Phishing. |
| 80 | Pièce jointe indésirable (Pièce jointe). |
| 90 | Programme malveillant détecté par Kaspersky Security Network (Urgent). |
| 100 | Lien inconnu (URL suspecte). |
| 110 | Autre programme malveillant (Comportemental). |

| Action en cas de détection d'une menace | |
|---|---|
| 0 | Inconnu (inconnu). |
| 1 | La menace a été éliminée (ok). |
| 2 | L'objet a été infecté et n'a pas été désinfecté (infecté). |
| 5 | L'objet se trouve dans une archive et n'a pas été désinfecté (archive). |
| 9 | L'objet a été désinfecté (désinfecté). |
| 10 | L'objet n'a pas été désinfecté (non désinfecté). |
| 11 | L'objet a été supprimé (supprimé). |
| 13 | Une copie de sauvegarde de l'objet a été créée (sauvegardé). |
| 15 | L'objet a été déplacé vers la Sauvegarde (quarantaine). |
| 23 | L'objet a été supprimé au redémarrage de l'ordinateur (supprimé au redémarrage). |
| 25 | L'objet a été désinfecté au redémarrage de l'ordinateur (désinfecté au redémarrage). |
| 29 | L'objet a été déplacé vers la Sauvegarde par un utilisateur (ajouté par l'utilisateur). |
| 30 | L'objet a été ajouté aux exclusions (ajouté aux exclusions). |
| 31 | L'objet a été déplacé vers la Sauvegarde au redémarrage de l'ordinateur (quarantaine au redémarrage). |
| 36 | Faux positif (fausse alerte). |
| 38 | Le processus a été interrompu (interrompu). |
| 40 | L'objet n'a pas été détecté (non trouvé). |
| 41 | Impossible de traiter la menace (non traitable). |
| 42 | L'objet a été restauré (restauré). |

| | |
|------------|--|
| 43 | L'objet a été créé à la suite d'une menace (créé par une menace). |
| 44 | L'objet a été restauré au redémarrage de l'ordinateur (restauré au redémarrage). |
| 0xffffffff | L'objet n'a pas été traité (abandonné). |

| Niveau de danger de la menace | |
|-------------------------------|---|
| 0 | Inconnu |
| 1 | Élevé |
| 2 | Analyse standard |
| 4 | Faible |
| 8 | Informations (inférieur à <i>Faible</i>) |

UpdateDefinitions. Mise à jour des bases de données et des modules de l'application

Lancer la tâche *Mise à jour*. Kaspersky Endpoint Security utilise la source par défaut : les serveurs de mises à jour de Kaspersky.

Syntaxe de la commande

```
--opswat UpdateDefinitions
```

Vous pouvez afficher la date et l'heure de la dernière tâche *Mise à jour* terminée à l'aide de la [commande GetDefinitionsetState](#).

Exemple :

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Calcul du temps requis pour la mise à jour

Recevez des informations à propos de la date et de l'heure d'achèvement de la dernière tâche *Mise à jour*.

Syntaxe de la commande

```
--opswat GetDefinitionState
```

Exemple :

```
kescli --opswat GetDefinitionState
```

EnableRTP. Activation de la protection

Sur l'ordinateur, activez les modules de protection de Kaspersky Endpoint Security : Protection contre les fichiers malicieux, Protection contre les menaces Internet, Protection contre les menaces par emails, Protection contre les menaces réseau et Prévention des intrusions.

Syntaxe de la commande

```
--opswat EnableRTP
```

Vous pouvez vérifier l'état de fonctionnement de la Protection contre les fichiers malicieux à l'aide de la [commande GetRealTimeProtectionState](#).

Exemple :

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. États de la Protection contre les fichiers malicieux

Recevez des informations à propos de l'état de fonctionnement du module Protection contre les fichiers malicieux :

- 1 : le module est activé.
- 0 : le module est désactivé.

Syntaxe de la commande

```
--opswat GetRealTimeProtectionState
```

Exemple :

```
kescli --opswat GetRealTimeProtectionState
```

Version. Identification de la version de l'application

Identifiez la version de Kaspersky Endpoint Security for Windows.

Syntaxe de la commande

```
--Version
```

Vous pouvez également utiliser la commande abrégée `-v`.

Exemple :

```
kescli -v
```

Codes d'erreur

Des erreurs peuvent survenir lors de l'utilisation de l'application via la ligne de commande. Dans ce cas, Kaspersky Endpoint Security affiche un message d'erreur, par exemple, Erreur : impossible de lancer la tâche 'EntAppControl'. Kaspersky Endpoint Security peut également afficher des informations supplémentaires sous la forme d'un code, par exemple, erreur = 8947906D (cf. tableau ci-dessous).

Codes d'erreur

| Code d'erreur | Description |
|---------------|--|
| 09479001 | Clé de licence de Kaspersky Endpoint Security est déjà utilisée sur cet ordinateur. |
| 0947901D | La durée de validité de la licence est écoulée. Mise à jour des bases de l'application inaccessible. |
| 89479002 | Clé introuvable. |
| 89479003 | Signature numérique endommagée ou introuvable. |
| 89479004 | Données corrompues. |
| 89479005 | Fichier clé corrompu. |
| 89479006 | La licence a expiré ou la clé de licence n'est plus valide. |
| 89479007 | Le fichier clé n'est pas indiqué. |
| 89479008 | Application du fichier clé impossible. |
| 89479009 | Impossible d'enregistrer les données. |
| 8947900A | Erreur de lecture des données. |
| 8947900B | Erreur d'entrée/de sortie. |
| 8947900C | Bases introuvables. |
| 8947900E | La bibliothèque de licence n'est pas chargée. |
| 8947900F | Les bases sont corrompues ou ont été mises à jour manuellement. |
| 89479010 | Bases corrompues. |
| 89479011 | Impossible d'appliquer un fichier clé non valide pour ajouter une clé complémentaire. |
| 89479012 | Erreur système. |
| 89479013 | Liste de refus des clés corrompue. |
| 89479014 | La signature numérique du fichier ne correspond pas à la signature numérique de Kaspersky. |
| 89479015 | Impossible d'utiliser une clé de licence non commerciale comme clé de licence commerciale. |
| 89479016 | Pour utiliser la version bêta de l'application, il faut une licence pour test bêta. |
| 89479017 | Le fichier clé n'est pas prévu pour cette application. |
| 89479018 | La clé a été bloquée par Kaspersky. |
| 89479019 | L'application a déjà été utilisée sous une licence d'évaluation. Impossible d'ajouter à nouveau la clé pour la licence d'évaluation. |
| 8947901A | Fichier clé corrompu. |
| 8947901B | La signature numérique est introuvable, corrompue ou ne correspond pas à celle de Kaspersky. |
| 8947901C | Impossible d'ajouter la clé si la licence commerciale lui correspondant a expiré. |
| 8947901E | La date de création ou d'application du fichier clé est incorrecte. Vérifiez la date système. |

| | |
|----------|---|
| 8947901F | Impossible d'ajouter une clé pour une licence d'évaluation si une autre licence similaire est toujours active. |
| 89479020 | Liste de refus des clés corrompue ou introuvable. |
| 89479021 | La description des mises à jour est corrompue ou introuvable. |
| 89479022 | Erreur dans les données de service de la clé de licence. |
| 89479023 | Impossible d'appliquer un fichier clé non valide pour ajouter une clé complémentaire. |
| 89479025 | Erreur lors de l'envoi de la requête au Serveur d'activation. Raisons possibles : erreur de connexion Internet ou problèmes temporaires sur le Serveur d'activation. Essayez d'activer l'application à l'aide du code d'activation plus tard. Si l'erreur se reproduit, contactez votre fournisseur d'accès Internet. |
| 89479026 | Erreur dans la réponse du Serveur d'activation. |
| 89479027 | Impossible d'obtenir l'état de l'objet. |
| 89479028 | Erreur d'enregistrement du fichier temporaire. |
| 89479029 | Le code d'activation n'a pas été saisi correctement ou la date de votre ordinateur est incorrecte. Vérifiez la date système de l'ordinateur. |
| 8947902A | Le fichier clé ne convient pas à cette application ou la licence a expiré. Impossible d'activer Kaspersky Endpoint Security à l'aide d'un fichier clé prévu pour une autre application. |
| 8947902B | Échec de l'obtention du fichier clé. Code d'activation saisi incorrect. |
| 8947902C | Le serveur d'activation a renvoyé l'erreur 400. |
| 8947902D | Le serveur d'activation a renvoyé l'erreur 401. |
| 8947902E | Le serveur d'activation a renvoyé l'erreur 403. |
| 8947902F | Le serveur d'activation a renvoyé l'erreur 404. |
| 89479030 | Le serveur d'activation a renvoyé l'erreur 405. |
| 89479031 | Le serveur d'activation a renvoyé l'erreur 406. |
| 89479032 | Authentification requise sur le serveur proxy. Vérifiez les paramètres du réseau. |
| 89479033 | Délai d'attente de la requête expiré. |
| 89479034 | Le serveur d'activation a renvoyé l'erreur 409. |
| 89479035 | Le serveur d'activation a renvoyé l'erreur 410. |
| 89479036 | Le serveur d'activation a renvoyé l'erreur 411. |
| 89479037 | Le serveur d'activation a renvoyé l'erreur 412. |
| 89479038 | Le serveur d'activation a renvoyé l'erreur 413. |
| 89479039 | Le serveur d'activation a renvoyé l'erreur 414. |
| 8947903A | Le serveur d'activation a renvoyé l'erreur 415. |
| 8947903C | Erreur interne du serveur. |
| 8947903D | La fonction n'est pas prise en charge. |
| 8947903E | Réponse non valide de la passerelle. Vérifiez les paramètres du réseau. |
| 8947903F | Service non disponible (erreur HTTP 503). |
| 89479040 | Le délai d'attente de la réponse de la passerelle a expiré. Vérifiez les paramètres du réseau. |

| | |
|----------|---|
| 89479041 | Le serveur ne prend pas ce rapport en charge. |
| 89479043 | Erreur HTTP inconnue. |
| 89479044 | Identificateur de ressource incorrecte. |
| 89479046 | Adresse (URL) incorrecte. |
| 89479047 | Dossier cible incorrect. |
| 89479048 | Erreur de répartition de la mémoire. |
| 89479049 | Erreur de conversion des paramètres en ligne ANSI (url, folder, agent). |
| 8947904A | Erreur de création du flux de travail. |
| 8947904B | Le flux de travail a déjà été lancé. |
| 8947904C | Le flux de travail n'est pas lancé. |
| 8947904D | Fichier clé introuvable sur le serveur d'activation. |
| 8947904E | La clé est bloquée. |
| 8947904F | Erreur interne du serveur d'activation. |
| 89479050 | La requête d'activation ne contient pas assez de données. |
| 89479053 | La clé de licence a expiré. |
| 89479054 | La date système de l'ordinateur n'est pas correcte. |
| 89479055 | La licence d'évaluation a expiré. |
| 89479056 | La durée de validité de la licence est écoulée. |
| 89479057 | Le nombre d'activations autorisées de l'application à l'aide du code indiqué est dépassé. |
| 89479058 | La procédure d'activation s'est soldée par une erreur. |
| 89479059 | Impossible d'utiliser une clé de licence non commerciale comme clé de licence commerciale. |
| 8947905C | Code d'activation requis. |
| 89479062 | Impossible de se connecter au serveur d'activation. |
| 89479064 | Le serveur d'activation n'est pas disponible. Vérifiez les paramètres de connexion Internet et essayez d'activer à nouveau l'application. |
| 89479065 | La date d'émission des bases de l'application est ultérieure à la date de fin de validité de la licence. |
| 89479066 | Impossible de remplacer la clé active par une clé de licence expirée. |
| 89479067 | Impossible d'ajouter une clé de licence de réserve si sa durée de validité expire avant celle de la licence active. |
| 89479068 | Clé mise à jour pour abonnement manquante. |
| 8947906A | Code d'activation non valide (la somme de contrôle ne correspond pas). |
| 8947906B | La clé est déjà active. |
| 8947906C | Les types de licence qui correspondent aux clés active et de licence de réserve ne correspondent pas. |
| 8947906D | La licence ne prend pas en charge le fonctionnement du module. |
| 8947906E | Impossible d'ajouter une clé par abonnement en tant que clé de licence de réserve. |

| | |
|----------|---|
| 89479213 | Erreur générale du niveau de transport. |
| 89479214 | Impossible de se connecter au serveur d'activation. |
| 89479215 | Format de l'adresse Internet incorrect. |
| 89479216 | Impossible de transformer l'adresse du serveur proxy. |
| 89479217 | Impossible de transformer l'adresse du serveur. Vérifiez les paramètres de connexion Internet. |
| 89479218 | Impossible de contacter le Serveur d'activation ou le serveur proxy. |
| 89479219 | Déni d'accès à distance. |
| 8947921A | Le délai d'attente de la réponse a expiré. |
| 8947921B | Erreur d'envoi de la demande HTTP. |
| 8947921C | Erreur de connexion SSL. |
| 8947921D | L'opération a été interrompue suite à l'appel inverse. |
| 8947921E | Trop de redirections. |
| 8947921F | La vérification du destinataire s'est soldée sur une erreur. |
| 89479220 | Réponse vide du serveur d'activation. |
| 89479221 | Erreur d'envoi des données. |
| 89479222 | Erreur de réception des données. |
| 89479223 | Erreur de certificat SSL local. |
| 89479224 | Erreur de chiffrement SSL. |
| 89479225 | Erreur de certificat SSL du serveur. |
| 89479226 | Contenu du paquet réseau incorrect. |
| 89479227 | Accès refusé pour l'utilisateur. |
| 89479228 | Fichier de certificat SSL incorrect. |
| 89479229 | Impossible d'établir une connexion SSL. |
| 8947922A | Échec de l'envoi ou de la réception du paquet réseau. Réessayez plus tard. |
| 8947922B | Fichier des certificats rappelés incorrect. |
| 8947922C | Erreur de demande du certificat SSL. |
| 89479401 | Erreur inconnue du serveur. |
| 89479402 | Erreur interne du serveur. |
| 89479403 | La clé de licence pour le code d'activation saisi est absente. |
| 89479404 | La clé active est bloquée. |
| 89479405 | Les paramètres obligatoires de la demande d'activation de l'application sont absents. |
| 89479406 | Nom d'utilisateur ou mot de passe incorrects. |
| 89479407 | Un code d'activation incorrect a été envoyé au serveur. |
| 89479408 | Le code d'activation ne convient pas à Kaspersky Endpoint Security. Impossible d'activer Kaspersky Endpoint Security à l'aide d'un fichier clé prévu pour une application inconnue. |
| 89479409 | Le code d'activation ne figure pas dans la requête. |

| | |
|----------|--|
| 8947940B | La licence a expiré (selon les données du Serveur d'activation). |
| 8947940C | Le nombre d'activations de l'application à l'aide de ce code d'activation est dépassé. |
| 8947940D | Format de l'identificateur de la demande incorrect. |
| 8947940E | Le code d'activation ne convient pas à Kaspersky Endpoint Security. Code d'activation prévu pour une autre application de Kaspersky. |
| 8947940F | Impossible de mettre à jour la clé de licence. |
| 89479410 | Le code d'activation ne correspond pas à cette région. |
| 89479411 | Le code d'activation ne correspond pas à la version linguistique de Kaspersky Endpoint Security. |
| 89479412 | Interrogation complémentaire du Serveur d'activation requise. |
| 89479413 | Le serveur d'activation a renvoyé l'erreur 643. |
| 89479414 | Le serveur d'activation a renvoyé l'erreur 644. |
| 89479415 | Le serveur d'activation a renvoyé l'erreur 645. |
| 89479416 | Le serveur d'activation a renvoyé l'erreur 646. |
| 89479417 | Le format du code d'activation n'est pas pris en charge par le Serveur d'activation. |
| 89479418 | Format du code d'activation incorrect. |
| 89479419 | L'heure système de l'ordinateur est incorrecte. |
| 8947941A | Le code d'activation ne convient pas à la version de Kaspersky Endpoint Security. |
| 8947941B | L'abonnement a expiré. |
| 8947941C | Le seuil du nombre d'activations est dépassé pour cette clé de licence. |
| 8947941D | Signature numérique de la clé de licence non valide. |
| 8947941E | Les données complémentaires de l'utilisateur sont requises. |
| 8947941F | La vérification des données de l'utilisateur s'est soldée sur une erreur. |
| 89479420 | L'abonnement n'est pas actif. |
| 89479421 | Maintenance en cours sur le serveur d'activation. |
| 89479501 | Erreur inconnue du côté de Kaspersky Endpoint Security. |
| 89479502 | Un paramètre inadmissible a été transmis (par exemple, la liste des adresses des serveurs d'activation est vide). |
| 89479503 | Code d'activation incorrect. |
| 89479504 | Nom d'utilisateur incorrect. |
| 89479505 | Le mot de passe de l'utilisateur est incorrect. |
| 89479506 | Le serveur d'activation a renvoyé une réponse incorrecte. |
| 89479507 | Demande d'activation interrompue. |
| 89479509 | Le serveur d'activation a renvoyé une liste de transfert d'adresse vide. |

Application. Profils d'application

Un *profil* désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Les profils sont prévus pour administrer l'application via la ligne de commande. Vous pouvez utiliser des profils pour exécuter les commandes `SART`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` et `IMPORT`. Les profils permettent de configurer les paramètres de l'application (par exemple, `STOP DeviceControl`) ou de lancer une tâche (par exemple `START Scan_My_Computer`).

Les profils suivants sont disponibles :

- `AdaptiveAnomaliesControl` : contrôle évolutif des anomalies.
- `AMSI` : Protection AMSI.
- `BehaviorDetection` : Détection comportementale.
- `DeviceControl` : Contrôle des appareils.
- `EntAppControl` : Contrôle des applications.
- `File_Monitoring` ou `FM` : protection contre les fichiers malicieux.
- `Firewall` ou `FW` : Pare-feu.
- `HIPS` : Prévention des intrusions.
- `IDS` : Protection contre les menaces réseau.
- `IntegrityCheck` : Vérification de l'intégrité.
- `Mail_Monitoring` ou `EM` : Protection contre les menaces par emails.
- `Rollback` : Restauration de la mise à jour.
- `Scan_ContextScan` : Analyse depuis le menu contextuel.
- `Scan_IdleScan` : Analyse en arrière-plan.
- `Scan_Memory` : Analyse de la mémoire du noyau.
- `Scan_My_Computer` : Analyse complète.
- `Scan_Objects` : Analyse personnalisée.
- `Scan_Qscan` : Analyse des objets chargés au lancement du système d'exploitation.
- `Scan_Removable_Drive` : Analyse des disques amovibles.
- `Scan_Startup` ou `STARTUP` : Analyse des zones critiques.
- `Updater` : Mise à jour.
- `Web_Monitoring` ou `WM` : Protection contre les menaces Internet.
- `WebControl` : Contrôle Internet.

Kaspersky Endpoint Security prend également en charge l'utilisation de profils de service. Les profils de service peuvent être utiles lors de l'interaction avec le Support Technique de Kaspersky.

Administration de l'application via l'API REST

Kaspersky Endpoint Security vous permet de configurer les paramètres de l'application, de lancer l'analyse, de mettre à jour les bases antivirus et d'effectuer d'autres tâches à l'aide de solutions tierces. Pour cela, Kaspersky Endpoint Security propose une API. L'API REST de Kaspersky Endpoint Security fonctionne selon le protocole HTTP et consiste en un ensemble de méthodes "requête/réponse". En d'autres termes, vous pouvez gérer Kaspersky Endpoint Security via une solution tierce et non pas via l'interface locale de l'application ou la Console d'administration de Kaspersky Security Center.

Pour commencer à utiliser l'API REST, vous devez [installer Kaspersky Endpoint Security avec prise en charge de l'API REST](#). Le client REST et Kaspersky Endpoint Security doivent être installés sur le même ordinateur.

Pour assurer une interaction sûre entre Kaspersky Endpoint Security et le client REST, procédez comme suit :

- Configurez la protection du client REST contre les accès non autorisés selon les recommandations du développeur du client REST. Configurez la protection du dossier client REST contre l'écriture à l'aide de la liste de contrôle d'accès discrétionnaire - DACL.
- Pour exécuter le client REST, utilisez un compte distinct avec des droits d'administrateur. Refuser la connexion interactive au système pour ce compte.

L'administration de l'application via l'API REST s'opère à l'adresse <http://127.0.0.1> ou <http://localhost>. Il n'est pas possible de réaliser l'administration à distance de Kaspersky Endpoint Security via l'API REST.



[OUVRIR LA DOCUMENTATION SUR L'API REST](#) 

Installation d'une application avec API REST

Pour pouvoir administrer une application via l'API REST, il faut installer Kaspersky Endpoint Security avec prise en charge de l'API REST. Si vous administrez Kaspersky Endpoint Security via l'API REST, il ne sera pas possible d'administrer l'application via Kaspersky Security Center.

Pour installer Kaspersky Endpoint Security avec prise en charge de l'API REST, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier qui renferme le paquet de distribution de Kaspersky Endpoint Security version 11.2.0 ou suivantes.
3. Installez Kaspersky Endpoint Security avec les paramètres suivants :

- RESTAPI=1
- RESTAPI_User=<Nom d'utilisateur>

Nom d'utilisateur pour l'administration de l'application via l'API REST. Saisissez un nom d'utilisateur au format <DOMAIN>\<UserName> (par exemple, RESTAPI_User=COMPANY\Administrator). Vous pouvez administrer l'application via l'API REST uniquement sous ce compte utilisateur. Vous ne pouvez sélectionner qu'un seul utilisateur pour utiliser l'API REST.

- RESTAPI_Port=<Port>

Port pour l'échange de données. Paramètre facultatif. Le port 6782 est sélectionné par défaut.

- AdminKitConnector=1

Administration de l'application à l'aide du système d'administration. L'administration est autorisée par défaut.

Vous pouvez également définir les paramètres d'utilisation de l'API REST à l'aide du [fichier setup.ini](#).

Vous pouvez définir les paramètres d'utilisation de l'API REST uniquement lors de l'installation de l'application. La modification des paramètres après l'installation de l'application est impossible. Si vous souhaitez modifier les paramètres, supprimez Kaspersky Endpoint Security, puis installez-le à nouveau avec les nouveaux paramètres d'utilisation de l'API REST.

Exemple :

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

Vous pourrez ainsi administrer l'application via l'API REST. Pour vérifier le fonctionnement, ouvrez la documentation de l'API REST à l'aide d'une requête GET.

Exemple :

```
GET http://localhost:6782/kes/v1/api-docs
```

Utilisation de l'API

Il n'est pas possible de limiter l'accès à l'application via l'API REST à l'aide de la [protection par mot de passe](#). Par exemple, il n'est pas possible d'interdire l'utilisation de l'API REST pour désactiver la protection. Vous pouvez configurer la protection par mot de passe via l'API REST et limiter l'accès des utilisateurs à l'application via l'interface locale.

Pour administrer l'application via l'API REST, vous devez exécuter le client REST sous le compte que vous avez indiqué lors de l'[installation du programme avec la prise en charge de l'API REST](#). Vous ne pouvez sélectionner qu'un seul utilisateur pour utiliser l'API REST.



[OUVRIR LA DOCUMENTATION SUR L'API REST](#)

L'administration de l'application via l'API REST comprend les étapes suivantes :

1. Récupérez les valeurs actuelles des paramètres de l'application. Pour ce faire, envoyez une requête GET.

Exemple :

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. L'application enverra la structure et les valeurs des paramètres en guise de réponse. Kaspersky Endpoint Security prend en charge les formats XML et JSON.

Exemple :

```
{  
  "action": 0,  
  "enableSystemProcessesMemoryProtection": true,  
  "enabled": true  
}
```

3. Modifiez les paramètres de l'application. Pour ce faire, envoyez une requête POST. Utilisez la structure de paramètres obtenue en réponse à la requête GET.

Exemple :

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. L'application modifiera les paramètres et enverra une réponse contenant les résultats de la configuration de l'application.

Sources d'informations sur l'application

Page de Kaspersky Endpoint Security sur le site Internet de Kaspersky

La [page de Kaspersky Endpoint Security](#) fournit des informations générales sur l'application, ses possibilités et ses particularités de fonctionnement.

La page de Kaspersky Endpoint Security propose un lien vers la boutique en ligne. Vous pourrez y acheter l'application ou prolonger vos droits d'utilisation.

Page de Kaspersky Endpoint Security dans la Base des connaissances

La *base de connaissances* est une rubrique du site du Support technique.

La [page de Kaspersky Endpoint Security dans la base de connaissances](#) propose des articles reprenant des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la base de connaissances peuvent répondre à des questions concernant non seulement Kaspersky Endpoint Security, mais également d'autres applications de Kaspersky. Ces articles peuvent également contenir des actualités du Support technique.

Discussion sur les applications de Kaspersky entre les membres de la communauté d'utilisateurs.

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky et aux autres utilisateurs de nos applications dans notre [communauté](#).

Dans la communauté, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

Contacter le Support Technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans d'autres [sources d'informations relatives à Kaspersky Endpoint Security](#), contactez le Support technique. Les experts du Support technique répondront à vos questions sur l'installation et l'utilisation de Kaspersky Endpoint Security.

Kaspersky fournit une assistance pour Kaspersky Endpoint Security pendant son cycle de vie (consultez la [page relative au cycle de vie de l'application](#)). Avant de contacter le Support Technique, veuillez prendre connaissance des [règles d'octroi de l'assistance technique](#).

Vous pouvez contacter les experts du Support technique d'une des manières suivantes :

- En [visitant le site Internet du Support Technique](#)
- Envoyer une demande au Support Technique de Kaspersky via le [portail Kaspersky CompanyAccount](#)

Une fois que les experts du Support Technique de Kaspersky sont au courant du problème survenu, ils peuvent vous demander de créer un *fichier de traçage*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

De plus, les experts du Support Technique peuvent avoir besoin d'informations complémentaires sur le système d'exploitation, les processus lancés sur l'ordinateur, ainsi que des rapports détaillés sur le fonctionnement des modules de l'application.

Lorsque les opérateurs du Support Technique cherchent à poser un diagnostic, ils peuvent vous demander de modifier certains paramètres de l'application :

- Activer la fonctionnalité de récupération des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules séparés de l'application, qui n'est pas disponibles via les outils standards de l'interface d'utilisateur.
- Modifier les paramètres de conservation des informations diagnostiques récupérées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Toutes les informations nécessaires pour exécuter les actions citées (la description de la suite des étapes, les paramètres modifiables, les fichiers de configuration, les scripts, les possibilités complémentaires de la ligne de commande, les modules de réparation, les utilitaires spécialisés, etc.), ainsi que la composition des données récupérées à des fins de débogage vous sont transmises par les experts du Support Technique. Les informations diagnostiques élargies récupérées sont enregistrées sur l'ordinateur de l'utilisateur. L'envoi automatique des données récupérées à Kaspersky n'est pas exécuté.

Les actions citées ci-dessus doivent être exécutées uniquement sous l'administration des experts du Support Technique à l'aide des instructions reçues. La modification indépendante des paramètres d'utilisation de l'application via les moyens, non décrits dans le Manuel de l'administrateur ou dans les recommandations des experts du Support Technique, peut amener au ralentissement et aux échecs dans le système d'exploitation, à la baisse du niveau de sécurité et à la perturbation de l'accessibilité et de l'intégrité des informations traitées.

À propos de la composition et de la conservation des fichiers de traçage

Vous seul êtes responsable de la sécurité des informations récupérées, et plus exactement du contrôle et de la restriction de l'accès aux informations récupérées et conservées sur l'ordinateur avant leur envoi à Kaspersky.

Les fichiers de traçage sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application.

Les fichiers de traçage, à l'exception des fichiers de traçage de l'Agent d'authentification, sont stockés dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces.

Les fichiers de traçage portent le nom : KES<numéro de version du service_dateXX.XX_timeXX.XX_pidXXX.><type de fichier de traçage>.log.

Vous pouvez consulter les données consignées dans les fichiers de traçage.

Tous les fichiers de traçage contiennent les données communes suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.

Ces informations ne contiennent pas le fichier de traçage de l'Agent d'authentification.

- Module de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (information, avertissement, critique, erreur).
- Description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande.

Kaspersky Endpoint Security enregistre les mots de passe de l'utilisateur dans le fichier de traçage uniquement sous forme chiffrée.

Contenu des fichiers de traçage SRV.log, GUI.log et ALL.log

Les fichiers de traçage SRV.log, GUI.log et ALL.log peuvent contenir, outre les informations générales, les informations suivantes :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur l'ordinateur local.
- Données sur le matériel installé sur l'ordinateur (par exemple, données de micrologiciel BIOS/UEFI). Ces données sont écrites dans le fichier de traçage lors du chiffrement du disque à l'aide de Kaspersky Disk Encryption.
- Nom d'utilisateur et mot de passe s'ils sont transmis en clair. Ces données peuvent être consignées dans les fichiers de traçage lors de l'analyse du trafic Internet.
- Nom d'utilisateur et mot de passe s'ils figurent dans les en-têtes du protocole HTTP.
- Nom du compte utilisateur d'accès à Microsoft Windows, si celui-ci fait partie du nom du fichier.

- Votre adresse de messagerie électronique ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.
- Les sites Internet que vous visitez ainsi que les liens de ces sites. Ces données sont consignées dans les fichiers de traçage lorsque l'application analyse les sites Internet.
- Adresse du serveur proxy, nom de l'ordinateur, adresse IP, nom de l'utilisateur employé pour l'autorisation sur le serveur Proxy. Ces données sont consignées dans les fichiers de traçage si l'application utilise un serveur proxy.
- Adresses IP externes d'où la connexion avec votre ordinateur a été établie.
- Objet du message, identifiant, nom de l'expéditeur et adresse de la page Internet de l'expéditeur du message dans le réseau social. Ces données sont consignées dans les fichiers de traçage si le module Contrôle Internet est activé.
- Données de trafic réseau. Ces données sont écrites dans les fichiers de traçage si des modules de surveillance du trafic (par exemple, Contrôle Internet) sont activés.
- Données reçues des serveurs de Kaspersky (par exemple, la version des bases antivirus).
- Statuts des composants de Kaspersky Endpoint Security et informations sur leur fonctionnement.
- Données sur les actions des utilisateurs dans l'application.
- Événements du système d'exploitation.

Contenu des fichiers de traçage HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Le fichier de traçage HST .log contient, outre les données générales, les informations relatives à l'exécution de la tâche de mise à jour des bases de données de l'application et des modules.

Le fichier de traçage BL .log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement de l'application, ainsi que les données indispensables à la résolution des problèmes de fonctionnement de l'application. Ce fichier est créé si l'application est lancée avec le paramètre `avp.exe -bl`.

Le fichier de traçage Dumpwriter .log contient, outre les données générales, les informations de service indispensables à la résolution des problèmes survenus pendant l'écriture du fichier dump de l'application.

Le fichier de traçage WD .log contient, outre les données générales, les informations sur les événements survenus pendant le fonctionnement du service avpsus, y compris les événements de mise à jour des modules de l'application.

Le fichier de traçage AVPCon .dll .log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu des fichiers de traçage des performances

Les fichiers de traçage des performances utilisent la nomenclature suivante : `KES<numéro de version_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Outre des données générales, les fichiers de traçage des performances contiennent des informations sur la charge du processeur, sur l'heure de démarrage du système d'exploitation et des applications, ainsi que sur les processus en cours d'exécution.

Contenu du fichier de traçage du module de la protection AMSI

Outre les données générales, le fichier de traçage AMSI.log contient des informations sur les résultats des analyses sollicitées par des applications tierces.

Contenu du fichier de traçage du module Protection contre les menaces par emails

Le fichier de traçage mcou.OUTLOOK.EXE.log peut contenir une partie des messages, y compris les adresses email.

Contenu du fichier de traçage du module Analyse depuis le menu contextuel

Le fichier de traçage shelllex.dll.log contient, outre les données générales, des informations sur l'exécution de la tâche d'analyse et les données nécessaires à l'élimination des incidents dans le fonctionnement de l'application.

Contenu des fichiers de traçage des plug-ins Internet de l'application

Les fichiers de traçage du plug-in Internet de l'application sont conservés sur l'ordinateur doté de Kaspersky Security Center 12 Web Console, dans le dossier Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Les fichiers de traçage du plug-in Internet de l'application sont nommés de la manière suivante : logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log. Web Console commence à enregistrer les données après l'installation et supprime les fichiers de traçage après sa suppression.

Les fichiers de traçage des plug-ins Internet de l'application contiennent, outre les données générales, les informations suivantes :

- le mot de passe de l'utilisateur KLAdmin pour le déverrouillage de l'interface Kaspersky Endpoint Security ([Protection par mot de passe](#)) ;
- le mot de passe temporaire pour le déverrouillage de l'interface de Kaspersky Endpoint Security ([Protection par mot de passe](#)) ;
- le nom d'utilisateur et le mot de passe pour le serveur de messagerie SMTP ([Notifications par e-mail](#)) ;
- le nom d'utilisateur et le mot de passe pour le serveur proxy du réseau Internet ([Serveur proxy](#)) ;
- le nom d'utilisateur et le mot de passe pour la [tâche Modification de la sélection des modules de l'application](#) ;
- les identifiants et les chemins indiqués dans les propriétés de la stratégie et les tâches de Kaspersky Endpoint Security.

Contenu du fichier de traçage de l'agent d'Authentification

Le fichier de traçage de l'Agent d'authentification est conservé dans le dossier System Volume Information et porte le nom KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin.


Le fichier de traçage de l'agent d'Authentification contient, outre les données générales, les informations sur le fonctionnement de l'Agent d'authentification et sur les actions exécutées par l'utilisateur dans l'Agent d'authentification.

Trace de l'application

La *trace de l'application* désigne l'enregistrement détaillé des activités de l'application et des messages sur les événements survenus pendant le fonctionnement de l'application.

Lancez le traçage de l'application conformément aux instructions du Support Technique de Kaspersky.

Pour créer un fichier de traçage de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .
La fenêtre **Assistance** s'ouvre.
2. Dans la fenêtre **Assistance**, cliquez sur le bouton **Outils de support**.
3. Utilisez le bouton **Activer les traces d'application** pour activer ou désactiver le traçage du fonctionnement de l'application.
4. Dans la liste déroulante **Traçages**, sélectionnez un mode de traçage de l'application :
 - **Avec rotation**. Enregistrer les résultats du traçage dans un nombre limité de fichiers de taille limitée et écraser les anciens fichiers quand la limite est atteinte. Si ce mode est sélectionné, vous pouvez définir le nombre maximum de fichiers pour la rotation et la taille maximum de chaque fichier.
 - **Enregistrer dans un seul fichier**. Enregistrer un fichier de traçage (sans limite de taille).
5. Choisissez le niveau de traçage dans la liste déroulante **Niveau**.
Il est recommandé de demander au spécialiste du Support Technique le niveau de traçage requis. Si les indications du Support Technique sont absentes, il est recommandé d'installer le niveau de traçage **Normal (500)**.
6. Relancez Kaspersky Endpoint Security.
7. Pour arrêter le processus de traçage, retournez à la fenêtre **Assistance** et désactivez le traçage.

Vous pouvez créer aussi les fichiers de traçage pendant l'installation de l'application via la [ligne de commande](#), y compris avec l'aide du [fichier setup.ini](#).


[Les fichiers de traçage](#) sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application. Les fichiers de traçage, à l'exception des fichiers de traçage de l'Agent d'authentification, sont stockés dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces. Par défaut, le traçage est désactivé.

Trace des performances de l'application

Kaspersky Endpoint Security vous permet d'obtenir des informations sur les problèmes rencontrés sur l'ordinateur lors de l'utilisation de l'application. Par exemple, vous pouvez obtenir des informations sur les délais de chargement du système d'exploitation après l'installation de l'application. Pour ce faire, Kaspersky Endpoint Security crée [des fichiers de traçage des performances](#). *La trace des performances* est un enregistrement des actions effectuées par l'application aux fins de diagnostic des problèmes de performances de Kaspersky Endpoint Security. Pour obtenir ces informations, Kaspersky Endpoint Security utilise le service de suivi d'événements pour Windows (ETW - Event Tracing for Windows). C'est le Support Technique de Kaspersky qui va poser le diagnostic du fonctionnement de Kaspersky Endpoint Security et identifier les causes des problèmes.

Lancez le traçage de l'application conformément aux instructions du Support Technique de Kaspersky.

Pour créer un fichier de traçage des performances, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .
La fenêtre **Assistance** s'ouvre.
2. Dans la fenêtre **Assistance**, cliquez sur le bouton **Outils de support**.
3. Utilisez le bouton **Activer les traces de performances** pour activer ou désactiver le traçage des performances de l'application.
4. Dans la liste déroulante **Traçages**, sélectionnez un mode de traçage de l'application :
 - **Avec rotation**. Enregistrer les résultats du traçage dans un nombre limité de fichiers de taille limitée et écraser les anciens fichiers quand la limite est atteinte. Si ce mode est sélectionné, vous pouvez définir la taille maximale de chaque fichier.
 - **Enregistrer dans un seul fichier**. Enregistrer un fichier de traçage (sans limite de taille).
5. Choisissez le niveau de traçage dans la liste déroulante **Niveau** :
 - **Léger**. Kaspersky Endpoint Security analyse les principaux processus du système d'exploitation liés aux performances.
 - **Détaillé**. Kaspersky Endpoint Security analyse tous les processus du système d'exploitation liés aux performances.
6. Sélectionnez le type de trace dans la liste déroulante **Type de traçage** :
 - **Informations de base**. Kaspersky Endpoint Security analyse les processus pendant l'exécution du système d'exploitation. Utilisez ce type de trace si le problème survient après le chargement du système d'exploitation, par exemple un problème d'accès à Internet dans le navigateur.
 - **Au redémarrage**. Kaspersky Endpoint Security analyse les processus uniquement au moment du chargement du système d'exploitation. Une fois le chargement du système d'exploitation terminé, Kaspersky Endpoint Security arrête la trace. Utilisez ce type de trace si le problème est lié à un délai dans le chargement du système d'exploitation.
7. Redémarrez l'ordinateur et reproduisez le problème.
8. Pour arrêter le processus de traçage, retournez à la fenêtre **Assistance** et désactivez le traçage.

Le fichier de traçage des performances est créé dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces. Après avoir créé le fichier de traçage, envoyez-le au Support Technique de Kaspersky.


Enregistrement des fichiers dump

Le fichier dump contient toutes les informations relatives à la mémoire de travail des processus de Kaspersky Endpoint Security au moment de la création de ce fichier dump.

Les vidages enregistrés peuvent contenir des données confidentielles. Pour contrôler l'accès aux données, vous devez garantir vous-même la protection des fichiers dump.

Les fichiers dump sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application. Les fichiers de vidage sont conservés dans le dossier %ProgramData%\Kaspersky Lab\KES\Traces.

Pour activer ou désactiver l'enregistrement des fichiers dump, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Dans le groupe **Données pour le débogage**, utilisez la case **Activer l'enregistrement des fichiers de vidage** pour activer ou désactiver l'enregistrement des fichiers de vidage de l'application.
4. Enregistrez vos modifications.


Protection des fichiers dump et de traçage

Les fichiers dump et les fichiers de traçage contiennent des informations sur le système d'exploitation, ainsi que des [données de l'utilisateur](#). Pour empêcher l'accès non autorisé à ces données, vous pouvez activer la protection des fichiers dump et des fichiers de traçage.

Si la protection des fichiers dump et des fichiers de traçage est activée, l'accès aux fichiers est réservé aux utilisateurs suivants :

- Les fichiers dump sont accessibles aux administrateurs local et système ainsi qu'à l'utilisateur qui a activé l'enregistrement des fichiers dump et des fichiers de traçage.
- Les fichiers de traçage sont accessibles uniquement aux administrateurs local et système.

Pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage, procédez comme suit :

1. Cliquez sur le bouton  situé dans la partie inférieure de la fenêtre principale de l'application.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Général**.
3. Dans le groupe **Données pour le débogage**, utilisez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers.
4. Enregistrez vos modifications.

Les fichiers dump et les fichiers de traçage enregistrés alors que la protection étaient activées resteront protégés même après la désactivation de cette fonction.

Restrictions et avertissements

Kaspersky Endpoint Security présente une série de restrictions n'affectant pas de manière critique l'utilisation de l'application.

[Installation de l'application](#) 

- Les particularités de la prise en charge des systèmes d'exploitation Microsoft Windows 10, Microsoft Windows Server 2016 et Microsoft Windows Server 2019 sont reprises dans la [base des connaissances du Support Technique](#).
- Après avoir été installée sur un ordinateur infecté, l'application n'informe pas l'utilisateur de la nécessité d'effectuer une analyse de l'ordinateur. Vous pourriez rencontrer des problèmes lors de l'[activation de l'application](#). Pour résoudre ces problèmes, [lancez une analyse des zones critiques](#).
- Si les fichiers setup.ini et setup.reg contiennent des caractères non-ASCII (par exemple, des lettres russes), il est conseillé de modifier le fichier à l'aide de notepad.exe et d'enregistrer le fichier en utilisant l'encodage UTF-16LE. Les autres encodages ne sont pas pris en charge.
- L'application ne prend pas en charge l'utilisation de caractères non-ASCII lors du choix du chemin d'installation de l'application dans les [paramètres du fichier d'installation](#).
- Lorsque les [paramètres de l'application sont importés à partir d'un fichier CFG](#), la valeur du paramètre qui définit la participation à Kaspersky Security Network n'est pas appliquée. Après avoir importé les paramètres, veuillez lire le texte de la Déclaration de Kaspersky Security Network et confirmer que vous acceptez de participer à Kaspersky Security Network. Vous pouvez lire le texte de la Déclaration dans l'interface de l'application ou dans le fichier ksn_*.txt situé dans le dossier contenant le kit de distribution de l'application.
- Lors de la mise à niveau à partir de Kaspersky Endpoint Security 10 Service Pack 2 for Windows (version 10.3.0.6294), le [module Prévention des intrusions est activé](#).
- Lors de la mise à jour de Kaspersky Endpoint Security 10 for Windows Service Pack 2 (version 10.3.0.6294), les fichiers placés dans la Sauvegarde et dans la Quarantaine de la version antérieure de l'application sont transférés dans la Sauvegarde de la nouvelle version. Ces fichiers ne sont pas transférés pour les versions antérieures à Kaspersky Endpoint Security 10 for Windows Service Pack 2 (version 10.3.0.6294). Pour les enregistrer, vous devez restaurer les fichiers à partir de la Quarantaine et de la Sauvegarde avant de mettre à niveau l'application. Une fois la mise à niveau terminée, analysez de nouveau les fichiers restaurés.
- Si vous souhaitez supprimer puis réinstaller le chiffrement (FLE ou FDE) ou le module de Contrôle des appareils, vous devez redémarrer le système avant la réinstallation.
- Lorsque vous utilisez le système d'exploitation Microsoft Windows 10, vous devez redémarrer le système après avoir supprimé le module File Level Encryption (FLE).
- Lorsque vous tentez d'installer une version du module AES Encryption Module sur un ordinateur qui dispose de Kaspersky Endpoint Security for Windows 11.6.0, mais sur lequel aucun module de chiffrement n'est installé, l'installation du module Encryption Module se termine par un message d'erreur indiquant qu'une version plus récente de l'application est installée. À partir de Kaspersky Endpoint Security 10 for Windows Service Pack 2 (version 10.3.0.6294), il n'y a pas de fichier d'installation séparé pour le module Encryption Module. Les bibliothèques de chiffrement sont incluses dans le paquet de distribution de l'application. Kaspersky Endpoint Security 11.6.0 est incompatible avec les modules de chiffrement AES. Les bibliothèques requises pour le chiffrement sont installées automatiquement lorsque le module Full Disk Encryption (FDE) ou File Level Encryption (FLE) est sélectionné.
- L'installation de l'application peut se terminer par une erreur indiquant *Une application dont le nom est manquant ou illisible est installée sur votre ordinateur*. Cela signifie que des applications incompatibles ou des fragments de celles-ci se trouvent toujours sur votre ordinateur. Pour supprimer des artefacts d'applications incompatibles, envoyez une demande accompagnée d'une description détaillée de la situation au Support Technique de Kaspersky via [Kaspersky CompanyAccount](#).
- À partir de la version 11.0.0 de l'application, vous pouvez installer le plug-in Kaspersky Endpoint Security for Windows MMC en plus de la version précédente du plug-in. Pour revenir à une version antérieure du plug-in,

supprimez le plug-in actuel et installez une version antérieure du plug-in.

- Lors de la mise à niveau de Kaspersky Endpoint Security 11.0.0 ou 11.0.1 for Windows, les [paramètres de la planification des tâches locales](#) pour les tâches de *mise à jour*, d'*analyse des zones critiques*, d'*analyse personnalisée* et de *vérification de l'intégrité* ne sont pas enregistrés.
- Si vous avez annulé la suppression de l'application, lancez sa restauration après le redémarrage de l'ordinateur.
- Sur les ordinateurs fonctionnant sous Windows 10 version 1903 et 1909, les mises à niveau effectuées à partir de Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (version 10.3.3.275), Service Pack 2 Maintenance Release 4 (version 10.3.3.304), 11.0.0 et 11.0.1 avec le module File Level Encryption (FLE) installé peuvent se terminer par une erreur. Cela est dû au fait que le chiffrement des fichiers n'est pas pris en charge pour ces versions de Kaspersky Endpoint Security for Windows dans Windows 10 version 1903 et 1909. Avant d'installer cette mise à niveau, il vous est conseillé de [supprimer le module de chiffrement des fichiers](#).
- Si vous mettez à niveau une version précédente de l'application vers la version 11.6.0, pour installer Kaspersky Endpoint Agent, redémarrez l'ordinateur et connectez-vous au système au moyen d'un compte disposant des droits d'administrateur local. Dans le cas contraire, Kaspersky Endpoint Agent ne sera pas installé pendant la procédure de mise à niveau.
- Si l'application n'est pas installée correctement, que le module Kaspersky Endpoint Agent est sélectionné dans le système d'exploitation d'un serveur et que la fenêtre *Windows Installer Coordinator Error* s'affiche, veuillez consulter les instructions sur le site Internet d'assistance de Microsoft.
- Si l'application a été installée localement en mode non interactif, utilisez le [fichier setup.ini](#) fourni pour remplacer les modules installés.
- Si vous mettez à niveau Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 avec le module Chiffrement des fichiers (FLE) installé sur des ordinateurs fonctionnant sous les versions 1809, 1903 et 1909 de Windows 10, les pilotes FDE ne seront pas installés sur l'image WinRE.
- Une fois que Kaspersky Endpoint Security for Windows est installé dans certaines configurations de Windows 7, Windows Defender continue de fonctionner. Il vous est conseillé de désactiver manuellement Windows Defender pour éviter une baisse des performances du système.
- Après la mise à niveau de l'application à partir de versions antérieures à Kaspersky Endpoint Security 11 for Windows, l'ordinateur doit être redémarré.

[Prise en charge de plateformes de serveurs ?](#)

- Prise en charge du système de fichiers ReFS avec des restrictions :
 - Après le lancement de l'analyse antivirus du serveur, les exclusions d'analyse ajoutées avec iChecker sont réinitialisées lorsque le serveur est redémarré.
 - Kaspersky Endpoint Security ne détecte pas les fichiers eicar.com et susp-eicar.com si le fichier meicar.exe existait sur l'ordinateur avant l'installation de Kaspersky Endpoint Security.
- Pas de prise en charge des configurations Server Core et Cluster Mode.
- Pas de prise en charge du chiffrement des fichiers et de la technologie de chiffrement du disque sur les plateformes pour serveurs.
- Pas de prise en charge du Contrôle des appareils sur les plateformes de serveurs.
- Le système d'exploitation Microsoft Windows Server 2008 est exclu de la prise en charge. - L'installation de l'application sur un ordinateur tournant sous un système d'exploitation Microsoft Windows Server 2008 n'est pas prise en charge.
- Si vous avez lancé plusieurs sessions de travail sur le serveur de terminaux, les notifications de Kaspersky Endpoint Security peuvent ne pas fonctionner correctement. Exemple : l'utilisateur de la session n° 1 exécute un contrôle de réputation de fichier dans KSN. Kaspersky Endpoint Security affichera une notification avec les résultats de la vérification à l'utilisateur de la session n° 2.

[Prise en charge de plateformes virtuelles](#)

- Le chiffrement du disque (FDE) n'est pas pris en charge sur les machines virtuelles Hyper-V.
- Le chiffrement du disque (FDE) n'est pas pris en charge sur les plateformes virtuelles Citrix.
- Windows 10 Enterprise multi-session est pris en charge avec certaines limitations :
 - Kaspersky Endpoint Security considère Windows 10 Enterprise multi-session comme un système d'exploitation de serveur. Par conséquent, Windows 10 Enterprise multi-session est pris en charge avec des limitations propres à la plateforme du serveur. Par exemple, les serveurs ne peuvent pas utiliser certains modules de Kaspersky Endpoint Security. L'application utilise également une clé de licence de serveur au lieu d'une clé de licence de poste de travail.
 - Le chiffrement du disque (FDE) n'est pas pris en charge.
 - La gestion de BitLocker n'est pas prise en charge.
 - L'utilisation de Kaspersky Endpoint Security avec des disques amovibles n'est pas prise en charge. L'infrastructure Microsoft Azure définit les disques amovibles comme des disques réseau.
- L'installation et l'utilisation du chiffrement des fichiers (FLE) ne sont pas prises en charge sur les plateformes virtuelles Citrix.
- Pour prendre en charge la compatibilité de Kaspersky Endpoint Security for Windows avec Citrix PVS, effectuez l'installation en [activant l'option Garantir la compatibilité avec Citrix PVS](#). Cette option peut être activée dans l'[Assistant d'installation](#) ou en utilisant le [paramètre de ligne de commande](#) /pCITRIXCOMPATIBILITY=1. En cas d'installation à distance, le [fichier KUD](#) doit être modifié en y ajoutant le paramètre suivant : /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop. Avant de commencer le clonage, vous devez [désactiver l'option Autodéfense](#) pour cloner les machines virtuelles qui utilisent vDisk.
- Lorsque vous préparez une machine modèle pour l'image maître Citrix XenDesktop avec une instance préinstallée de Kaspersky Endpoint Security for Windows et de l'Agent d'administration de Kaspersky Security Center, ajoutez les types d'exclusions suivants au fichier de configuration :

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Pour en savoir plus sur Citrix XenDesktop, visitez le [site du service d'assistance de Citrix](#).

- Dans certains cas, une tentative de déconnexion sécurisée d'un disque amovible peut échouer sur une machine virtuelle déployée sur un hyperviseur VMware ESXi. Essayez de déconnecter de nouveau l'appareil en toute sécurité.

[Compatibilité avec Kaspersky Security Center](#)

- Vous pouvez administrer le module Contrôle évolutif des anomalies uniquement dans la version 11 de Kaspersky Security Center ou dans une version ultérieure.
- Il se peut que le rapport sur les menaces de Kaspersky Security Center 11 n'affiche pas les informations sur les mesures prises à l'égard des menaces qui ont été détectées par la protection AMSI.
- L'état de fonctionnement des modules Protection AMSI et Contrôle évolutif des anomalies est disponible uniquement dans la version 11 de Kaspersky Security Center ou dans une version ultérieure. Vous pouvez consulter l'état de fonctionnement dans Kaspersky Security Center Console, dans les propriétés de l'ordinateur, dans la section **Tâches**. Les rapports concernant ces modules sont également disponibles uniquement dans la version 11 de Kaspersky Security Center ou dans une version ultérieure.

Licence

- Si le message système *Erreur de réception des données* s'affiche, vérifiez que l'ordinateur sur lequel vous effectuez l'activation dispose d'un accès au réseau ou configurez les paramètres d'activation via Kaspersky Security Center Activation Proxy.
- L'application ne peut pas être activée par abonnement via Kaspersky Security Center si la licence a expiré ou si une licence d'essai est active sur l'ordinateur. Pour remplacer une licence d'essai ou une licence sur le point d'expirer par une licence d'abonnement, [utilisez la tâche de distribution des licences](#).
- Dans l'interface de l'application, la date d'expiration de la licence est affichée selon l'heure locale de l'ordinateur.
- L'installation de l'application avec un fichier clé intégré sur un ordinateur ayant un accès Internet instable peut entraîner l'affichage temporaire d'événements indiquant que l'application n'est pas activée ou que la licence ne permet pas aux modules de fonctionner. En effet, l'application s'installe d'abord et tente d'activer la licence d'essai intégrée, et l'activation nécessite un accès Internet pendant la procédure d'installation.
- Pendant la période d'essai, l'installation de toute mise à niveau ou de tout correctif d'une application sur un ordinateur dont l'accès Internet est instable peut entraîner l'affichage temporaire d'événements indiquant que l'application n'est pas activée. En effet, l'application s'installe et tente de nouveau d'activer la licence d'essai intégrée, et l'activation nécessite un accès Internet lors de l'installation d'une mise à niveau.
- Si la licence d'essai a été automatiquement activée lors de l'installation de l'application et que l'application a ensuite été supprimée sans que les informations relatives à la licence soient enregistrées, l'application ne sera pas automatiquement activée avec la licence d'essai lorsqu'elle sera réinstallée. Dans ce cas, activez manuellement l'application.
- Si vous utilisez la version 11 de Kaspersky Security Center et la version 11.6.0 de Kaspersky Endpoint Security, les rapports de performance des modules peuvent ne pas fonctionner correctement. Si vous avez installé des modules de Kaspersky Endpoint Security qui ne sont pas inclus dans votre licence, il se peut que l'Agent d'administration envoie des erreurs concernant l'état des modules au journal des événements Windows. Pour éviter toute erreur, supprimez les modules qui ne sont pas inclus dans votre licence.

Réparation des actions malicieuses

- L'application restaure les fichiers uniquement sur les appareils dotés du système de fichiers NTFS et FAT32.
- L'application restaure les fichiers portant les extensions suivantes : odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xslm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Il est impossible de restaurer les fichiers installés sur les disques réseau, ainsi que sur les CD/DVD réinscriptibles.
- Il est impossible de restaurer les fichiers chiffrés à l'aide d'Encryption File System (EFS). Pour en savoir plus sur le fonctionnement d'EFS, consultez le [site de Microsoft](#).
- L'application ne contrôle pas les modifications de fichiers exécutées par les processus au niveau du noyau du système d'exploitation.
- L'application ne contrôle pas les modifications des fichiers exécutées via l'interface réseau (par exemple, le fichier se trouve dans un dossier partagé et le processus est lancé à distance depuis un autre ordinateur).

Pare-feu

- Le filtrage des paquets ou des connexions par adresse locale, interface physique et durée de vie des paquets (TTL) est pris en charge dans les cas suivants :
 - Par adresse locale pour les connexions ou les paquets sortants dans les règles d'application pour les protocoles TCP et UDP, et pour les règles de paquets.
 - Par adresse locale pour les connexions ou les paquets entrants (sauf UDP) dans les règles de blocage d'application et les règles de paquets.
 - Par durée de vie des paquets (TTL) dans les règles de paquets de blocage pour les paquets entrants ou sortants.
 - Par interface réseau pour les paquets entrants et sortants ou les connexions dans les règles de paquets.
- Dans les versions d'application 11.0.0 et 11.0.1, les adresses MAC définies sont incorrectement appliquées. Les paramètres des adresses MAC pour les versions 11.0.0, 11.0.1 et 11.1.0 ou les versions ultérieures ne sont pas compatibles. Après avoir effectué la mise à niveau de l'application ou du plug-in à partir de ces versions vers la version 11.1.0 ou vers une version ultérieure, vous devez vérifier et reconfigurer les adresses MAC définies dans les règles du pare-feu.
- Lorsque l'application est mise à niveau à partir des versions 11.1.1 et 11.2.0 vers la version 11.6.0, les états des autorisations pour les règles de pare-feu suivantes ne procèdent à aucune migration :
 - Requêtes vers le serveur DNS via le protocole TCP.
 - Requêtes vers le serveur DNS via le protocole UDP.
 - N'importe quelle activité réseau.
 - Réponses entrantes inaccessibles à la destination ICMP.
 - Flux ICMP entrant.
- Si vous avez configuré une règle pour un adaptateur réseau ou une règle de durée de vie des paquets (TTL) pour autoriser un paquet, la priorité de cette règle est inférieure à celle d'une règle pour bloquer une application. Autrement dit, si l'activité réseau est bloquée pour une application (par exemple, l'application se trouve dans le groupe de confiance *Restrictions élevées*), il est impossible d'autoriser l'activité réseau de l'application en utilisant une règle pour les paquets avec ces paramètres. Dans tous les autres cas, la priorité d'une règle pour les paquets est plus élevée que celle d'une règle réseau d'applications.
- Une erreur peut se produire dans Kaspersky Endpoint Security for Windows 11.5.0-11.6.0 lors de [l'importation d'une liste de règles pour les paquets du pare-feu](#). Il se peut que cela entraîne la suppression d'adresses locales ou distantes définies par l'utilisateur dans une règle. Pour corriger l'erreur, veuillez contacter le Support technique. Le Support technique vous fournira une mise à jour corrigée pour le plug-in. Vous pouvez également mettre l'application à niveau vers la version suivante après sa sortie.
- Lors de [l'importation d'une liste de règles pour les paquets du pare-feu](#), Kaspersky Endpoint Security peut changer les noms des règles. L'application identifie les règles qui présentent le même ensemble de paramètres principaux, comme le protocole, la direction, les ports distants et locaux ainsi que la durée de vie des paquets (TTL). Si cet ensemble de paramètres principaux est identique pour plusieurs règles, l'application attribue le même nom à ces règles ou ajoute un tag de paramètre au nom. Cela signifie que Kaspersky Endpoint Security importe toutes les règles de paquets, mais le nom des règles qui ont des paramètres principaux identiques peut être modifié.

- Lorsqu'une règle pour les paquets réseau est déclenchée dans Kaspersky Endpoint Security 11.6.0 ou une version antérieure, la colonne **Nom de l'application** dans le rapport du Pare-feu affichera toujours la valeur de *Kaspersky Endpoint Security*. En outre, le Pare-feu bloquera la connexion au niveau des paquets pour toutes les applications. Ce comportement a été modifié pour Kaspersky Endpoint Security 11.7.0 ou toute version ultérieure. La colonne **Type de règle** a été ajoutée au rapport du Pare-feu. Lorsqu'une règle pour les paquets réseau est déclenchée, la valeur de la colonne **Nom de l'application** reste vide.

Contrôle des applications ⓘ

- Lorsque vous travaillez sous Microsoft Windows 10 en mode liste de refus d'applications, les règles de blocage peuvent être mal appliquées, ce qui peut entraîner le blocage d'applications qui ne sont pas indiquées dans les règles.
- Lorsque les applications Web progressives (PWA) sont bloquées par le module Contrôle Internet, le fichier appManifest.xml est indiqué comme l'application bloquée dans le rapport.

Contrôle des appareils ⓘ

- L'accès aux appareils d'impression qui ont été ajoutés à la liste des appareils de confiance est bloqué par des règles de blocage des appareils et des bus.
- Pour les appareils MTP, le contrôle des opérations de lecture, d'écriture et de connexion est pris en charge si vous utilisez les pilotes Microsoft intégrés au système d'exploitation. Si un utilisateur installe un pilote personnalisé pour travailler avec un appareil (par exemple, dans le cadre d'iTunes ou d'Android Debug Bridge), il se peut que le contrôle des opérations de lecture et d'écriture ne fonctionne pas.
- Lorsque vous utilisez des appareils MTP, les règles d'accès sont modifiées après que vous avez reconnecté l'appareil.
- Si vous ajoutez un appareil à la liste des appareils confiance en vous fondant sur un masque de modèle et que vous utilisez des caractères qui sont inclus dans l'identifiant, mais pas dans le nom du modèle, ces appareils ne sont pas ajoutés. Sur un poste de travail, ces appareils seront ajoutés à la liste des appareils de confiance sur la base d'un masque d'identifiant.

Contrôle Internet ⓘ

- Les formats OGV et WEBM ne sont pas pris en charge.
- Le protocole RTMP n'est pas pris en charge.

Contrôle évolutif des anomalies ⓘ

- Il est recommandé de créer des exclusions automatiques en fonction de l'événement. Lorsque vous [ajoutez manuellement une exclusion](#), ajoutez le caractère * au début du chemin lors de la spécification de l'objet cible.
- Il est [impossible de générer un rapport sur les règles du Contrôle évolutif des anomalies](#) si l'échantillon comprend ne serait-ce qu'un seul événement dont le nom contient plus de 260 caractères.
- Ajout des exclusions à partir du stockage de règles du Contrôle évolutif des anomalies n'est pas pris en charge si les propriétés d'un objet ou d'un processus ont une valeur composée de plus de 256 caractères (par exemple, le chemin vers l'objet cible). Vous pouvez [ajouter une exclusion manuellement dans les paramètres de la stratégie](#). Vous pouvez également ajouter une exclusion dans le [rapport lors du déclenchement des règles du Contrôle évolutif des anomalies](#).

[Chiffrement de disque \(FDE\)](#) ²

- Après l'installation de l'application, vous devez redémarrer le système d'exploitation pour que le chiffrement du disque dur fonctionne correctement.
- L'Agent d'authentification ne prend pas en charge les hiéroglyphes ni les caractères spéciaux `||` et `\`.
- Pour des performances optimales de l'ordinateur après le chiffrement, il est nécessaire que le processeur prenne en charge le jeu d'instructions AES-NI (Intel Advanced Encryption Standard New Instructions). Si le processeur ne prend pas en charge AES-NI, les performances de l'ordinateur peuvent diminuer.
- Lorsqu'il existe des processus qui tentent d'accéder à des appareils chiffrés avant que l'application ait accordé l'accès à ces appareils, l'application affiche un avertissement indiquant que ces processus doivent être interrompus. Si les processus ne peuvent être interrompus, reconnectez les appareils chiffrés.
- Les identifiants uniques des disques durs sont affichés dans les statistiques de chiffrement des appareils en format inversé.
- Il n'est pas recommandé de formater les appareils pendant leur chiffrement.
- Lorsque plusieurs disques amovibles sont connectés simultanément à un ordinateur, la stratégie de chiffrement ne peut être appliquée qu'à un seul disque amovible. Lorsque les appareils amovibles sont reconnectés, la stratégie de chiffrement est correctement appliquée.
- Il se peut que le chiffrement ne démarre pas sur un disque dur fortement fragmenté. Défragmentez le disque dur.
- Lorsque les disques durs sont chiffrés, l'hibernation est bloquée entre le moment où la tâche de chiffrement démarre et le premier redémarrage de l'ordinateur fonctionnant sous Microsoft Windows 7/8/8.1/10, et entre le chiffrement du disque dur et le premier redémarrage des systèmes d'exploitation Microsoft Windows 8/8.1/10. Lorsque les disques durs sont déchiffrés, l'hibernation est bloquée entre le moment où le disque de démarrage est entièrement déchiffré et le premier redémarrage du système d'exploitation. Lorsque l'option **Démarrage rapide** est activée dans Microsoft Windows 8/8.1/10, le blocage de l'hibernation vous empêche d'éteindre le système d'exploitation.
- Les ordinateurs Windows 7 ne permettent pas de modifier le mot de passe pendant la récupération lorsque le disque est chiffré avec la technologie BitLocker. Une fois que la clé de récupération est saisie et que le système d'exploitation est chargé, Kaspersky Endpoint Security n'invite pas l'utilisateur à modifier le mot de passe ou le code PIN. Il est donc impossible de définir un nouveau mot de passe ou un nouveau code PIN. Ce problème provient des particularités du système d'exploitation. Pour continuer, vous devez de nouveau chiffrer le disque dur.
- Il n'est pas recommandé d'utiliser l'outil xbootmgr.exe avec des fournisseurs supplémentaires activés. Par exemple, Dispatcher, Network, ou Drivers.
- Le formatage d'un disque amovible chiffré n'est pas pris en charge sur un ordinateur sur lequel une instance de Kaspersky Endpoint Security for Windows est installée.
- Le formatage d'un disque amovible chiffré avec le système de fichiers FAT32 n'est pas pris en charge (le disque est affiché comme étant chiffré). Pour formater un disque, reformatez-le au système de fichiers NTFS.
- Pour en savoir plus sur la restauration d'un système d'exploitation à partir d'une copie de sauvegarde vers un appareil GPT chiffré, consultez la [base des connaissances du Support Technique](#).
- Plusieurs agents de téléchargement ne peuvent pas coexister sur un seul ordinateur chiffré.

- Il est impossible d'accéder à un disque amovible qui était auparavant chiffré sur un autre ordinateur lorsque toutes les conditions suivantes sont simultanément remplies :
 - Il n'y a aucune connexion au serveur de Kaspersky Security Center.
 - L'utilisateur tente de procéder à une autorisation avec un nouveau jeton ou mot de passe.

Si une situation semblable se produit, redémarrez l'ordinateur. Après que l'ordinateur aura été redémarré, l'accès au disque amovible chiffré sera accordé.

- Il se peut que l'Agent d'authentification ne puisse pas découvrir les appareils USB lorsque le mode xHCI pour USB est activé dans les paramètres du BIOS.
- La technologie Kaspersky Disk Encryption (FDE) pour la partie SSD d'un appareil qui sert à mettre en cache les données les plus fréquemment utilisées n'est pas prise en charge pour les appareils SSHD.
- Le chiffrement des disques durs dans les systèmes d'exploitation Microsoft Windows 8/8.1/10 32 bits fonctionnant en mode UEFI n'est pas pris en charge.
- Redémarrez l'ordinateur avant de chiffrer de nouveau un disque dur déchiffré.
- Le chiffrement des disques durs n'est pas compatible avec Kaspersky Anti-Virus for UEFI. Il n'est pas recommandé d'utiliser le chiffrement de disques durs sur les ordinateurs sur lesquels une instance de Kaspersky Anti-Virus for UEFI est installée.
- [La création de comptes d'Agent d'authentification](#) reposant sur des comptes Microsoft est prise en charge avec les restrictions suivantes :
 - La technologie [Single Sign-On](#) n'est pas prise en charge.
 - La création automatique de comptes d'Agent d'authentification n'est pas prise en charge si l'option de création de comptes pour les utilisateurs qui se connectent au système au cours des X derniers jours est sélectionnée.
- Si le nom de compte d'un Agent d'authentification présente le format <domaine>/<nom du compte Windows>, après avoir changé le nom de l'ordinateur, vous devez également changer les noms des comptes qui ont été créés pour les utilisateurs locaux de cet ordinateur. Par exemple, imaginez que l'ordinateur de Dubois de l'utilisateur local Dubois dispose d'un compte d'Agent d'authentification portant le nom Dubois/Dubois et qu'un compte a été créé pour cet utilisateur. Si le nom de l'ordinateur Dubois a été changé en Dubois-PC, vous devez changer le nom du compte de l'Agent d'authentification pour l'utilisateur Dubois de Dubois/Dubois à Dubois-PC/Dubois. Vous pouvez modifier le nom du compte en utilisant la tâche d'administration de comptes locaux de l'Agent d'authentification. Avant que le nom du compte n'ait été modifié, il est possible de s'authentifier dans l'environnement préalable au démarrage à l'aide de l'ancien nom (par exemple, Dubois/Dubois).
- Si un utilisateur est autorisé à accéder à un ordinateur qui a été chiffré à l'aide de la technologie Kaspersky Disk Encryption uniquement en utilisant un jeton et que cet utilisateur doit suivre la procédure de récupération de l'accès, assurez-vous que cet utilisateur est autorisé à accéder à cet ordinateur en utilisant un mot de passe après que l'accès à l'ordinateur chiffré a été rétabli. Le mot de passe que l'utilisateur a défini lors de la récupération de l'accès peut ne pas être enregistré. Dans ce cas, l'utilisateur devra suivre la procédure de récupération de l'accès à l'ordinateur chiffré lors du prochain redémarrage de l'ordinateur.
- Lors du déchiffrement d'un disque dur à l'aide de l'outil [FDE Recovery Tool](#), le processus de déchiffrement peut se terminer par une erreur si les données de l'appareil source sont remplacées par les données déchiffrées. Une partie des données sur le disque dur restera chiffrée. Lors de l'utilisation de l'outil FDE Recovery Tool, dans les paramètres de déchiffrement de l'appareil, il est recommandé de choisir l'option permettant d'enregistrer les données déchiffrées dans un fichier.

- Si le mot de passe de l'Agent d'authentification a été modifié, un message contenant le texte *Votre mot de passe a bien été modifié s'affiche. Le message Cliquez sur OK s'affiche*, l'utilisateur redémarre l'ordinateur, et le nouveau mot de passe n'est pas enregistré. L'ancien mot de passe doit être utilisé pour toute authentification ultérieure dans l'environnement préalable au démarrage.
- La technologie Intel Rapid Start ne prend pas en charge le chiffrement des disques.
- La technologie ExpressCache ne prend pas en charge le chiffrement des disques.
- Dans certains cas, lorsque l'on tente de déchiffrer un disque chiffré à l'aide de l'outil [FDE Recovery Tool](#), celui-ci détecte par erreur que l'état de l'appareil est "non chiffré" après que la procédure "Demande-Réponse" a été effectuée. Le journal de l'outil montre un événement indiquant que l'appareil a bien été déchiffré. Dans ce cas, vous devez relancer la procédure de restauration des données pour déchiffrer l'appareil.
- Après la mise à jour du plug-in Kaspersky Endpoint Security for Windows dans Web Console, les propriétés du poste client n'affichent pas la clé de restauration BitLocker avant le redémarrage du service de Web Console.
- Pour connaître les autres restrictions de la prise en charge du chiffrement des disques ainsi que la liste des appareils pour lesquels le chiffrement des disques durs est pris en charge avec des restrictions, veuillez consulter la [base des connaissances du Support Technique](#).

[Chiffrement des fichiers \(FLE\)](#)

- Le chiffrement des fichiers et des dossiers n'est pas pris en charge par les systèmes d'exploitation de la famille Microsoft Windows Embedded.
- Une fois que l'application est installée, vous devez redémarrer le système d'exploitation pour que le chiffrement des fichiers et des dossiers fonctionne correctement.
- Si un fichier chiffré est stocké sur un ordinateur qui dispose d'une fonctionnalité de chiffrement et que vous accédez au fichier à partir d'un ordinateur où le chiffrement n'est pas possible, vous aurez un accès direct à ce fichier. Un fichier chiffré qui est stocké dans un dossier réseau sur un ordinateur qui propose une fonctionnalité de chiffrement est copié sous forme déchiffrée sur un ordinateur qui n'offre aucune fonctionnalité de chiffrement.
- Il est conseillé de déchiffrer les fichiers qui ont été chiffrés avec Encrypting File System avant de les chiffrer à l'aide de Kaspersky Endpoint Security for Windows.
- Une fois qu'un fichier est chiffré, sa taille augmente de 4 Ko.
- Une fois qu'un fichier est chiffré, l'attribut *Archive* est défini dans les propriétés du fichier.
- Si un fichier décompressé d'une archive chiffrée porte le même nom qu'un fichier existant sur votre ordinateur, ce dernier sera écrasé par le nouveau fichier décompressé d'une archive chiffrée. L'utilisateur n'est pas informé de l'opération de remplacement.
- L'interface du [Gestionnaire de fichiers portable](#) n'affiche aucun message à propos des erreurs qui se produisent pendant son fonctionnement.
- Kaspersky Endpoint Security for Windows ne lance pas le [Gestionnaire de fichiers portable](#) sur un ordinateur sur lequel est installé le module de chiffrement des fichiers.
- Le [Gestionnaire de fichiers portable](#) ne peut pas être utilisé pour accéder à un disque amovible si les conditions suivantes sont simultanément réunies :
 - Il n'y a aucune connexion à Kaspersky Security Center ;
 - Kaspersky Endpoint Security for Windows est installé sur l'ordinateur ;
 - Le chiffrement des données (FDE ou FLE) n'a pas été effectué sur l'ordinateur.

Dans ce cas, l'accès n'est pas possible même si vous connaissez le mot de passe du Gestionnaire de fichiers portable.

- Lorsque le chiffrement des fichiers est utilisé, l'application est incompatible avec le client de messagerie Sylpheed.
- Kaspersky Endpoint Security for Windows ne prend pas en charge [les règles de restriction d'accès aux fichiers chiffrés](#) pour certaines applications. Cela est dû au fait que certaines opérations sur les fichiers sont effectuées par une application tierce. Par exemple, la copie de fichiers est effectuée par le gestionnaire de fichiers, et non par l'application elle-même. Ainsi, si l'accès aux fichiers chiffrés est refusé au client de messagerie Outlook, Kaspersky Endpoint Security permettra au client de messagerie d'accéder au fichier chiffré, si l'utilisateur a copié des fichiers dans l'email via le presse-papiers ou en utilisant la fonctionnalité glisser-déposer. L'opération de copie a été effectuée par un gestionnaire de fichiers, pour lequel les règles de restriction d'accès aux fichiers chiffrés ne sont pas précisées, c'est-à-dire que l'accès est autorisé.
- La modification des paramètres du fichier de page n'est pas prise en charge. Le système d'exploitation utilise les valeurs par défaut au lieu des valeurs des paramètres définis.

- Utilisez la fonctionnalité de retrait en toute sécurité lorsque vous utilisez des disques amovibles chiffrés. Nous ne pouvons pas garantir l'intégrité des données si le disque amovible n'est pas retiré en toute sécurité.
- Une fois que les fichiers sont chiffrés, leurs originaux non chiffrés sont effacés de manière sécurisée.
- La synchronisation des fichiers hors ligne à l'aide de la mise en cache côté client (CSC) n'est pas prise en charge. Il est recommandé d'interdire l'administration hors ligne des ressources partagées au niveau de la stratégie de groupe. Les fichiers qui sont en mode hors ligne peuvent être modifiés. Après la synchronisation, les modifications apportées à un fichier hors ligne peuvent être perdues. Pour en savoir plus sur la prise en charge de la mise en cache côté client (CSC) lors de l'utilisation du chiffrement, veuillez consulter la [base des connaissances du Support Technique](#).
- [La création d'une archive chiffrée](#) dans la racine du disque dur du système n'est pas prise en charge.
- Vous risquez de rencontrer des problèmes pour accéder à des fichiers chiffrés sur le réseau. Il vous est conseillé de déplacer les fichiers vers une autre source ou de vous assurer que l'ordinateur utilisé comme serveur de fichiers est administré par le même Serveur d'administration de Kaspersky Security Center.
- La modification de la disposition du clavier peut entraîner le blocage de la fenêtre de saisie du mot de passe d'une archive auto-extractible chiffrée. Pour résoudre ce problème, fermez la fenêtre de saisie du mot de passe, changez la disposition du clavier de votre système d'exploitation et saisissez de nouveau le mot de passe de l'archive chiffrée.
- Lorsque le chiffrement des fichiers est utilisé sur des systèmes qui comportent plusieurs partitions sur un même disque, il est conseillé d'utiliser l'option qui détermine automatiquement la taille du fichier pagefile.sys. Une fois que l'ordinateur redémarre, le fichier pagefile.sys peut être déplacé entre les partitions du disque.
- Une fois que vous avez appliqué les règles de chiffrement des fichiers, y compris les fichiers du dossier Mes documents, assurez-vous que les utilisateurs pour lesquels le chiffrement a été appliqué peuvent correctement accéder aux fichiers chiffrés. Pour ce faire, demandez à chaque utilisateur de se connecter au système lorsqu'une connexion à Kaspersky Security Center est proposée. Si un utilisateur tente d'accéder à des fichiers chiffrés sans se connecter à Kaspersky Security Center, le système risque de se bloquer.
- Si les fichiers système sont d'une manière ou d'une autre inclus dans la zone d'action du chiffrement des fichiers, il se peut que des événements concernant des erreurs survenues lors du chiffrement de ces fichiers figurent dans les rapports. En réalité, les fichiers indiqués lors de ces événements ne sont pas chiffrés.
- Les processus Pico ne sont pas pris en charge.
- Les chemins d'accès sensibles à la casse ne sont pas pris en charge. Lorsque des règles de chiffrement ou de déchiffrement sont appliquées, les chemins d'accès aux événements des produits sont affichés en minuscules.
- Il n'est pas recommandé de chiffrer les fichiers que le système utilise au démarrage. Si ces fichiers sont chiffrés, une tentative d'accès à des fichiers chiffrés sans connexion à Kaspersky Security Center peut entraîner le blocage du système ou faire apparaître des invites d'accès à des fichiers non chiffrés.
- Lorsque des disques amovibles sont chiffrés avec la [prise en charge du mode portable](#), il est impossible de désactiver le contrôle de l'âge par mot de passe.
- Si des utilisateurs travaillent conjointement avec un fichier sur le réseau conformément aux règles FLE au moyen d'applications qui utilisent la méthode de mappage fichier-mémoire (comme WordPad ou FAR) et d'applications conçues pour travailler avec des fichiers volumineux (comme Notepad++), il se peut que le

fichier sous forme non chiffrée se bloque pour une durée indéterminée, sans qu'il soit possible d'y accéder à partir de l'ordinateur sur lequel il se trouve.

- Le chiffrement des fichiers n'est pas pris en charge dans les dossiers de synchronisation OneDrive. L'ajout de dossiers contenant des fichiers déjà chiffrés à la liste de synchronisation OneDrive peut entraîner la perte de données dans les fichiers chiffrés.
- Lorsque le module de chiffrement des fichiers est installé, l'administration des utilisateurs et des groupes ne fonctionne pas en mode WSL (Windows Subsystem for Linux).
- Lorsque le module de chiffrement des fichiers est installé, l'interface POSIX (Portable Operating System Interface) n'est pas prise en charge pour renommer et supprimer des fichiers.
- Après la mise à jour de Kaspersky Endpoint Security for Windows version 11.0.1 ou antérieure, pour accéder aux fichiers chiffrés après le redémarrage de l'ordinateur, assurez-vous que l'Agent d'administration est en cours d'exécution. L'Agent d'administration a un démarrage retardé, vous ne pouvez donc pas accéder aux fichiers chiffrés immédiatement après le chargement du système d'exploitation. Il n'est pas nécessaire d'attendre que l'Agent d'administration démarre après le prochain démarrage de l'ordinateur.

[Autres restrictions](#)

- Les systèmes d'exploitation des serveurs n'affichent aucun avertissement concernant la nécessité de procéder à une désinfection avancée.
- Il se peut que les adresses Internet qui sont [ajoutées à la liste des adresses de confiance](#) soient traitées de manière incorrecte.
- Kaspersky Endpoint Security surveille le trafic HTTP conforme aux normes RFC 2616, RFC 7540, RFC 7541 et RFC 7301. Si Kaspersky Endpoint Security détecte un autre format d'échange de données dans le trafic HTTP, l'application bloque cette connexion pour empêcher le téléchargement de fichiers malveillants depuis Internet.
- Kaspersky Endpoint Security ne prend pas en charge la norme RFC9218 pour le protocole HTTP/2. Si Kaspersky Endpoint Security détecte ce format d'échange de données dans le trafic, l'application bloque cette connexion, et le navigateur affiche l'erreur ERR_HTTP2_PROTOCOL_ERROR. Si vous avez besoin d'accéder à cette ressource Internet, vous pouvez [exclure la ressource Internet des analyses de connexions chiffrées](#) ou contacter le Support Technique pour obtenir un correctif.
- System Watcher. Les renseignements complets sur les processus ne sont pas affichés.
- Lorsque Kaspersky Endpoint Security for Windows est lancé pour la première fois, il se peut qu'une application dotée d'une signature numérique soit temporairement placée dans le mauvais groupe. L'application dotée d'une signature numérique sera ensuite placée dans le bon groupe.
- Lorsque vous analysez des emails au moyen de l'extension [Protection contre les menaces par emails pour Microsoft Outlook](#), il vous est conseillé d'utiliser le mode d'échange en cache (l'option Utiliser le mode d'échange en cache).
- [La tâche Recherche de virus](#) ne prend pas en charge la version 64 bits de Microsoft Outlook. Cela signifie que Kaspersky Endpoint Security n'analyse pas les fichiers Outlook x64 (fichiers PST et OST) même si [l'email est inclus dans la zone d'analyse](#).
- Dans Kaspersky Security Center 10, lors du passage de Kaspersky Security Network mondial à Kaspersky Security Network privé, ou vice versa, [l'option de participation à Kaspersky Security Network est désactivée](#) dans la stratégie du produit en particulier. Après le changement, lisez attentivement le texte de la Déclaration de Kaspersky Security Network et confirmez votre consentement à participer à KSN. Vous pouvez lire le texte de la Déclaration dans l'interface de l'application ou en modifiant la stratégie du produit.
- Lors d'une nouvelle analyse d'un objet malveillant qui a été bloqué par un logiciel tiers, l'utilisateur n'est pas averti lorsque la menace est de nouveau détectée. L'événement de redétection de la menace est affiché dans le rapport du produit et dans le rapport de Kaspersky Security Center 10.
- Le module [Endpoint Sensor](#) ne peut pas être installé dans Microsoft Windows Server 2008.
- Le rapport de Kaspersky Security Center 10 sur le chiffrement des appareils ne contiendra aucune information sur les appareils qui ont été chiffrés à l'aide de Microsoft BitLocker sur des plateformes de serveurs ou sur des postes de travail sur lesquels le module Contrôle des appareils n'est pas installé.
- Lorsque vous utilisez une hiérarchie de stratégies, les paramètres de la section Chiffrement des disques amovibles dans une stratégie enfant sont accessibles et peuvent être modifiés si la stratégie parente interdit la modification de ces paramètres.
- Vous devez activer l'audit d'ouverture de session dans les paramètres du système d'exploitation afin de garantir le bon fonctionnement des [exclusions pour la protection des dossiers partagés contre le chiffrement externe](#).

- Si la [protection des dossiers partagés est activée](#), Kaspersky Endpoint Security for Windows surveille les tentatives de chiffrement des dossiers partagés de chaque session d'accès à distance qui a été lancée avant le démarrage de Kaspersky Endpoint Security for Windows, y compris si l'ordinateur à partir duquel la session d'accès à distance a été lancée a été ajouté aux exclusions. Si vous ne souhaitez pas que Kaspersky Endpoint Security for Windows surveille les tentatives de chiffrement des dossiers partagés des sessions d'accès à distance qui ont été lancées à partir d'un ordinateur ajouté aux exclusions avant le démarrage de Kaspersky Endpoint Security for Windows, mettez fin à la session d'accès à distance et rétablissez-la ou redémarrez l'ordinateur sur lequel Kaspersky Endpoint Security for Windows est installé.
- Si la [tâche de mise à jour est exécutée avec les autorisations d'un compte utilisateur particulier](#), les correctifs du produit ne seront pas téléchargés lors d'une mise à jour à partir d'une source qui nécessite une autorisation.
- L'application risque de ne pas démarrer en raison de performances insuffisantes du système. Pour résoudre ce problème, utilisez l'option Ready Boot ou augmentez le délai d'attente du système d'exploitation pour le démarrage des services.
- L'application ne peut pas fonctionner en mode protégé.
- Pour que les versions 11.5.0 et 11.6.0 de Kaspersky Endpoint Security for Windows puissent fonctionner correctement avec le logiciel Cisco AnyConnect, vous devez installer la version 4.3.183.2048 de Compliance Module ou une version ultérieure. Pour en savoir plus à propos de la compatibilité avec Cisco Identity Services Engine, consultez la [documentation de Cisco](#).
- Nous ne pouvons pas garantir que la fonctionnalité Audio Control fonctionnera jusqu'au premier redémarrage après l'installation de l'application.
- Lorsque la rotation des fichiers de traçage est activée, aucune trace n'est créée pour le module AMSI ni pour le plug-in Outlook.
- Les traces de performances ne peuvent pas être collectées manuellement dans Windows Server 2008.
- Les traces de performances ne sont pas prises en charge pour le type de trace "Restart".
- La tâche de contrôle de la disponibilité de KSN n'est plus prise en charge.
- La désactivation de l'option "Désactiver l'administration externe des services système" ne vous permettra pas d'arrêter le service de l'application qui a été installée avec le paramètre AMPPL=1 (par défaut, la valeur du paramètre est fixée à 1 à partir de la version du système d'exploitation Windows 10RS2). Le paramètre AMPPL portant la valeur 1 permet de recourir à la technologie des processus de protection pour le service produit.
- Pour effectuer une analyse personnalisée d'un dossier, l'utilisateur qui lance l'analyse personnalisée doit avoir l'autorisation de lire les attributs de ce dossier. Dans le cas contraire, l'analyse du dossier personnalisé sera impossible et se terminera par une erreur.
- Lorsqu'une règle d'analyse définie dans une stratégie comprend un chemin sans le caractère \ à la fin, par exemple, C:\folder1\folder2, l'analyse sera exécutée pour le chemin C:\folder1\.
- Lors de la mise à niveau de l'application de la version 11.1.0 vers la version 11.6.0, les paramètres de la protection AMSI seront réinitialisés à leurs valeurs par défaut.
- Si vous utilisez des stratégies de restriction logicielle (SRP), l'ordinateur peut ne pas se charger (écran noir). Il vous est conseillé de modifier les paramètres SRP comme suit : définissez la valeur **Tous les fichiers de logiciels à l'exception des bibliothèques (ex. fichiers DLL)** pour le paramètre **Appliquer les stratégies de restriction logicielle aux fichiers suivants** et ajoutez des règles avec le niveau de sécurité **Sans restriction** aux chemins d'accès aux fichiers de l'application (C:\Program Files\Common

Files\Kaspersky Lab et C:\Program Files\Kaspersky Lab). Pour en savoir plus à propos de l'utilisation des SRP, consultez la [documentation de Microsoft](#).

- L'administration des paramètres du plug-in Outlook via l'API Rest n'est pas prise en charge.
- Les paramètres d'exécution des tâches pour un utilisateur particulier ne peuvent pas être transférés entre les appareils via un fichier de configuration. Une fois que les paramètres sont appliqués à partir d'un fichier de configuration, indiquez manuellement le nom d'utilisateur et le mot de passe.
- Après qu'une mise à jour a été installée, la tâche de vérification de l'intégrité ne fonctionne pas tant que le système n'est pas redémarré pour appliquer la mise à jour.
- Lorsque le niveau de traçage pivoté est modifié par l'utilitaire de diagnostic à distance, Kaspersky Endpoint Security for Windows affiche incorrectement une valeur vide pour le niveau de traçage. Toutefois, les fichiers de traçage sont rédigés en fonction du niveau de traçage correct. Lorsque le niveau de traçage pivoté est modifié via l'interface locale de l'application, le niveau de traçage est correctement modifié, mais l'utilitaire de diagnostic à distance affiche incorrectement le niveau de traçage qui a été défini en dernier lieu par l'utilitaire. Par conséquent, il se peut que l'administrateur ne dispose pas d'informations à jour sur le niveau de traçage actuel et que des renseignements pertinents ne figurent pas dans les traçages si un utilisateur modifie manuellement le niveau de traçage dans l'interface locale de l'application.
- Dans l'interface locale, les paramètres de protection par mot de passe ne permettent pas de modifier le nom du compte administrateur (KLAdmin par défaut). Pour modifier le nom du compte administrateur, vous devez désactiver la protection par mot de passe, puis activer la protection par mot de passe et définir un nouveau nom pour le compte administrateur.
- Kaspersky Endpoint Security surveille le trafic HTTP conforme aux normes RFC 2616, RFC 7540, RFC 7541 et RFC 7301. Si Kaspersky Endpoint Security détecte un autre format d'échange de données dans le trafic HTTP, l'application bloque cette connexion pour empêcher le téléchargement de fichiers malveillants depuis Internet.
- Lors de l'analyse d'une connexion chiffrée, Kaspersky Endpoint Security force HTTP/1.
- L'application Kaspersky Endpoint Security, lorsqu'elle est installée sur un serveur Windows Server 2019, est incompatible avec Docker. Le déploiement de conteneurs Docker sur un ordinateur avec Kaspersky Endpoint Security provoque un plantage (BSOD).

Glossaire

Agent d'administration

Module de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce module est unique pour toutes les applications de Kaspersky qui fonctionnent sous Windows. Des versions distinctes de l'Agent d'administration sont prévues pour les applications qui fonctionnent sous d'autres systèmes d'exploitation.

Agent d'authentification

Interface permettant après le chiffrement du secteur d'amorçage du disque de réaliser la procédure d'authentification pour accéder aux disques durs chiffrés et pour charger le système d'exploitation.

Archive

Un ou plusieurs fichiers réunis au sein d'un fichier compressé. La compression et la décompression des données requièrent une application spéciale : un outil de compression.

Base des URL de phishing

Liste d'adresses Internet identifiées par les spécialistes de Kaspersky comme étant des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky.

Base des URL malveillantes

Liste des adresses de sites Internet dont le contenu pourrait constituer une menace. La liste est créée par les experts de Kaspersky. Elle est actualisée régulièrement et elle est comprise dans le kit de distribution de l'application de Kaspersky.

Bases antivirus

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky à la date de publication des bases antivirus. Les signatures des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Ces bases antivirus sont créées par les experts de Kaspersky et mises à jour toutes les heures.

Certificat de licence

Document fourni par Kaspersky avec le fichier clé ou le code d'activation. Il contient les informations concernant la licence octroyée.

Clé active

Clé utilisée au moment actuel pour faire fonctionner l'application.

Clé complémentaires

Clé qui confirme le droit d'utilisation de l'application, mais non utilisée pour le moment.

Émetteur de certificat

Centre de certification qui a émis le certificat.

Faux positif

Situation où un fichier non infecté est considéré comme infecté par l'application de Kaspersky car son code évoque celui d'un virus.

Fichier infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit de fichiers exécutables avec, par exemple, les extensions com, exe, dll, etc. Il existe un risque assez élevé d'intrusion de code malveillant dans ces fichiers.

Fichier infecté

Fichier qui contient un code malveillant (pendant l'analyse le code d'une application présentant une menace connue a été détecté). Les experts de Kaspersky vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

Forme normalisée de l'adresse du site Internet

La forme normalisée de l'adresse du site Internet est une représentation écrite de l'adresse du site Internet obtenue grâce à la normalisation. La normalisation est un processus de modification de la représentation écrite de l'adresse du site Internet conformément aux règles spécifiques (par exemple, exclusion du nom d'utilisateur, du mot de passe et du port de connexion de la représentation écrite de l'adresse du site Internet, conversion des caractères majuscules de l'adresse du site Internet en caractères minuscules).

Le but de la normalisation des adresses des sites Internet dans le contexte du fonctionnement des modules de la protection est de vérifier une seule fois les adresses des sites Internet qui ont une équivalence physique, mais qui sont différentes du point de vue de la syntaxe.

Exemple :

La forme non normalisée de l'adresse : `www.Example.com\.`

La forme normalisée de l'adresse : `www.example.com.`

Gestionnaire de fichiers portable

Application qui fait office d'interface pour manipuler les fichiers chiffrés sur les disques amovibles si la fonction de chiffrement n'est pas disponible sur l'ordinateur.

Groupe d'administration

Ensemble d'appareils regroupés selon les fonctions exécutées et les applications de Kaspersky installées. Les appareils sont regroupés pour en faciliter la gestion dans son ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

Masque

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:**.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
- Deux caractères `**` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier***.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:***.txt` n'est pas un masque valide. Le masque `**` est disponible uniquement pour créer des exceptions pour l'analyse.
- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

Objet OLE

Fichier attaché ou intégré à un autre fichier. Les applications de Kaspersky permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel® dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

Réparation d'objets

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Certains objets infectés ne peuvent pas être désinfectés.

Tâche

Fonctions exécutées par l'application de Kaspersky sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète du périphérique, Mise à jour des bases de données.

Trusted Platform Module

Puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Le Trusted Platform Module s'installe en général sur la carte mère de l'ordinateur et interagit avec les autres modules système via le bus matériel.

Zone d'analyse

Objets analysés par Kaspersky Endpoint Security pendant l'exécution de l'analyse.

Zone de protection

Objets analysés en permanence durant le fonctionnement du module de la protection principale. Les propriétés de la zone de protection des modules différents peuvent varier.

Annexes

Cette section contient des informations qui viennent compléter le texte principal.

Annexe 1. Paramètres de l'application

Vous pouvez utiliser une [stratégie](#), des [tâches](#) ou l'[interface de l'application](#) pour configurer Kaspersky Endpoint Security. Les informations détaillées sur les modules de l'application sont fournies dans les sous-sections correspondantes.

Protection contre les fichiers malicieux



Le module Protection contre les fichiers malicieux permet d'éviter l'infection du système de fichiers de l'ordinateur. Par défaut, le module Protection contre les fichiers malicieux se trouve en permanence dans la mémoire vive de l'ordinateur. Le module analyse les fichiers sur tous les disques de l'ordinateur, ainsi que sur les disques connectés. Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.

Le module analyse les fichiers auxquels l'utilisateur ou l'application accède. Si un fichier malveillant est détecté, Kaspersky Endpoint Security bloque l'opération sur le fichier. L'application désinfecte ou supprime ensuite le fichier malveillant, en fonction des paramètres du module Protection contre les fichiers malicieux.

En cas d'accès à un fichier dont le contenu sur OneDrive, Kaspersky Endpoint Security charge et analyse le contenu de ce fichier.

Paramètres du module Protection contre les fichiers malicieux

| Paramètre | Description |
|---|--|
| Niveau de sécurité <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les fichiers malicieux. Ces groupes de paramètres stockés dans l'application sont appelés <i>niveaux de sécurité</i> :</p> <ul style="list-style-type: none">• Élevé. Niveau de sécurité des fichiers auquel le module Protection contre les fichiers malicieux assure un contrôle maximal sur tous les fichiers ouverts, enregistrés et exécutés. Le module Protection contre les fichiers malicieux analyse tous les types de fichiers sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur. Il scanne aussi des archives, des paquets d'installation et des objets OLE intégrés.• Recommandé. Ce niveau de protection du fichier est recommandé par les experts de Kaspersky. Le module Protection contre les fichiers malicieux analyse uniquement les formats de fichiers spécifiés sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur, ainsi que les objets OLE intégrés. Le module Protection contre les fichiers malicieux n'analyse pas les archives ni les paquets d'installation.• Faible. Les paramètres de ce niveau de protection du fichier garantissent une vitesse de numérisation maximale. Le module Protection contre les fichiers malicieux analyse uniquement les fichiers avec les extensions spécifiées sur l'ensemble des disques durs, des disques amovibles et des disques réseau de l'ordinateur. Le module Protection contre les fichiers malicieux n'analyse pas les fichiers composés. |

| | |
|---|---|
| <p>Types de fichiers</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Tous les fichiers. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension).</p> <p>Fichiers analysés par format. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables . Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte.</p> <p>Fichiers analysés selon l'extension. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables . Le format du fichier sera déterminé sur la base de son extension.</p> |
| <p>Zone de protection</p> | <p>Contient les objets que le module Protection contre les fichiers malicieux analyse. L'objet à vérifier peut être un disque dur, un disque amovible ou disque réseau, un dossier, un fichier ou plusieurs fichiers définis selon un masque.</p> <p>Le module Protection contre les fichiers malicieux analyse par défaut les fichiers exécutés sur tous les disques durs, les disques amovibles et les disques réseau. La zone de protection de ces objets ne peut être ni modifiée, ni supprimée. Vous pouvez uniquement exclure l'objet (par exemple, les disques amovibles) de l'analyse.</p> |
| <p>Machine learning et analyse sur la base de signatures</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Machine learning et l'analyse sur la base de signatures utilisent les bases de Kaspersky Endpoint Security qui contiennent les descriptions des menaces connues et les méthodes de désinfection. La protection à l'aide de cette méthode d'analyse garantit le niveau de sécurité minimal admissible.</p> <p>Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.</p> |
| <p>Analyse heuristique</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| <p>Action en cas de détection d'une menace</p> | <p>Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.</p> <p>Désinfecter ; bloquer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.</p> |

| | |
|---|--|
| | <p>Interdire. Si cette option est sélectionnée, le module Protection contre les fichiers malicieux bloque automatiquement les fichiers infectés sans tenter de les désinfecter.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Avant de tenter de désinfecter ou de supprimer un fichier infecté, Kaspersky Endpoint Security crée une copie de sauvegarde du fichier au cas où vous auriez besoin de restaurer le fichier ou au cas où il pourrait être désinfecté à l'avenir.</p> </div> |
| Analyser uniquement les nouveaux fichiers et les fichiers modifiés | Analyse uniquement les nouveaux fichiers et les fichiers qui ont été modifiés depuis la dernière fois qu'ils ont été analysés. Cela permettra de réduire la durée de l'analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. |
| Analyser les archives | Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE. |
| Analyser les paquets de distribution | La case active/désactive l'analyse des paquets de distribution des logiciels tiers. |
| Analyser les fichiers aux formats Microsoft Office | Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. |
| Ne pas décompresser les fichiers composés de grande taille | <p>Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie.</p> <p>Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.</p> </div> |
| Décompresser les fichiers composés en arrière-plan | <p>Si la case est cochée, Kaspersky Endpoint Security permet d'accéder aux fichiers composés dont la taille est supérieure à la valeur spécifiée avant que ces fichiers ne soient analysés. Dans ce cas, Kaspersky Endpoint Security décompresse et analyse en arrière-plan les fichiers composés.</p> <p>Kaspersky Endpoint Security permet d'accéder aux fichiers composés qui sont plus petits que cette valeur uniquement après le déballage et l'analyse de ces fichiers.</p> <p>Si cette case n'est pas cochée, Kaspersky Endpoint Security permet d'accéder aux fichiers composés uniquement après la décompression et l'analyse des fichiers de n'importe quelle taille.</p> |
| Mode d'analyse | <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security analyse les fichiers auxquels accède l'utilisateur, le système d'exploitation ou une application fonctionnant sous le compte de l'utilisateur.</p> </div> |

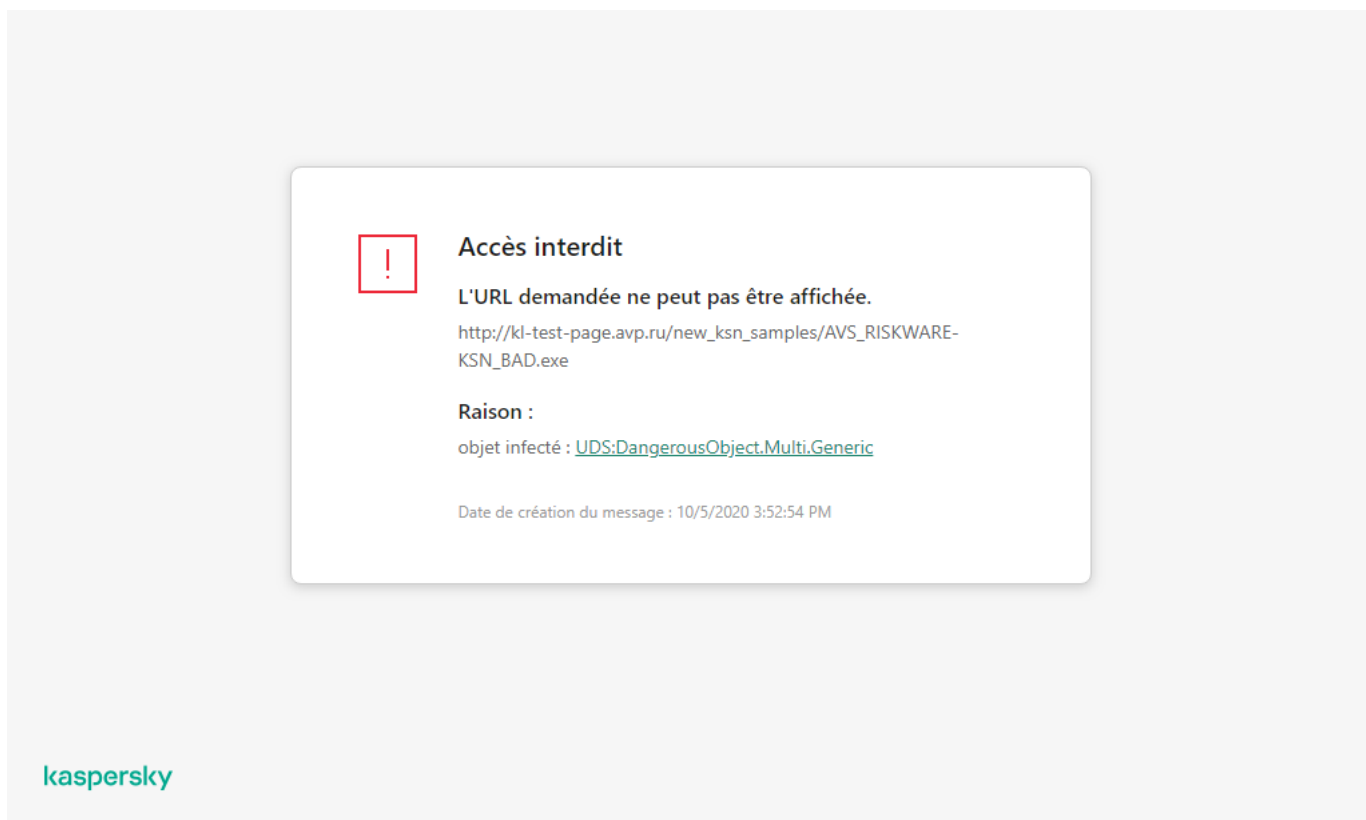
| | |
|---|---|
| <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Intelligente. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse un objet sur la base de l'analyse des opérations exécutées sur l'objet. Par exemple, dans le cas d'un document Microsoft Office, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.</p> <p>À l'ouverture et en cas de modification. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets chaque fois qu'il y a une tentative de les ouvrir ou de les modifier.</p> <p>À l'accès. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets uniquement lors des tentatives d'ouverture.</p> <p>À l'exécution. Il s'agit du mode d'analyse dans le cadre duquel le module Protection contre les fichiers malicieux analyse les objets uniquement lors des tentatives d'exécution.</p> |
| <p>Technologie iSwift</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.</p> |
| <p>Technologie iChecker</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).</p> |
| <p>Suspendre la Protection contre les fichiers malicieux</p> <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Cela met temporairement et automatiquement en pause le fonctionnement de la Protection contre les fichiers malicieux à l'heure spécifiée ou lorsque vous travaillez avec les applications spécifiées.</p> |

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants via Internet. Il bloque également l'accès aux sites Internet malveillants et de phishing. Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.

Kaspersky Endpoint Security analyse le trafic HTTP, HTTPS et FTP. Kaspersky Endpoint Security analyse les adresses Internet et IP. Vous pouvez [définir les ports que Kaspersky Endpoint Security va surveiller](#) ou sélectionner tous les ports.

Pour contrôler le trafic HTTPS, vous devez [activer l'analyse des connexions sécurisées](#).

Lorsqu'un utilisateur tente d'ouvrir un site Internet malveillant ou de phishing, Kaspersky Endpoint Security bloque l'accès et affiche un avertissement (cf. figure ci-dessous).



Message sur l'interdiction de l'accès à la page Internet

Paramètres du module Protection contre les menaces Internet

| Paramètre | Description |
|---|---|
| Niveau de sécurité <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les menaces Internet. Ces groupes de paramètres stockés dans l'application sont appelés <i>niveaux de sécurité</i> :</p> <ul style="list-style-type: none">• Élevé. Niveau de sécurité du trafic Internet auquel le module Protection contre les menaces Internet garantit l'analyse maximale du trafic Internet transmis à l'ordinateur via les protocoles HTTP et FTP. Le module Protection contre les menaces Internet analyse en détail tous les objets du trafic Internet à l'aide de la sélection complète des bases de l'application et réalise également une analyse heuristique très minutieuse.• Recommandé. Le niveau de sécurité du trafic Internet qui garantit l'équilibre optimum entre les performances de Kaspersky Endpoint Security et la sécurité du trafic Internet. Le module Protection contre les menaces Internet exécute l'analyse heuristique au niveau de valeur moyenne. Le niveau de sécurité du trafic Internet recommandé par les experts de Kaspersky. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Faible. Niveau de sécurité du trafic Internet dont les paramètres garantissent l'analyse la plus rapide. Le module Protection contre les menaces Internet exécute l'analyse heuristique au niveau de valeur superficielle. |
| Action en cas de détection d'une menace | <p>Interdire le téléchargement. Si cette action est sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche un message dans le navigateur.</p> <p>Notifier. Si cette option est sélectionnée, Kaspersky Endpoint Security permet, en cas de détection d'un objet infecté dans le trafic Internet, de télécharger cet objet sur l'ordinateur et ajoute les informations sur l'objet infecté à la liste des menaces actives.</p> |
| Vérifier l'adresse Internet en fonction de la base des adresses Internet de phishing <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>L'analyse des liens pour déterminer s'ils sont inclus dans la base de données des adresses Internet malveillantes vous permet de suivre les sites Internet qui ont été ajoutés à la liste de refus. La base des adresses Internet malveillantes est créée par les experts de Kaspersky. Elle est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security.</p> |
| Utiliser l'analyse heuristique <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lorsque le trafic Internet est analysé à la recherche de virus et d'autres applications qui présentent une menace, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| Vérifiez l'URL par rapport à la base de données des URL de phishing <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>La base des adresses Internet de phishing comprend les URL connues actuellement qui sont utilisées lors des attaques de phishing. Les experts de Kaspersky ajoutent à la base des adresses Internet de phishing fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). La base des adresses Internet de phishing est livrée avec le kit de distribution de l'application et enrichie lors de la mise à jour des bases de données de Kaspersky Endpoint Security.</p> |
| Ne pas analyser le trafic Internet en provenance | <p>Si la case est cochée, le module Protection contre les menaces Internet n'analyse pas le contenu des pages Internet/des sites Internet dont les adresses figurent dans la liste des URL de confiance. Vous pouvez ajouter à la liste des URL de confiance une adresse</p> |

des adresses
URL de
confiance

particulière d'une page Internet/d'un site Internet ou le masque de l'adresse de la page Internet/du site Internet.

Protection contre les menaces par emails

Le module Protection contre les menaces par emails analyse les pièces jointes des messages entrants et sortants à la recherche d'éventuels virus et d'autres programmes présentant une menace. Le module analyse également les messages à la recherche de liens malveillants et de phishing. Par défaut, le module Protection contre les menaces par emails se trouve en permanence dans la RAM de l'ordinateur et analyse tous les messages reçus ou envoyés à l'aide des protocoles POP3, SMTP, IMAP, NNTP ou dans le client de messagerie Microsoft Office Outlook (MAPI). Le module protège l'ordinateur à l'aide de bases antivirus, du [service cloud Kaspersky Security Network](#) et d'une analyse heuristique.

Le module Protection contre les menaces par emails n'analyse pas les messages si le client de messagerie est ouvert dans un navigateur.

Lorsqu'un fichier malveillant est détecté dans une pièce jointe, Kaspersky Endpoint Security change l'objet du message comme suit : [Message infecté] <objet du message> ou [Objet infecté supprimé] <objet du message>.

Le module interagit avec les clients de messagerie installés sur l'ordinateur. Pour le client de messagerie Microsoft Office Outlook, il existe une [extension avec des paramètres complémentaires](#). L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

Paramètres du module Protection contre les menaces par emails

| Paramètre | Description |
|---|--|
| Niveau de sécurité <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i> | <p>Kaspersky Endpoint Security peut appliquer différents groupes de paramètres pour le module Protection contre les menaces par emails. Ces groupes de paramètres stockés dans l'application sont appelés <i>niveaux de sécurité</i> :</p> <ul style="list-style-type: none">• Élevé. Niveau de sécurité du courrier auquel la Protection contre les menaces par emails garantit le contrôle maximal des messages. Le module Protection contre les menaces par emails analyse les messages électroniques entrants et sortants et effectue également une analyse heuristique minutieuse. Un niveau de sécurité Élevé est recommandé pour un travail en environnement dangereux. Parmi les environnements dangereux, citons la connexion à un service de messagerie en ligne gratuit depuis le réseau domestique dépourvu de protection centralisée du courrier.• Recommandé. Le niveau de sécurité du courrier qui garantit l'équilibre optimum entre les performances de Kaspersky Endpoint Security et la sécurité du courrier. Le module Protection contre les menaces par emails analyse l'ensemble des messages électroniques entrants et sortants et réalise également une analyse heuristique au niveau moyen. Le niveau de sécurité du courrier recommandé par les experts de Kaspersky.• Faible. Le niveau de sécurité du courrier auquel le module Protection contre les menaces par emails analyse uniquement les messages électroniques entrants et réalise également une analyse heuristique superficielle. Il n'analyse pas les archives jointes aux messages |

| | |
|---|---|
| | <p>électroniques. À ce niveau de sécurité du courrier, le module Protection contre les menaces par emails réalise l'analyse la plus rapide des messages électroniques et utilise le minimum de ressources du système d'exploitation. Le niveau de sécurité Faible pour la protection du courrier est recommandé pour les environnements bien protégés. Exemple de cet environnement : réseau local d'entreprise avec un système centralisé de protection du courrier.</p> |
| <p>Action en cas de détection d'une menace</p> | <p>Désinfecter ; supprimer si la désinfection est impossible. Si un objet infecté est détecté dans un message entrant ou sortant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. L'utilisateur pourra accéder à un message avec une pièce jointe qui ne présente aucun danger. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security le supprime. Kaspersky Endpoint Security ajoute des informations relatives à l'action réalisée dans l'objet du message: [Objet infecté supprimé] <objet du message>.</p> <p>Désinfecter ; bloquer si la désinfection est impossible. Si un objet infecté est détecté dans un message entrant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. L'utilisateur pourra accéder à un message avec une pièce jointe qui ne présente aucun danger. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security ajoute un avertissement à l'objet du message: [Message infecté] <objet du message>. L'utilisateur pourra accéder au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, Kaspersky Endpoint Security tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, Kaspersky Endpoint Security bloque l'envoi du message et le client de messagerie affiche une erreur.</p> <p>Interdire. Si un objet infecté est détecté dans un message entrant, Kaspersky Endpoint Security ajoute un avertissement à l'objet du message: [Message infecté] <objet du message>. L'utilisateur pourra accéder au message avec la pièce jointe d'origine. Si un objet infecté est détecté dans un message sortant, Kaspersky Endpoint Security bloque l'envoi du message et le client de messagerie affiche une erreur.</p> |
| <p>Zone de protection <i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>La <i>Zone d'analyse</i> comprend les objets que le module vérifie lorsqu'il est exécuté : Analyser les messages entrants et sortants ou Analyser uniquement les messages entrants.</p> <p>Afin de protéger vos ordinateurs, il vous suffit de scanner les messages entrants. Vous pouvez activer l'analyse des messages sortants pour empêcher l'envoi de fichiers infectés dans les archives. Vous pouvez également activer l'analyse des messages sortants si vous souhaitez empêcher l'envoi de fichiers dans des formats particuliers, tels que des fichiers audio et Vidéo, par exemple.</p> |
| <p>Analyser le trafic POP3/SMTP/NNTP/IMAP</p> | <p>La case active/désactive l'analyse par le module Protection contre les menaces par emails du trafic de messagerie transmis par les protocoles POP3, SMTP, NNTP et IMAP.</p> |
| <p>Connecter l'extension Microsoft Outlook</p> | <p>Si la case est activée, l'analyse des messages électroniques transmis via les protocoles POP3, SMTP, NNTP, IMAP est activée au niveau de l'extension intégrée à Microsoft Outlook.</p> <p>En cas d'analyse du courrier à l'aide d'une extension pour Microsoft Outlook, il est recommandé d'utiliser le mode de mise en cache Exchange (Cached Exchange Mode). Vous pouvez obtenir tous les détails sur le mode Exchange mis en cache et sur ses recommandations d'utilisation dans la base de connaissances de Microsoft.</p> |
| <p>Analyse heuristique</p> | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de</p> |

| | |
|---|---|
| <p><i>(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| <p>Analyser les archives jointes</p> | <p>Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE.</p> <div data-bbox="525 497 1493 828" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Si pendant l'analyse, Kaspersky Endpoint Security détecte un mot de passe pour une archive dans le texte du message, ce mot de passe sera utilisé pour analyser le contenu de l'archive à la recherche d'applications malveillantes. Dans ce cas, le mot de passe n'est pas enregistré. Une archive est décompressée pendant l'analyse. Si une erreur d'application se produit pendant le processus de décompression, vous pouvez supprimer manuellement les fichiers décompressés qui sont enregistrés dans le chemin suivant : %systemroot%\temp. Les fichiers ont le préfixe PR.</p> </div> |
| <p>Analyser les fichiers joints aux formats Office</p> | <p>Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE.</p> |
| <p>Ne pas analyser les archives de plus de X Mo</p> | <p>Si la case est cochée, le module Protection contre les menaces par emails exclut de l'analyse les archives jointes aux messages électroniques dont la taille est supérieure à la valeur définie. Si la case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques.</p> |
| <p>Ne pas analyser les archives pendant plus de X s.</p> | <p>Si la case est cochée, la durée d'analyse des archives jointes aux emails est limitée à la valeur définie.</p> |
| <p>Filtre des pièces jointes</p> | <div data-bbox="525 1379 1493 1469" style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Le filtre des pièces jointes ne s'applique pas aux emails sortants.</p> </div> <p>Désactiver le filtre. Si cette option est sélectionnée, le module Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques.</p> <p>Renommer les types de pièces jointes indiqués. Si vous sélectionnez cette option, le module Protection contre les menaces par emails remplacera le dernier caractère d'extension trouvé dans les fichiers joints des types spécifiés par le caractère de soulignement (par exemple, pièce jointe.doc_). Ainsi, dans l'ordre d'ouvrir le fichier, l'utilisateur doit renommer le fichier.</p> <p>Supprimer les types de pièces jointes indiqués. Si cette option est sélectionnée, le module Protection contre les menaces par emails supprime les fichiers joints des types de messages électroniques indiqués.</p> <p>Vous pouvez indiquer les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.</p> |

Protection contre les menaces réseau

Le module Protection contre les menaces réseau (Intrusion Detection System en anglais) recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque la connexion réseau issue de l'ordinateur attaquant.

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Endpoint Security. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la [mise à jour des bases et des modules de l'application](#).

Paramètres du module Protection contre les menaces réseau

| Paramètre | Description |
|---|--|
| Détecter les attaques par balayage des ports et par inondation des réseaux | <p>L'<i>inondation des réseaux</i> est une attaque contre les ressources réseau d'une organisation (comme les serveurs Internet). Cette attaque consiste à envoyer un grand nombre de requêtes pour surcharger la bande passante des ressources réseau. Lorsque cela se produit, les utilisateurs ne peuvent pas accéder aux ressources réseau de l'organisation.</p> <p>Une attaque par <i>analyse des ports</i> consiste à analyser les ports UDP, les ports TCP et les services réseau de l'ordinateur. Cette attaque permet à l'attaquant d'identifier le degré de vulnérabilité de l'ordinateur avant de mener des types d'attaques réseau plus dangereux. L'analyse des ports permet également au pirate informatique d'identifier le système d'exploitation de l'ordinateur et de sélectionner les attaques réseau appropriées pour ce système d'exploitation.</p> <p>Si cette case est cochée, Kaspersky Endpoint Security surveille le trafic réseau pour détecter ces attaques. Lorsqu'une attaque est détectée, l'application filtre et bloque le trafic associé à l'attaque. De cette façon, si une attaque par inondation des réseaux est lancée contre l'ordinateur, l'application réduit la charge sur la ressource attaquée. Si une attaque d'analyse des ports est lancée contre l'ordinateur, Kaspersky Endpoint Security empêche les fuites de données sur l'ordinateur.</p> <p>Vous pouvez désactiver la détection de ces types d'attaques au cas où certaines de vos applications autorisées effectueraient des opérations typiques de ces types d'attaques. Cela permettra d'éviter les fausses alertes.</p> |
| Bloquer l'ordinateur à l'origine de l'attaque pendant X minutes | <p>Si la case est cochée, le module Prévention des intrusions ajoute l'ordinateur à l'origine de l'attaque à la liste des ordinateurs à bloquer. Cela signifie que le module Protection contre les menaces réseau bloque la connexion réseau avec l'ordinateur attaquant après la première tentative d'attaque réseau pendant la durée indiquée. Ce groupe protège automatiquement l'ordinateur de l'utilisateur contre d'éventuelles attaques réseau futures à partir de la même adresse.</p> <p>Vous pouvez consulter la liste des groupes dans la fenêtre de l'outil Surveillance du réseau.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>Kaspersky Endpoint Security efface la liste du groupe lorsque l'application est redémarrée et lorsque les paramètres de la Protection contre les menaces réseau sont modifiés.</p></div> |
| Exclusions | <p>La liste contient les adresses IP à l'origine des attaques réseau que le module Prévention des intrusions ne bloque pas.</p> <p>Kaspersky Endpoint Security n'ajoute pas au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions.</p> |
| Protection | <p>Une <i>attaque MAC spoofing</i> consiste à substituer l'adresses MAC de l'appareil réseau</p> |

contre le MAC Spoofing

(adaptateur réseau). Par conséquent, un individu malintentionné peut rediriger les données envoyées vers un appareil vers un autre et accéder à ces données. Kaspersky Endpoint Security permet de bloquer les attaques de type MAC Spoofing et de recevoir les notifications relatives aux attaques.

Firewall

Le pare-feu bloque les connexions non autorisées à l'ordinateur lorsque vous travaillez sur Internet ou sur un réseau local. De plus, le pare-feu contrôle l'activité des applications de l'ordinateur sur le réseau. Cela permet de protéger le réseau local de l'organisation contre le vol de données personnelles et d'autres attaques. Le module assure la protection de l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et de *règles réseau* prédéfinies.

L'Agent d'administration est utilisé dans le cadre de l'interaction avec Kaspersky Security Center. Le pare-feu crée automatiquement les règles réseau nécessaires au fonctionnement de l'application et de l'Agent d'administration. En conséquence, le pare-feu ouvre plusieurs ports sur l'ordinateur. Les ports qui sont ouverts dépendent du rôle de l'ordinateur (par exemple, le point de distribution). Pour en savoir plus à propos des ports qui seront ouverts sur l'ordinateur, consultez la rubrique [Aide de Kaspersky Security Center](#).

Règles réseau

Vous pouvez configurer les règles réseau aux niveaux suivants :

- *Règles pour les paquets réseau*. Elles sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Kaspersky Endpoint Security possède des règles de paquets réseau prédéfinies avec les autorisations recommandées par les experts de Kaspersky.
- *Règles réseau des applications* Elles sont utilisées pour limiter l'activité réseau d'une application spécifique. Elles tiennent compte non seulement des caractéristiques du paquet réseau, mais aussi de l'application spécifique destinataire ou expéditeur de ce paquet réseau.

Le contrôle de l'accès des applications aux ressources du système d'exploitation, aux processus et aux données personnelles est assuré par le [module Prévention des intrusions](#) avec l'aide des *autorisations de l'application*.

Lors du premier lancement de l'application, le pare-feu exécute les actions suivantes :

1. Il vérifie la sécurité de l'application à l'aide des bases antivirus chargées.
2. Il vérifie la sécurité de l'application dans Kaspersky Security Network.

Pour garantir le fonctionnement le plus efficace du Pare-feu, il est conseillé de [participer au Kaspersky Security Network](#).

3. Il place l'application dans un des *groupes de confiance* : de confiance, restrictions faibles, restrictions élevées, douteuses.

Le [groupe de confiance définit les privilèges](#) que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications. Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction du niveau de danger que cette application peut représenter pour l'ordinateur.

Kaspersky Endpoint Security place l'application dans un groupe de confiance pour les modules Pare-feu et Prévention des intrusions. Vous ne pouvez pas modifier le groupe de confiance uniquement pour le Pare-feu ou la Prévention des intrusions.

Si vous avez refusé de participer au KSN ou s'il n'y a pas de réseau, Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction des [paramètres du module Prévention des intrusions](#). Après la récupération des données sur la réputation de l'application dans KSN, le groupe de confiance peut être modifié automatiquement.

4. Il bloque l'activité réseau de l'application en fonction du groupe de confiance. Par exemple, les applications du groupe de confiance Restrictions élevées ne peuvent établir aucune connexion réseau.

Lors du prochain démarrage de l'application, Kaspersky Endpoint Security vérifie l'intégrité de l'application. Si l'application n'a pas été modifiée, le module lui applique les règles réseau en vigueur. En cas de modification de l'application, Kaspersky Endpoint Security l'analyse comme s'il s'agissait de sa première exécution.

Priorités des règles réseau

Chaque règle a une priorité. Plus haut se situe une règle dans la liste, plus haute est sa priorité. Si l'activité réseau est ajoutée à plusieurs règles, le Pare-feu réglemente l'activité réseau selon la règle affichant la priorité la plus élevée.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau pour les applications. Si des règles pour les paquets réseau et des règles réseau pour les applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Les règles réseau des applications fonctionnent comme suit : une règle réseau des applications comprend les règles d'accès selon l'état du réseau : *public*, *local* ou *fiable*. Par exemple, pour le groupe de confiance Restrictions élevées, toute activité réseau de l'application dans les réseaux de n'importe quel état est interdite. Si une règle réseau est définie pour une application individuelle (application parent), les processus enfants d'autres applications seront exécutés conformément à la règle réseau de l'application parent. S'il n'y a pas de règle réseau pour l'application, les processus enfant seront exécutés conformément à la règle d'accès aux réseaux du groupe de confiance.

Par exemple, vous avez interdit toute activité réseau de toutes les applications quel que soit l'état du réseau, sauf pour le navigateur X. Si vous lancez l'installation du navigateur Y (processus enfant) dans le navigateur X (processus parent), le programme d'installation du navigateur Y aura accès au réseau et téléchargera les fichiers requis. Après l'installation, le navigateur Y se verra refuser toutes les connexions réseau conformément aux paramètres du pare-feu. Pour interdire l'activité réseau au programme d'installation du navigateur Y en tant que processus enfant, vous devez ajouter une règle réseau pour le programme d'installation du navigateur Y.

États des connexions réseau.

Le Pare-feu permet de surveiller l'activité du réseau en fonction de l'état de la connexion réseau. Kaspersky Endpoint Security obtient l'état de la connexion réseau via le système d'exploitation de l'ordinateur. L'état de la connexion réseau dans le système d'exploitation est défini par l'utilisateur lors de la configuration de la connexion. Vous pouvez [modifier l'état de la connexion réseau dans les paramètres de Kaspersky Endpoint Security](#). Le Pare-feu contrôle l'activité réseau en fonction de l'état du réseau dans les paramètres de Kaspersky Endpoint Security, et non pas du système d'exploitation.

Il existe les états suivant de la connexion réseau :

- **Réseau public.** Le réseau n'est pas protégé par des logiciels antivirus, des pare-feu, des filtres (par exemple, le Wi-Fi dans un café). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur d'accéder aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur. Le Pare-feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.

Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.

- **Réseau local.** Réseau pour les utilisateurs dont l'accès est limité aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).
- **Réseau de confiance.** Réseau sûr dont l'utilisation n'expose pas l'ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état n'importe quelle activité réseau dans le cadre de ce réseau.

Paramètres du module Pare-feu

| Paramètre | Description |
|---------------------------------------|--|
| Règles pour les paquets réseau | <p>Tableau contenant la liste des règles pour les paquets réseau. Règles pour les paquets réseau sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné.</p> <p>Le tableau reprend les règles préinstallées pour les paquets réseau qui sont recommandées par les experts de Kaspersky pour une protection optimale du trafic réseau des ordinateurs sous l'administration des systèmes d'exploitation Microsoft Windows.</p> <p>Le Pare-feu établit une priorité d'exécution pour chaque règle pour le paquet réseau. Pare-feu traite les règles pour les paquets réseau selon leur ordre d'apparition dans la liste des pour les paquets réseau haut/bas. Le Pare-feu trouve dans la liste la première règle pour le paquet réseau convenant pour la connexion réseau et exécute son action : autorise ou bloque l'activité réseau. Ensuite, le Pare-feu ignore toutes les règles pour les paquets réseau suivants pour cette connexion réseau.</p> <p>Les règles pour les paquets réseau ont priorité sur les règles réseau pour les applications.</p> |
| Connexions réseau | <p>Le tableau qui contient les informations sur les connexions réseau que le Pare-feu a détectées sur l'ordinateur de l'utilisateur.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>Le réseau Internet reçoit par défaut l'état <i>Réseau public</i>. Vous ne pouvez pas modifier l'état du réseau Internet.</p> </div> |
| Règles réseau | <p>Annexes</p> <p>Tableau des applications contrôlées par le module Pare-feu. Les applications sont réparties en groupes de confiance. Le groupe de confiance définit les privilèges que Kaspersky Endpoint Security utilise pour contrôler l'activité réseau des applications.</p> <p>Vous pouvez sélectionner une application dans une liste unique de l'ensemble des applications installées sur les ordinateurs régis par la stratégie et ajouter l'application à un groupe de confiance.</p> <p>Règles réseau</p> <p>Le tableau qui contient les règles des applications qui appartiennent au groupe de confiance. Conformément à ces règles, le Pare-feu règle l'activité réseau pour les applications.</p> |

Le tableau reprend les règles réseau prédéfinies recommandées par les experts de Kaspersky. Ces règles réseau ont été ajoutées pour protéger de manière optimale le trafic réseau des ordinateurs tournant sous des systèmes d'exploitation Windows. Il n'est pas possible de supprimer les règles réseau prédéfinies.

Protection BadUSB

Certains virus modifient l'application interne des appareils USB afin que le système d'exploitation considère l'appareil USB comme un clavier. Par conséquent, le virus peut exécuter des commandes sous votre compte d'utilisateur, par exemple, pour télécharger des logiciels malveillants.

Le module Protection BadUSB permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier.

Quand un appareil USB est connecté à l'ordinateur et que le système d'exploitation le reconnaît comme étant un clavier, l'application génère un code numérique et invite l'utilisateur à le saisir à partir de ce clavier ou à l'aide d'[un clavier numérique, si ce dernier est disponible](#) (cf. ill. ci-après). C'est ce qu'on appelle l'autorisation du clavier.

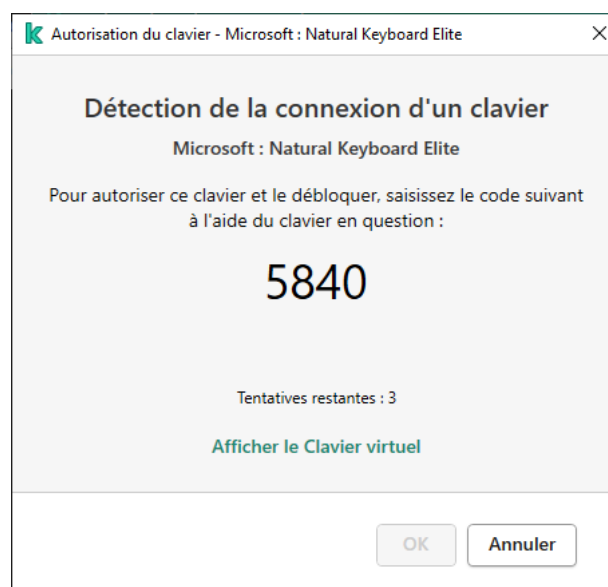
Si le code est saisi correctement, l'application enregistre les paramètres d'identification VID/PID du clavier et le numéro de port utilisé pour la connexion dans la liste des claviers autorisés. Il ne sera pas nécessaire d'autoriser à nouveau le clavier lors de la prochaine connexion ou suite au redémarrage du système d'exploitation.

Par contre, si vous connectez un clavier autorisé à un autre port USB, l'application sollicitera à nouveau l'autorisation.

Si le code numérique n'est pas saisi correctement, l'application crée un autre code. Le nombre maximum de tentatives de saisie est limité à trois. Après trois tentatives infructueuses ou si la fenêtre **Autorisation de clavier** <nom du clavier> est fermée, l'application bloque la saisie à l'aide de ce clavier. Si le clavier est reconnecté ou si le système d'exploitation redémarre, l'application proposera à nouveau d'autoriser le clavier.

L'application autorise l'utilisation du clavier autorisé et bloque tout clavier qui n'a pas réussi l'autorisation.

Le module Protection BadUSB n'est pas installé par défaut. Si vous avez besoin du module Protection BadUSB, vous pouvez l'ajouter dans les propriétés du [paquet d'installation](#) avant d'installer l'application ou [modifier la sélection des modules de l'application](#) après avoir installé l'application.



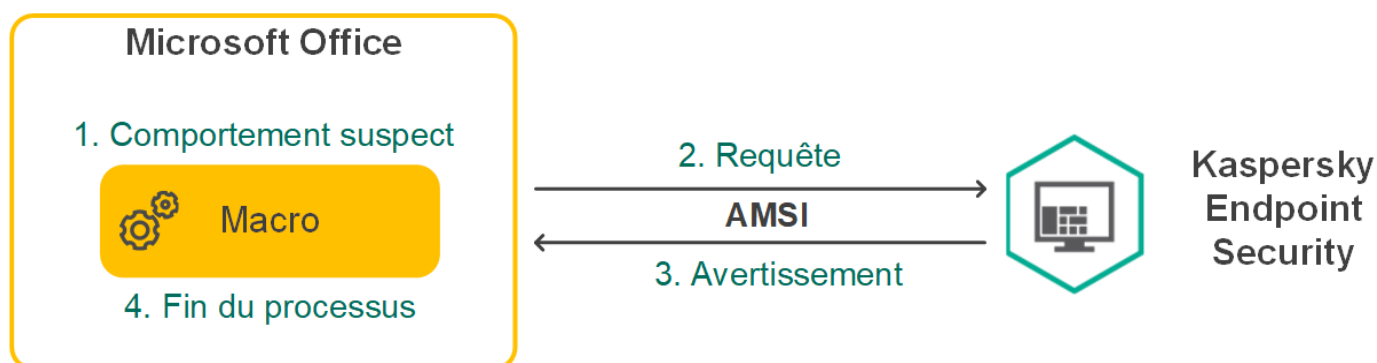
Paramètres du module Protection BadUSB

| Paramètre | Description |
|---|---|
| Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB | Si la case est cochée, l'application autorise l'utilisation d'un clavier virtuel pour autoriser l'appareil USB à partir duquel la saisie du code d'autorisation est impossible. |

Protection AMSI

Le module de la protection AMSI est prévu pour la prise en charge de l'interface Antimalware Scan Interface de Microsoft. *L'interface AMSI (Antimalware Scan Interface)* permet aux applications tierces compatibles avec AMSI d'envoyer des objets (par exemple, des scripts PowerShell) à Kaspersky Endpoint Security pour une analyse supplémentaire et de recevoir les résultats de l'analyse de ces objets. Les applications tierces peuvent être, par exemple, des applications Microsoft Office (cf. ill. ci-dessous). Pour en savoir plus sur l'interface AMSI, consultez la [documentation de Microsoft](#).

La protection AMSI peut uniquement détecter une menace et la signaler à une application tierce. Après la réception de la notification sur la menace, l'application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt le fonctionnement).



Exemple de fonctionnement d'AMSI

Le module de la protection AMSI peut rejeter la demande d'une application tierce, par exemple, si cette application a dépassé le nombre maximum de demandes pour l'intervalle défini. Kaspersky Endpoint Security envoie les informations relatives au rejet de la demande de l'application tierce au Serveur d'administration. Le module de la protection AMSI ne rejette pas les demandes des applications tierces pour lesquelles la [case Ne pas bloquer l'interaction avec le fournisseur de protection AMSI](#) a été cochée

La protection AMSI est disponible pour les systèmes d'exploitation suivants pour postes de travail et serveurs :

- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise ;
- Windows Server 2016 Essentials/Standard/Datacenter ;
- Windows Server 2019 Essentials/Standard/Datacenter.

Paramètres du module Fournisseur de protection AMSI

| Paramètre | Description |
|------------------------------|---|
| Analyser les archives | Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE. |

| | |
|---|--|
| Analyser les paquets de distribution | La case active/désactive l'analyse des paquets de distribution des logiciels tiers. |
| Analyser les fichiers aux formats Microsoft Office | Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. |
| Ne pas décompresser les fichiers composés de grande taille | <p>Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie.</p> <p>Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille.</p> <p>Kaspersky Endpoint Security analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.</p> |

Protection contre les Exploits

Le module Protection contre les Exploits surveille le code qui exploite les vulnérabilités d'un ordinateur pour obtenir des privilèges d'administrateur ou effectuer des actions malveillantes de la part de l'exploit. Les exploits, par exemple, utilisent l'attaque par débordement de tampon. Dans ce cas, l'exploit envoie un gros volume de données à l'application vulnérable. Lors du traitement de ces données, l'application vulnérable exécute un code malveillant. Suite à cette attaque, un exploit pourrait lancer l'installation non autorisée d'une application malveillante.

Si l's'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier ou le signale à l'utilisateur.

Paramètres du module Protection contre les Exploits

| Paramètre | Description |
|--|--|
| En cas de détection d'un exploit | <ul style="list-style-type: none"> • Bloquer l'opération. Si vous choisissez cette option, Kaspersky Endpoint Security bloque toutes les actions de cet exploit après la détection de ce dernier. • Notifier. Si vous choisissez cette option, en cas de détection d'un exploit, Kaspersky Endpoint Security ne bloque pas l'action de l'exploit et ajoute les informations relatives à l'exploit dans la liste des menaces actives. |
| Activer la protection de la mémoire des processus système | Si le commutateur est activé, Kaspersky Endpoint Security bloque les processus tiers qui tentent d'accéder à la mémoire des processus système. |

Détection comportementale

Le module Détection comportementale récupère des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent intervenir avec plus d'efficacité.

Le module Détection comportementale utilise des modèles de comportement d'applications dangereux. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Endpoint Security exécute la réaction choisie. La fonction de Kaspersky Endpoint Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

| Paramètre | Description |
|--|--|
| En cas de détection de l'activité d'une application malveillante | <ul style="list-style-type: none"> • Supprimer le fichier. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application. • Interrompre l'application. Si cette option est sélectionnée, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application. • Notifier. Si vous avez choisi cette option, Kaspersky Endpoint Security, en cas de détection d'une activité malveillante de l'application, n'arrête pas cette application, mais ajoute les informations relatives à l'activité malveillante de cette application à la liste des menaces actives. |
| Activer la protection des dossiers partagés contre le chiffrement externe | <p>Si le commutateur est activé, Kaspersky Endpoint Security analyse l'activité dans les dossiers partagés. Si l'activité correspond à un modèle de comportement dangereux caractéristique du chiffrement externe, Kaspersky Endpoint Security exécute l'action choisie.</p> <div data-bbox="389 904 1493 1099" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>La protection contre les tentatives de chiffrement externe offerte par Kaspersky Endpoint Security porte uniquement sur les fichiers qui se trouvent sur des supports dotés d'un système de fichiers NTFS et qui ne sont pas chiffrés à l'aide du système EFS.</p> </div> <ul style="list-style-type: none"> • Notifier. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté une tentative de modification des fichiers dans les dossiers partagés, ajoute les informations relatives à cette tentative de modification des fichiers dans les dossiers partagés à la liste des menaces actives. • Bloquer la connexion. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté une tentative de modification des fichiers dans les dossiers partagés, bloque l'activité réseau de l'ordinateur à l'origine de la modification et crée des copies de sauvegarde des fichiers modifiés. <div data-bbox="389 1494 1493 1653" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Si le module Réparation des actions malicieuses a été activé et que l'option Bloquer la connexion a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.</p> </div> |
| Bloquer la connexion pendant X minutes | <p>Durée pendant laquelle Kaspersky Endpoint Security bloque l'activité réseau d'un ordinateur distant qui chiffre les dossiers partagés.</p> |
| Exclusions | <p>La liste des ordinateurs pour lesquels les tentatives de chiffrement des dossiers partagés ne sont pas traquées.</p> |

Pour utiliser la liste des exclusions d'ordinateurs de la protection des dossiers partagés contre le chiffrement externe, vous devez activer l'audit d'ouverture de session dans la stratégie d'audit de sécurité Windows. Par défaut, l'audit d'ouverture de session est désactivé. Pour en savoir plus sur la stratégie d'audit de sécurité de Windows, consultez le [site de Microsoft](#)).

Prévention des intrusions

Le module Prévention des intrusions (en anglais, HIPS – Host Intrusion Prevention System) empêche l'exécution des actions dangereuses pour le système et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles. Le module assure la protection de l'ordinateur à l'aide de bases antivirus et du service cloud Kaspersky Security Network.

Le module contrôle le fonctionnement des applications à l'aide des *privileges des applications*. Les privilèges des applications incluent les paramètres d'accès suivants :

- l'accès aux ressources du système d'exploitation (par exemple, les options de démarrage automatique, les clés de registre) ;
- l'accès aux données personnelles (par exemple, les fichiers, les applications).

L'activité réseau des applications est contrôlée par le [pare-feu](#) à l'aide de *règles réseau*.

Lors du premier lancement de l'application, le module Prévention des intrusions exécute les actions suivantes :

1. Il vérifie la sécurité de l'application à l'aide des bases antivirus chargées.
2. Il vérifie la sécurité de l'application dans Kaspersky Security Network.

Pour contribuer au fonctionnement plus efficace du module Prévention des intrusions, il est conseillé de [participer au Kaspersky Security Network](#).

3. Il place l'application dans un des *groupes de confiance* : de confiance, restrictions faibles, restrictions élevées, douteuses.

Le [groupe de confiance définit les privilèges](#) que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications. Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction du niveau de danger que cette application peut représenter pour l'ordinateur.

Kaspersky Endpoint Security place l'application dans un groupe de confiance pour les modules Pare-feu et Prévention des intrusions. Vous ne pouvez pas modifier le groupe de confiance uniquement pour le Pare-feu ou la Prévention des intrusions.

Si vous avez refusé de participer au KSN ou s'il n'y a pas de réseau, Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction des [paramètres du module Prévention des intrusions](#). Après la récupération des données sur la réputation de l'application dans KSN, le groupe de confiance peut être modifié automatiquement.

4. Il bloque les actions de l'application en fonction du groupe de confiance. Par exemple, les applications du groupe de confiance Restrictions élevées n'ont pas accès aux modules du système d'exploitation.

Lors du prochain démarrage de l'application, Kaspersky Endpoint Security vérifie l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les privilèges des applications existants. En cas de modification de l'application, Kaspersky Endpoint Security l'analyse comme s'il s'agissait de sa première exécution.

Paramètres du module Prévention des intrusions

| Paramètre | Description |
|------------------------------------|--|
| Privilèges des applications | <p>Applications</p> <p>Tableau des applications contrôlées par le module Prévention des intrusions. Les applications sont réparties en groupes de confiance. Le groupe de confiance définit les privilèges que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications.</p> <p>Vous pouvez sélectionner une application dans une liste unique de l'ensemble des applications installées sur les ordinateurs régis par la stratégie et ajouter l'application à un groupe de confiance.</p> <p>Les privilèges d'accès de l'application figurent dans les tableaux suivants :</p> <ul style="list-style-type: none">• Fichiers et base de registre. Le tableau qui contient les privilèges d'accès des applications du groupe de confiance aux ressources du système d'exploitation et aux données personnelles.• Privilèges. Le tableau qui contient les privilèges d'accès des applications du groupe de confiance aux processus et aux ressources du système d'exploitation.• Règles réseau. Le tableau qui contient les règles des applications qui appartiennent au groupe de confiance. Conformément à ces règles, le Pare-feu règle l'activité réseau pour les applications. Le |

tableau reprend les règles réseau prédéfinies recommandées par les experts de Kaspersky. Ces règles réseau ont été ajoutées pour protéger de manière optimale le trafic réseau des ordinateurs tournant sous des systèmes d'exploitation Windows. Il n'est pas possible de supprimer les règles réseau prédéfinies.

Ressources protégées

Nom

Le tableau contient les ressources de l'ordinateur réparties en catégories. Le module Prévention des intrusions contrôle l'accès des autres programmes aux ressources de ce tableau.

La ressource peut être une catégorie de registre, un fichier ou un dossier, une clé de registre.

Applications

Tableau des applications contrôlées par le module Prévention des intrusions pour la ressource sélectionnée. Les applications sont réparties en groupes de confiance. Le groupe de confiance définit les privilèges que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications.

Groupe de confiance pour les applications lancées avant le démarrage de Kaspersky Endpoint Security

Le groupe de confiance dans lequel Kaspersky Endpoint Security placera les applications lancées avant Kaspersky Endpoint Security.

Mettre à jour les droits pour les applications précédemment inconnues de la base de données KSN

Si la case est cochée, le module Prévention des intrusions met à jour les privilèges des applications inconnues jusqu'alors à l'aide des bases Kaspersky Security Network.

Faire confiance aux applications dotées d'une signature numérique

Si la case est cochée, le module Prévention des intrusions place les applications dotées d'une signature numérique d'éditeurs de confiance dans le groupe De confiance.

Les *éditeurs de confiance* sont les éditeurs d'applications auxquels Kaspersky fait confiance. Vous pouvez également [ajouter manuellement le certificat de l'éditeur au stockage sécurisé des certificats](#).

| | |
|---|--|
| | <p>Si la case est décochée, le module Prévention des intrusions ne considère pas de telles applications comme des applications de confiance et détermine leur groupe de confiance sur la base d'autres paramètres.</p> |
| <p>Supprimer les droits des applications non lancées depuis plus de X jours</p> | <p>Si la case est cochée, Kaspersky Endpoint Security supprime automatiquement les informations relatives à l'application (groupe de confiance, privilèges d'accès) si les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> • Vous avez placé manuellement l'application dans un groupe de confiance ou vous avez configuré manuellement des privilèges d'accès. • L'application n'a plus été lancée depuis une durée déterminée. <p>Si le groupe de confiance et les privilèges sont déterminés automatiquement, Kaspersky Endpoint Security supprime les informations relatives à cette application après 30 jours. Il n'est pas possible de modifier la durée de conservation des informations relatives à l'application ou de désactiver la suppression automatique.</p> <p>Au prochain lancement de l'application, Kaspersky Endpoint Security l'examine comme au premier lancement.</p> |
| <p>Groupe de confiance pour les applications qui n'ont pas pu être attribuées à d'autres groupes</p> | <p>La liste déroulante dont les éléments déterminent le groupe de confiance dans lequel Kaspersky Endpoint Security va placer l'application inconnue.</p> <p>Vous avez le choix entre les options suivantes :</p> <ul style="list-style-type: none"> • Restrictions faibles. • Restrictions élevées. • Douteuses. |

Réparation des actions malicieuses

Le module Réparation des actions malicieuses permet à Kaspersky Endpoint Security d'exécuter le retour à l'état antérieur aux actions des applications malveillantes dans le système d'exploitation.

Lors de la restauration des actions du programme malveillant dans le système d'exploitation, Kaspersky Endpoint Security traite les types suivants d'activité de programme malveillant :

- **Activité de fichiers**

Kaspersky Endpoint Security réalise les opérations suivantes :

- suppression des fichiers exécutables créés par l'application malveillante (sur tous les supports, sauf les disques réseau) ;
- suppression des fichiers exécutables créés par les applications dans lesquelles une application malveillante s'est introduite ;
- restauration des fichiers modifiés ou supprimés par l'application malveillante.

La fonction de restauration est soumise à une [série de restrictions](#).

- **Activité sur la base de registre**

Kaspersky Endpoint Security réalise les opérations suivantes :

- suppression des sections et des clés de registre créées par l'application malveillante ;
- non-restauration des sections et clés de registre modifiées ou supprimées par l'application malveillante.

- **Activité système**

Kaspersky Endpoint Security réalise les opérations suivantes :

- arrêt des processus lancés par l'application malveillante ;
- arrêt des processus dans lesquels l'application malveillante s'est introduite ;
- non-rétablissement des processus arrêtés par l'application malveillante.

- **Activité réseau**

Kaspersky Endpoint Security réalise les opérations suivantes :

- interdiction de l'activité réseau de l'application malveillante ;
- interdiction de l'activité réseau des processus dans lesquels l'application malveillante s'est introduite.

L'annulation des actions de l'application malveillante peut être lancée par le module [Protection contre les fichiers malicieux](#), [Détection comportementale](#) ou lors de la [recherche de virus](#).

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cela n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau Kaspersky Security Network permet de récupérer ces données.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite. Si vous participez au Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la catégorie et la réputation des fichiers analysés, ainsi que sur la réputation des adresses Internet analysées.

L'utilisation de Kaspersky Security Network est volontaire. L'application propose d'utiliser le KSN pendant la configuration initiale de l'application. Vous pouvez commencer à utiliser le KSN ou arrêter de l'utiliser à n'importe quel moment.

Vous pouvez lire des informations plus détaillées sur l'envoi à Kaspersky, le stockage et la destruction des informations statistiques obtenues lors de l'utilisation de KSN dans la Déclaration de Kaspersky Security Network et sur le [site Internet de Kaspersky](#). Le fichier ksn_<ID de la langue>.txt qui contient la Déclaration de Kaspersky Security Network figure dans le [kit de distribution](#).

Pour réduire la charge sur les serveurs de KSN, les spécialistes de Kaspersky peuvent lancer des mises à jour de l'application qui désactivent temporairement ou limitent en partie la communication dans Kaspersky Security Network. Dans ce cas, l'état de la connexion à KSN dans l'interface de programme locale est *Inclus avec des restrictions*.

Infrastructure du KSN

Kaspersky Endpoint Security prend en charge les infrastructures KSN suivantes :

- Le *KSN global* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky Security Network et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques de Kaspersky.
- Le *KSN privé* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Endpoint Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KSN privé a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :
 - absence de connexion des postes de travail locaux à Internet ;
 - interdiction législative ou restriction imposée par la sécurité de l'entreprise sur l'envoi de données hors du pays ou hors du réseau local de l'organisation.

Par défaut, Kaspersky Security Center utilise le KSN global. Vous pouvez configurer l'utilisation du KSN privé dans la Console d'administration (MMC), dans Kaspersky Security Center 12 Web Console et dans la [ligne de commande](#). Il n'est pas possible de configurer l'utilisation du KSN privé dans Kaspersky Security Center Cloud Console.

Pour en savoir plus sur le fonctionnement du KSN local, reportez-vous à la *documentation de Kaspersky Private Security Network*.

KSN Proxy

Les ordinateurs des utilisateurs qui sont administrés par le Serveur d'administration de Kaspersky Security Center peuvent interagir avec KSN à l'aide du service KSN Proxy.

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur de l'utilisateur peut interroger KSN et transmettre à KSN des informations, même s'il n'a pas d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication avec le réseau externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Pour en savoir plus sur le service KSN Proxy consultez l'[aide de Kaspersky Security Center](#).

Paramètres de Kaspersky Security Network

| Paramètre | Description |
|---|--|
| Activer le mode étendu de KSN | <p>Le <i>mode étendu du KSN</i> est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Endpoint Security envoie des données supplémentaires à Kaspersky. Quelle que soit la position du commutateur, Kaspersky Endpoint Security utilise KSN pour détecter les menaces.</p> |
| Activer le mode Cloud | <p>Le <i>mode Cloud</i> est un mode de fonctionnement de l'application dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données antivirus. L'utilisation avec les bases antivirus allégées est garantie par Kaspersky Security Network. La version allégée des bases de données antivirus peut réduire de moitié la charge sur la mémoire vive de l'ordinateur. Si vous ne participez pas à Kaspersky Security Network ou si le mode cloud est désactivé, Kaspersky Endpoint Security télécharge la version complète des bases de données antivirus depuis les serveurs de Kaspersky.</p> <p>Si le commutateur est activé, Kaspersky Endpoint Security utilise la version allégée des bases antivirus, ce qui réduit la charge sur les ressources du système d'exploitation.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security télécharge la version allégée des bases antivirus lors de la première mise à jour après que la case a été cochée.</p></div> <p>Si le commutateur est désactivé, Kaspersky Endpoint Security utilise la version complète des bases antivirus.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>Kaspersky Endpoint Security télécharge la version complète des bases antivirus lors de la première mise à jour après que la case a été décochée.</p></div> |
| État de l'ordinateur en cas d'indisponibilité de KSN | <p>Liste déroulante dont les éléments déterminent l'état de l'ordinateur dans Kaspersky Security Center quand les serveurs KSN ne sont pas accessibles.</p> |

| | |
|---|---|
| <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | |
| Utiliser KSN Proxy <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | Si la case est cochée, Kaspersky Endpoint Security utilise le service KSN Proxy. Vous pouvez configurer les paramètres du service du proxy KSN dans les propriétés du Serveur d'administration. |
| Utiliser les serveurs de KSN lorsque KSN Proxy est inaccessible <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | Si la case est cochée, Kaspersky Endpoint Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent se trouver du côté de Kaspersky en cas d'utilisation du KSN global ou sur des serveurs en cas d'utilisation du KSN privé. |

Contrôle Internet

Le Contrôle Internet contrôle l'accès des utilisateurs aux ressources Internet. Il permet de réduire la consommation de données et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur essaie d'ouvrir un site Internet dont l'accès est limité par Contrôle Internet, Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement (cf. illustration ci-dessous).

Kaspersky Endpoint Security contrôle uniquement le trafic HTTP et HTTPS.

Pour contrôler le trafic HTTPS, vous devez [activer l'analyse des connexions sécurisées](#).

Outils d'administration de l'accès aux sites Internet

Contrôle Internet permet de configurer l'accès aux sites Internet des manières suivantes :

- **Catégorie du site Internet** La catégorisation des sites Internet est assurée par le service cloud Kaspersky Security Network, l'analyse heuristique ainsi qu'à l'aide d'une base de données de sites Internet connus (incluse dans les bases de données d'application). Par exemple, vous pouvez restreindre l'accès des utilisateurs à la catégorie "Réseaux sociaux" ou à d'autres catégories.
- **Types de données** Vous pouvez restreindre l'accès des utilisateurs aux données d'un site Internet et, par exemple, masquer les images. Kaspersky Endpoint Security détermine le type de données selon le format du fichier et non pas selon son extension.

Kaspersky Endpoint Security n'analyse pas les fichiers de tous les types au sein des archives. Par exemple, si des fichiers image figurent dans l'archive, Kaspersky Endpoint Security optera pour le type de données "Archives" au lieu de "Fichiers image".

- **Adresse distincte.** Vous pouvez saisir une adresse Internet ou [utiliser des masques](#).

Vous pouvez utiliser plusieurs modes de contrôle de l'accès aux sites Internet en même temps. Par exemple, vous pouvez limiter l'accès au type de données "Fichiers Office" uniquement pour la catégorie de sites Internet "Emails en ligne".

Règles d'accès aux ressources Internet

Le Contrôle Internet contrôle l'accès des utilisateurs aux sites Internet à l'aide de *règles d'accès*. Vous pouvez configurer les paramètres complémentaires suivants pour une règle d'accès à un site Internet :

- Utilisateurs qui seront soumis à la règle.
Par exemple, vous pouvez limiter l'accès à Internet via un navigateur pour tous les utilisateurs de l'entreprise, à l'exception du service informatique.
- Planification de l'application de la règle.
Par exemple, vous pouvez limiter l'accès à Internet via un navigateur uniquement pendant les heures ouvrables.

Priorités de règle d'accès

Chaque règle a une priorité. Plus haut se situe une règle dans la liste, plus haute est sa priorité. Si un site Internet est ajouté à plusieurs règles, Contrôle Internet utilise la règle dont la priorité est la plus élevée. Par exemple, Kaspersky Endpoint Security peut définir le portail de l'entreprise en tant que réseau social. Pour limiter l'accès aux réseaux sociaux et octroyer un accès au portail de l'entreprise, créez deux règles : une règle d'interdiction pour la catégorie de sites Internet "Réseaux sociaux" et une règle d'autorisation pour le portail de l'entreprise. La priorité de la règle d'accès au portail de l'entreprise doit être supérieure à celle de la règle d'accès aux réseaux sociaux.



Impossible d'ouvrir la page Internet demandée.

Adresse : <http://kaspersky.ru/>.

La page Internet est bloquée par la règle "kasp".

Raison : le site Internet appartient à la catégorie (aux catégories) de contenu "Contenu inconnu" et à la catégorie (aux catégories) de type de données "Données inconnues".

Ce site Internet est interdit dans l'entreprise. En cas de blocage par erreur et/ou s'il est nécessaire d'accéder au site Internet, contacter l'administrateur du réseau local de l'entreprise ([Demander l'accès](#)).

Date de création du message : 10/14/2020 1:07:28 AM



La page Internet sollicitée peut être dangereuse ou l'accès à celle-ci est interdit par la stratégie de l'entreprise.

Adresse : <http://kaspersky.ru/>.

La page Internet est bloquée par la règle "kasp".

Raison : le site Internet appartient à la catégorie (aux catégories) de contenu "Contenu inconnu" et à la catégorie (aux catégories) de type de données "Données inconnues".

Cliquez sur le lien <http://kaspersky.ru/> pour ouvrir la page Internet demandée.

Cliquez sur le lien http://kaspersky.ru/* pour accéder à tout le contenu du site Internet avec la page Internet demandée.

Cliquez sur le lien */*/kaspersky.ru/* pour accéder à tous les domaines existants du niveau marqué (inférieur ou égal au niveau) par un **.

L'accès aux sites Internet énumérés sera autorisé lors de la session en cours de l'application.

Si cet avertissement vous parvient par erreur, contactez l'administrateur du réseau local de l'entreprise ([Demander l'accès](#)).

Date de création du message : 10/14/2020 1:08:04 AM

Notifications du Contrôle Internet

Paramètres du module Contrôle Internet

| Paramètre | Description |
|-----------------------------------|---|
| Règles d'accès aux sites Internet | Liste des règles d'accès aux sites Internet. Chaque règle a une priorité. Plus haut se situe une règle dans la liste, plus haute est sa priorité. Si un site Internet est ajouté à plusieurs règles, Contrôle Internet utilise la règle dont la priorité est la plus élevée. |
| Règle par défaut | La <i>règle par défaut</i> est une règle d'accès aux sites Internet qui ne figurent dans aucune des règles. Les options suivantes existent : <ul style="list-style-type: none"> • Autoriser tout ce qui ne figure pas dans la liste des règles, également connue sous le mode liste de refus pour les sites Internet interdits. • Interdire tout ce qui ne figure pas dans la liste des règles, également connue sous le mode liste d'autorisation pour les sites Internet autorisés. |
| Modèles de messages | <ul style="list-style-type: none"> • Avertissement. Le champ de saisie contient un modèle de message qui s'affiche |

| | |
|--|---|
| | <p>lorsque la règle qui avertit de la tentative d'accès au site Internet déconseillé est appliquée.</p> <ul style="list-style-type: none"> • Message sur le blocage. Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui bloque l'accès au site Internet est appliquée. • Message à l'administrateur. Le champ de saisie contient le modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès au site Internet est intervenu par erreur. |
| <p>Enregistrer les données relatives aux visites des pages autorisées dans le journal</p> | <p>Kaspersky Endpoint Security enregistre les données relatives aux visites de tous les sites Internet, y compris les sites autorisés. Kaspersky Endpoint Security envoie les événements à Kaspersky Security Center, au journal local de Kaspersky Endpoint Security et au journal des événements Windows. Pour surveiller l'activité des utilisateurs sur Internet, il faut configurer les paramètres d'enregistrement des événements.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Il se peut que la surveillance de l'activité des utilisateurs sur Internet requiert davantage de ressources informatiques lors du déchiffrement du trafic HTTPS.</p> </div> |

Contrôle des appareils

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à l'ordinateur (par exemple, disques durs, caméra ou module Wi-Fi). Cela permet de protéger l'ordinateur contre l'infection lors de la connexion de ces appareils et de prévenir la perte ou la fuite de données.

Niveaux d'accès aux appareils

Le Contrôle des appareils gère l'accès aux niveaux suivants :

- **Type d'appareil.** Par exemple, imprimantes, disques amovibles, lecteurs CD/DVD.

Vous pouvez configurer l'accès des appareils de la manière suivante :

- Autoriser : ✓.
- Interdire : ⛔.
- Dépend du bus connexion (excepté Wi-Fi) : 🌐.
- Interdit, avec des exceptions (seulement Wi-Fi) : 🚫.
- **Bus de connexion.** Un *bus de connexion* est une interface qui permet de connecter des appareils à l'ordinateur (USB, FireWire, etc.). Ainsi, vous pouvez limiter la connexion de tous les appareils, par exemple, via USB.

Vous pouvez configurer l'accès des appareils de la manière suivante :

- Autoriser : ✓.
- Interdire : ⚡.
- **Appareils de confiance** Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Vous pouvez ajouter des appareils de confiance selon les données suivantes :

- **Appareils en fonction de l'identificateur.** Chaque appareil possède un identifiant unique (en anglais, Hardware ID - HWID). Vous pouvez consulter l'identificateur dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Exemple d'identifiant d'appareil : `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'ajout d'un appareil par identifiant est pratique si vous souhaitez ajouter plusieurs appareils spécifiques.
- **Appareils en fonction du modèle.** Chaque appareil possède un identifiant de fabricant (en anglais, Vendor ID - VID) et un identifiant de produit (en anglais, Product ID - PID). Vous pouvez consulter les identificateurs dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Modèle de saisie du VID et du PID : `VID_1234&PID_5678`. L'ajout d'appareil par modèle est pratique si vous utilisez des appareils d'un certain modèle dans votre organisation. Ainsi, vous pouvez ajouter tous les appareils de ce modèle.
- **Appareils en fonction du masque de l'identifiant.** Si vous utilisez plusieurs appareils avec des identifiants similaires, vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `WDC_C*`.
- **Appareils selon le masque du modèle.** Si vous utilisez plusieurs appareils avec des VID ou PID similaires (par exemples, appareils d'un même fabricant), vous pouvez les ajouter à la liste des appareils de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security ne prend pas en charge le caractère `?` dans la saisie d'un masque. Par exemple, `VID_05AC & PID_*`.

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils à l'aide [de règles d'accès](#). Le Contrôle des appareils permet également d'enregistrer les événements de connexion/déconnexion des appareils. Pour enregistrer les événements, vous devez configurer l'envoi des événements dans la stratégie.

Si l'accès à l'appareil dépend du bus de connexion (état 🌐), Kaspersky Endpoint Security n'enregistre pas l'événement de connexion/de déconnexion de l'appareil. Pour que l'application Kaspersky Endpoint Security enregistre les événements de connexion/de déconnexion de l'appareil, autorisez l'accès au type d'appareil correspondant (état ✓) ou ajoutez l'appareil à la liste des appareils de confiance.

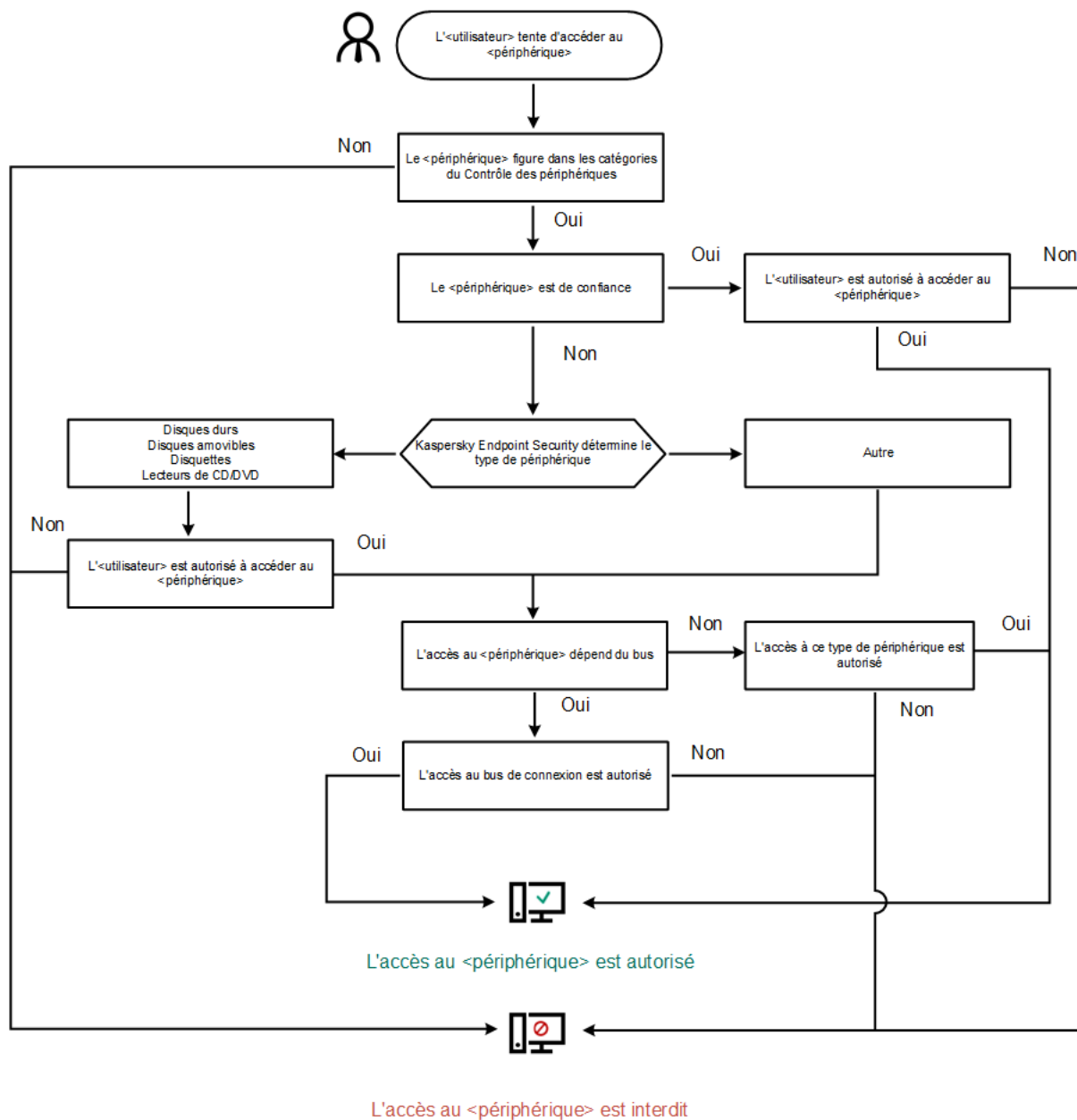
Quand l'appareil se connecte à un ordinateur auquel l'accès est interdit par le Contrôle des appareils, Kaspersky Endpoint Security bloque l'accès et affiche une notification (cf. ill. ci-dessous).



Notification du Contrôle des appareils

Algorithme de fonctionnement du Contrôle des appareils

Une fois que l'utilisateur a connecté un appareil à l'ordinateur, Kaspersky Endpoint Security prend la décision sur l'accès à cet appareil (cf. ill. ci-après).



Algorithme de fonctionnement du Contrôle des appareils

Si l'appareil est connecté et que l'accès est autorisé, vous pouvez modifier la règle d'accès et refuser l'accès. Dans ce cas, lors du prochain accès à l'appareil (consultation de l'arborescence de dossiers, lecture, écriture), Kaspersky Endpoint Security en bloque l'accès. Le blocage de l'appareil sans système de fichiers aura lieu uniquement lors de la connexion suivante de l'appareil.

Si l'utilisateur de l'ordinateur doté de Kaspersky Endpoint Security doit demander l'accès à un appareil qui, d'après lui, a été bloqué par erreur, transmettez lui [l'instruction de demande d'accès](#).

Paramètres du module Contrôle des appareils

| Paramètre | Description |
|-----------------------------|--|
| Autoriser la demande | Si la case est cochée, alors le bouton Demander l'accès dans l'interface locale de Kaspersky Endpoint Security est accessible. Cliquez sur ce bouton pour ouvrir la |

| | |
|---|--|
| <p>d'accès temporaire</p> <p><i>(disponible uniquement dans Kaspersky Security Center Console)</i></p> | <p>fenêtre Demande d'accès à l'appareil. Cette fenêtre permet à l'utilisateur de demander un accès temporaire à l'appareil bloqué.</p> |
| <p>Appareils et réseaux Wi-Fi</p> | <p>Tableau reprenant tous les types possibles d'appareils selon la classification du module Contrôle des appareils, ainsi que l'état d'accès à ceux-ci.</p> |
| <p>Bus de connexion</p> | <p>Liste de tous les types possibles de bus de connexion selon la classification du module Contrôle des appareils, ainsi que l'état d'accès à ces types de bus.</p> |
| <p>Appareils de confiance</p> | <p>Liste des appareils de confiance et des utilisateurs autorisés à accéder à ceux-ci.</p> |
| <p>Anti-Bridging</p> | <p>L'Anti-Bridging empêche la création de ponts réseau, ce qui élimine la possibilité d'établir simultanément plusieurs connexions réseau pour un ordinateur. Il offre une protection du réseau de l'entreprise contre les attaques via des réseaux non sécurisés et non autorisés.</p> <p>Anti-Bridging bloque l'établissement de plusieurs connexions en fonction des priorités de l'appareil. Plus l'appareil est haut dans la liste, plus sa priorité est élevée.</p> <p>Si les connexions actives et nouvelles sont du même type (Wi-Fi, par exemple), Kaspersky Endpoint Security bloque la connexion active et permet l'établissement d'une nouvelle connexion.</p> <p>Si les connexions actives et nouvelles sont de types différents (par exemple, adaptateur réseau et Wi-Fi), Kaspersky Endpoint Security bloque la connexion dont la priorité est inférieure et autorise la connexion avec une priorité supérieure.</p> <p>Anti-Bridging est compatible avec les types d'appareil suivants : carte réseau, Wi-Fi et modem.</p> |
| <p>Modèles de messages</p> | <ul style="list-style-type: none"> • Message sur le blocage. Modèle du message qui apparaît lorsqu'un utilisateur accède à un appareil bloqué. Ce message apparaît également lorsqu'un utilisateur tente d'exécuter une opération interdite sur le contenu de l'appareil. • Message à l'administrateur. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès à l'appareil ou l'interdiction des opérations impliquant le contenu de l'appareil sont intervenus par erreur. |

Contrôle des applications

Le Contrôle des applications contrôle le lancement des applications sur les ordinateurs des utilisateurs. Cela permet de mettre en œuvre la stratégie de sécurité de l'organisation dans le cadre de l'utilisation des applications. De plus, le Contrôle des applications réduit le risque d'infection de l'ordinateur en limitant l'accès aux applications.

La configuration du Contrôle des applications comprend les étapes suivantes :

1. [Création des catégories d'applications.](#)

L'administrateur crée des catégories d'application que l'administrateur souhaite administrer. Les catégories d'applications sont prévues pour tous les ordinateurs du réseau de l'organisation, quels que soient les groupes d'administration. Pour créer une catégorie, vous pouvez utiliser les critères suivants : catégorie KL (par exemple, *Navigateurs*), hachage du fichier, éditeurs d'applications, etc.

2. Création de règles de Contrôle des applications.

L'administrateur crée les règles de Contrôle des applications dans la stratégie pour le groupe d'administration. La règle inclut les catégories d'application et l'état du lancement des applications de ces catégories : interdit ou autorisé.

3. Sélection du mode de fonctionnement du Contrôle des applications.

L'administrateur choisit le mode d'utilisation des applications qui ne figurent dans aucune des règles (liste de refus et liste d'autorisation de l'application).

Lorsqu'un utilisateur tente de lancer une application interdite, Kaspersky Endpoint Security empêche le lancement de celle-ci et affiche une notification (cf. ill. ci-dessous).

Pour vérifier les paramètres du Contrôle des applications, utilisez le *mode de test*. Dans ce mode, Kaspersky Endpoint Security exécute les actions suivantes :

- il autorise le lancement des applications, y compris les applications interdites ;
- il affiche une notification concernant le lancement d'une application interdite et ajoute des informations dans le rapport sur l'ordinateur de l'utilisateur ;
- il envoie des données sur le lancement des applications interdites à Kaspersky Security Center.



Notification du Contrôle des applications

Modes de fonctionnement du Contrôle des applications

Le module Contrôle des applications peut fonctionner selon deux modes :

- **Liste de refus.** Mode dans le cadre duquel le Contrôle des applications autorise les utilisateurs à lancer n'importe quelle application, sauf celles interdites dans les règles de Contrôle des applications. Il s'agit du mode de fonctionnement du Contrôle des applications définies par défaut.
- **Liste d'autorisation.** Mode selon lequel le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception de celles autorisées et non interdites dans les règles de Contrôle des applications.

Si les règles d'autorisation de Contrôle des applications sont les plus strictes, le module interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

Vous pouvez prendre connaissance des [recommandations sur la configuration des règles du Contrôle des applications en mode de liste d'autorisation](#).

La configuration du Contrôle des applications pour le fonctionnement dans ces modes est possible à partir de l'interface locale de Kaspersky Endpoint Security ou via Kaspersky Security Center.

Ceci étant dit, Kaspersky Security Center propose des outils qui ne sont pas accessibles dans l'interface locale de Kaspersky Endpoint Security et qui sont indispensables pour réaliser les tâches suivantes :

- [Création des catégories d'applications](#).

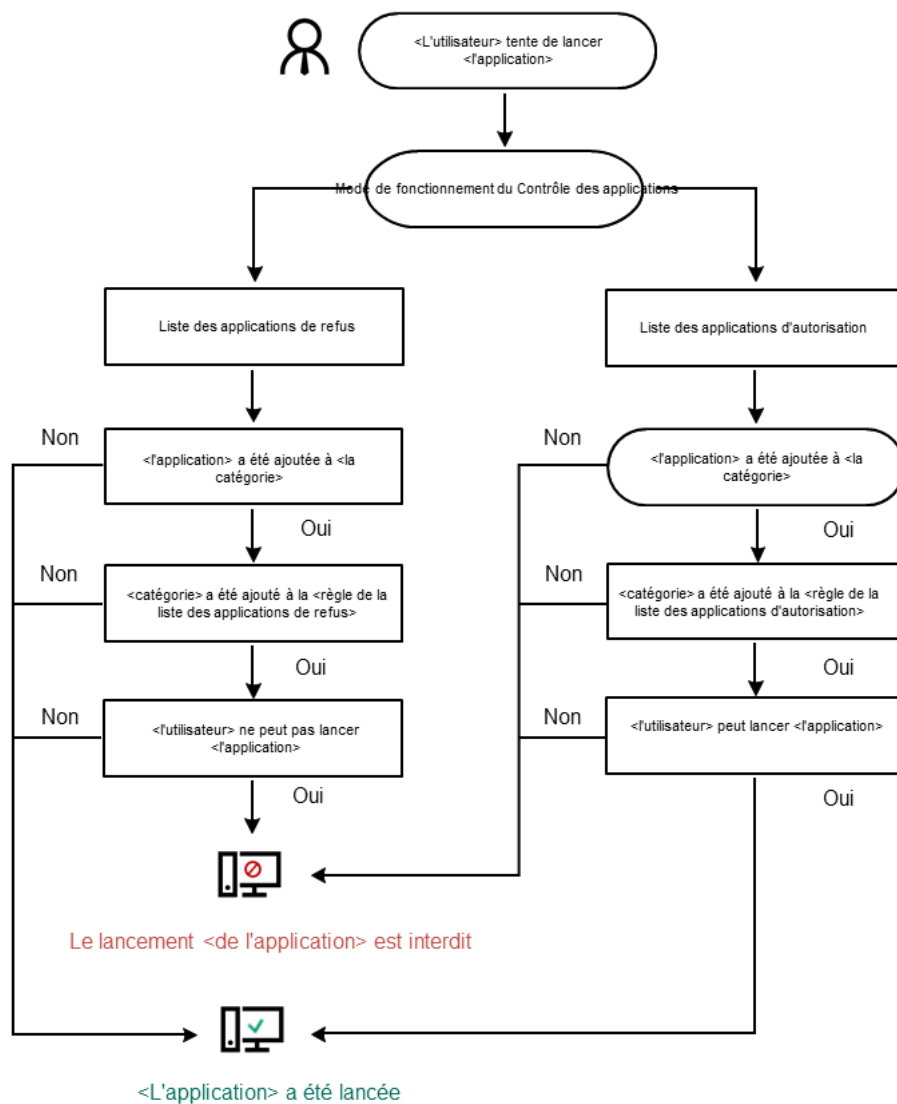
Les règles de Contrôle des applications créées dans la Console d'administration de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.

- [Récupération des informations relatives aux applications installées sur les ordinateurs du réseau local de l'entreprise](#).

C'est pour cette raison qu'il est conseillé de configurer le fonctionnement du module Contrôle des applications via Kaspersky Security Center.

Algorithme de fonctionnement du Contrôle des applications

Kaspersky Endpoint Security utilise un algorithme pour décider de lancer ou non une application (cf. ill. ci-dessous).



Algorithme de fonctionnement du Contrôle des applications

Paramètres du module Contrôle des applications

| Paramètre | Description |
|--|---|
| Mode d'essai | Si le commutateur est activé, Kaspersky Endpoint Security autorise le lancement de l'application interdite dans le mode actuel du Contrôle des applications et consigne les informations relatives au lancement dans le rapport. |
| Mode de Contrôle des applications | <p>Vous avez le choix entre les options suivantes :</p> <ul style="list-style-type: none"> • Liste de refus. Si vous choisissez cette option, le Contrôle des applications permet à tous les utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'interdiction de Contrôle des applications. • Liste d'autorisation. Si vous choisissez cette option, le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'autorisation de Contrôle des applications. <p>Le choix du mode Liste d'autorisation entraîne la création automatique de deux règles du Contrôle des applications :</p> <ul style="list-style-type: none"> • Image d'or. |

| | |
|----------------------------|---|
| | <ul style="list-style-type: none"> • Programmes de mise à jour de confiance. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Il est impossible de modifier les paramètres et de supprimer les règles créées automatiquement. Vous pouvez activer ou désactiver ces règles.</p> </div> |
| Contrôle DLL | <p>Si la case est cochée, Kaspersky Endpoint Security contrôle le chargement des modules DLL lors du lancement des applications par les utilisateurs. Les informations relatives au module DLL et à l'application qui a chargé celui-ci seront enregistrées dans le rapport.</p> <div style="border: 1px solid black; background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut Image d'or ou toute autre règle qui contient la catégorie KL "Certificats de confiance" est activée dans les paramètres du Contrôle des applications et qu'elle garantit le chargement des modules DLL et des pilotes de confiance avant le lancement de Kaspersky Endpoint Security. L'activation du contrôle du chargement des modules DLL et des pilotes lorsque la règle Image d'or est désactivée peut provoquer l'instabilité du système d'exploitation.</p> </div> <p>Kaspersky Endpoint Security contrôle uniquement les modules DLL et les pilotes chargés à partir du moment où la case a été cochée. Après avoir coché la case, il est recommandé de redémarrer l'ordinateur pour s'assurer que l'application surveille tous les modules DLL et les pilotes, y compris ceux chargés avant le démarrage de Kaspersky Endpoint Security.</p> |
| Modèles de messages | <p>Message sur le blocage. Modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application.</p> <p>Message à l'administrateur. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'application est intervenu par erreur.</p> |

Contrôle évolutif des anomalies

Ce module est disponible uniquement pour Kaspersky Endpoint Security for Business Advanced et Kaspersky Total Security for Business. Pour en savoir plus à propos de Kaspersky Endpoint Security for Business, veuillez consulter le [site de Kaspersky](#)).

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le module Contrôle évolutif des anomalies surveille et bloque les actions atypiques pour les ordinateurs du réseau d'une organisation. Le Contrôle évolutif des anomalies utilise un ensemble de règles (par exemple, la règle *Lancement de Windows PowerShell depuis une application de bureautique*) pour suivre les actions atypiques. Ces règles sont créées par les experts de Kaspersky sur la base des scénarios typiques d'action malveillantes. Vous pouvez choisir le comportement du Contrôle évolutif des anomalies pour chacune des règles et, par exemple, autoriser le lancement de scripts PowerShell pour automatiser l'exécution des tâches d'entreprise. Kaspersky Endpoint Security met à jour l'ensemble de règles à l'aide des bases de données de l'application. La mise à jour de l'ensemble de règles doit être [confirmer manuellement](#).

Configuration du Contrôle évolutif des anomalies

La configuration du Contrôle évolutif des anomalies comprend les étapes suivantes :

1. Apprentissage du Contrôle évolutif des anomalies

Une fois que le Contrôle évolutif des anomalies a été activé, les règles fonctionnent en *mode d'apprentissage*. Au cours de l'apprentissage, le Contrôle évolutif des anomalies surveille le déclenchement des règles et envoie les événements déclencheurs à Kaspersky Security Center. La durée du mode d'apprentissage est propre à chaque règle. Celle-ci est définie par les experts de Kaspersky. En règle générale, le mode d'apprentissage dure 2 semaines.

Si une règle n'a jamais été déclenchée lors de l'apprentissage, le Contrôle évolutif des anomalies considère les actions associées à cette règle comme atypiques. Kaspersky Endpoint Security bloquera toutes les actions associées à cette règle.

Si la règle s'est déclenchée lors de l'apprentissage, Kaspersky Endpoint Security enregistre les événements dans [rapport sur les déclenchements des règles](#) et dans le stockage **Fonctionnement des règles en mode d'apprentissage**.

2. Analyse du rapport sur les déclenchements des règles

L'administrateur analyse le [rapport sur les déclenchements des règles](#) ou le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Ensuite, l'administrateur peut sélectionner le comportement du Contrôle évolutif des anomalies lors du déclenchement d'une règle : bloquer ou autoriser. En outre, l'administrateur peut continuer à surveiller le déclenchement de la règle et prolonger le fonctionnement d'application en mode d'apprentissage. Si l'administrateur ne prend aucune mesure, l'application continuera également à fonctionner en mode d'apprentissage. Le décompte de la durée du mode d'apprentissage est remis à zéro.

La configuration du Contrôle évolutif des anomalies se déroule en temps réel. La configuration du Contrôle évolutif des anomalies se déroule de la manière suivante :

- Le Contrôle évolutif des anomalies commence automatiquement à bloquer les actions associées aux règles qui ne se sont pas déclenchées lors de l'apprentissage.
- Kaspersky Endpoint Security ajoute de nouvelles règles ou supprime les règles qui ne sont plus pertinentes.
- L'administrateur configure le fonctionnement du Contrôle évolutif des anomalies après avoir analysé le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Il est recommandé de vérifier le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**.

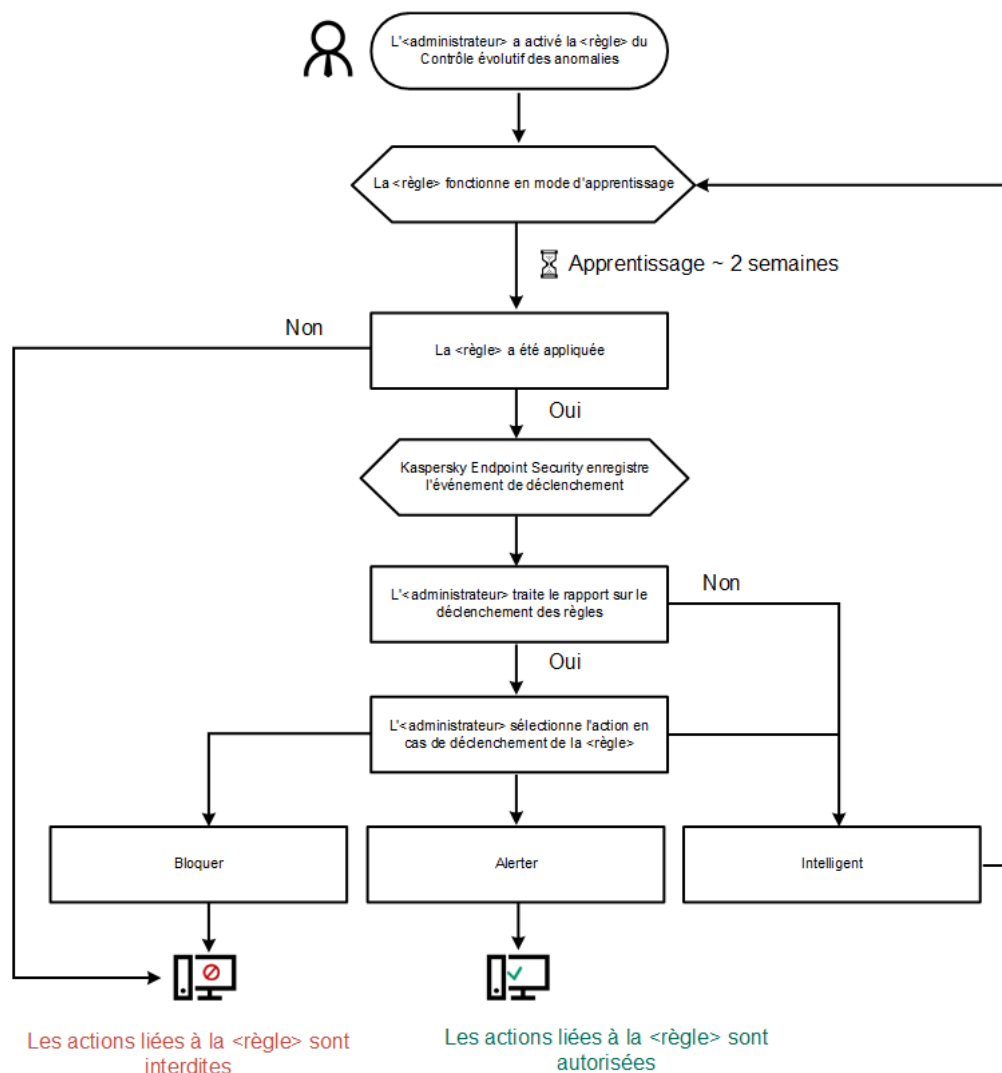
Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



Notification du Contrôle évolutif des anomalies

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Kaspersky Endpoint Security autorise ou non l'exécution d'une action associée à une règle selon l'algorithme suivant (cf. ill. ci-dessous).



Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Paramètres du module Contrôle évolutif des anomalies

| Paramètre | Description |
|---|--|
| Rapport sur l'état des règles <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | Ce rapport contient des informations sur l'état des règles de détection du Contrôle évolutif des anomalies (par exemple, les états <i>Désactivé</i> ou <i>Bloquer</i>). Le rapport est créé pour tous les groupes d'administration. |
| Rapport sur les déclenchements des règles <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | Ce rapport contient les informations sur les actions suspectes détectées par le Contrôle évolutif des anomalies. Le rapport est créé pour tous les groupes d'administration. |
| Règles | Tableau des règles du Contrôle évolutif des anomalies Les règles ont été créées par les experts de Kaspersky sur la base des scénarios typiques d'activités |

| | |
|----------------|--|
| | potentiellement malveillantes. |
| Modèles | <ul style="list-style-type: none"> • Message sur le blocage. Modèle de message destiné à l'utilisateur et qui s'affiche en cas de déclenchement de la règle du Contrôle évolutif des anomalies qui bloque l'action atypique. • Message à l'administrateur. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'action est intervenu par erreur. |

Endpoint Sensor

Dans Kaspersky Endpoint Security 11.4.0, le module Endpoint Sensor est exclu de l'application.

Vous pouvez gérer Endpoint Sensor dans Kaspersky Security Center 12 Web Console et la Console d'administration de Kaspersky Security Center. Il n'est pas possible d'administrer Endpoint Sensor dans Kaspersky Security Center Cloud Console.

Endpoint Sensor est prévu pour l'interaction avec Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* est une solution conçue pour la détection ponctuelle de menaces complexes, telles que les attaques ciblées, les menaces persistantes avancées (APT en anglais), les attaques zero day, etc. Kaspersky Anti Targeted Attack Platform comprend deux ensembles fonctionnels : Kaspersky Anti Targeted Attack (ci-après également appelé *KATA*) et Kaspersky Endpoint Detection and Response (ci-après également appelé *KEDR*). Vous pouvez acheter KEDR séparément. Pour en savoir plus sur la solution, [consultez l'aide de Kaspersky Anti Targeted Attack Platform](#).

L'administration d'Endpoint Sensor possède les caractéristiques suivantes :

- Si Kaspersky Endpoint Security version 11.0.0 à 11.3.0 est installé sur l'ordinateur, vous pouvez configurer les paramètres d'Endpoint Sensor à l'aide d'une stratégie. Pour plus d'informations sur la configuration des paramètres d'Endpoint Sensor à l'aide d'une stratégie, consultez l'[aide des versions antérieures de Kaspersky Endpoint Security](#).
- Si Kaspersky Endpoint Security 11.4.0 et versions ultérieures est installé sur l'ordinateur, vous ne pouvez pas configurer Endpoint Sensor à l'aide d'une stratégie.

Endpoint Sensor est installé sur les ordinateurs clients. Sur ces ordinateurs, le module contrôle en permanence les processus, les connexions réseau ouvertes et les fichiers modifiés. Endpoint Sensor transmet les informations au serveur KATA.

Les fonctions du module sont disponibles pour les systèmes d'exploitation suivants :

- Windows 7 Service Pack 1 Home/Professional/Enterprise;
- Windows 8.1.1 Professional/Enterprise ;
- Windows 10 RS3 Home/Professional/Education/Enterprise ;
- Windows 10 RS4 Home/Professional/Education/Enterprise ;

- Windows 10 RS5 Home/Professional/Education/Enterprise ;
- Windows 10 RS6 Home/Professional/Education/Enterprise ;
- Windows Server 2008 R2 Foundation/Standard/Enterprise (64 bits) ;
- Windows Server 2012 Foundation/Standard/Enterprise (64 bits) ;
- Windows Server 2012 R2 Foundation/Standard/Enterprise (64 bits) ;
- Windows Server 2016 Essentials/Standard (64 bits).

Pour en savoir plus sur le fonctionnement de KATA, [consultez l'aide de Kaspersky Anti Targeted Attack Platform](#).

Chiffrement du disque

Vous pouvez choisir la technologie du chiffrement : Kaspersky Disk Encryption ou le Chiffrement de disque BitLocker (ci-après "BitLocker").

Kaspersky Disk Encryption

Une fois que les disques durs système auront été chiffrés, l'accès à ceux-ci et le chargement du système d'exploitation lors du prochain démarrage de l'ordinateur seront possibles uniquement après avoir suivi la procédure d'authentification à l'aide de l'[Agent d'authentification](#). Pour ce faire, il faut saisir le mot de passe du token ou de la carte à puce connecté à l'ordinateur, ou le nom et le mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur système du réseau local de l'organisation à l'aide de la tâche [Gérer les comptes de l'Agent d'authentification](#). Ces comptes utilisateur reposent sur les comptes utilisateur Microsoft Windows utilisés pour accéder au système d'exploitation. Vous pouvez également [utiliser la technologie d'authentification unique \(SSO, Single Sign-On\)](#) qui permet d'accéder automatiquement au système d'exploitation à l'aide du nom et du mot de passe du compte utilisateur de l'Agent d'Authentification.

L'authentification de l'utilisateur dans l'Agent d'authentification peut s'exécuter par deux moyens :

- via la saisie du nom d'utilisateur et du mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur du réseau local de l'organisation via Kaspersky Security Center ;
- via la saisie du mot de passe du token ou de la carte à puce rattaché à l'ordinateur.

L'utilisation du token ou de la carte à puce est disponible uniquement si les disques durs de l'ordinateur sont chiffrés à l'aide d'un algorithme AES256. Si les disques durs de l'ordinateur ont été chiffrés à l'aide d'un algorithme de chiffrement AES56, le fichier de certificat électronique ne pourra pas être ajouté à la commande.

Chiffrement de disque BitLocker

BitLocker est une technologie de chiffrement intégrée au système d'exploitation Windows. Kaspersky Endpoint Security vous permet de contrôler et de gérer BitLocker à l'aide de Kaspersky Security Center. BitLocker chiffre le volume logique. BitLocker ne permet pas de chiffrer les disques amovibles. Pour en savoir plus sur le fonctionnement de BitLocker, consultez la [documentation de Microsoft](#).

BitLocker fournit un stockage sécurisé des clés d'accès à l'aide d'un module de plateforme sécurisée. *Module de plateforme sécurisée (en anglais, Trusted Platform Module (TPM))* : puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Un module de plateforme sécurisée est généralement installé sur la carte mère de l'ordinateur et interagit avec tous les autres modules du système par le bus matériel. L'utilisation du module de plateforme sécurisée est le moyen le plus sûr de stocker des clés d'accès BitLocker, car ce module permet de vérifier l'intégrité du système avant le démarrage. Sur les ordinateurs sans TPM, vous pouvez également chiffrer des disques. Dans ce cas, la clé d'accès sera chiffrée à l'aide d'un mot de passe. Ainsi, BitLocker utilise les méthodes d'authentification suivantes :

- TPM.
- TPM et code PIN.
- Mot de passe.

Après avoir chiffré le disque, BitLocker crée une clé principale. Kaspersky Endpoint Security envoie la clé principale à Kaspersky Security Center afin que vous puissiez [restaurer l'accès au disque](#) si l'utilisateur a oublié le mot de passe, par exemple.

Si un utilisateur a chiffré un disque à l'aide de BitLocker, Kaspersky Endpoint Security envoie les [informations sur le chiffrement du disque à Kaspersky Security Center](#). Dans ce cas, Kaspersky Endpoint Security n'envoie pas la clé principale à Kaspersky Security Center et il est impossible de restaurer l'accès au disque à l'aide de Kaspersky Security Center. Pour que BitLocker fonctionne correctement avec Kaspersky Security Center, [déchiffrez le disque](#) et [chiffrez-le à nouveau](#) à l'aide d'une stratégie. Vous pouvez déchiffrer un disque localement ou à l'aide d'une stratégie.

Après avoir chiffré le disque dur du système, l'utilisateur doit passer par l'authentification BitLocker pour lancer le système d'exploitation. Une fois l'authentification réussie, BitLocker pourra se connecter. BitLocker n'est pas compatible avec la technologie d'authentification unique (SSO).

Si vous utilisez des stratégies de groupe pour Windows, désactivez l'administration de BitLocker dans les paramètres de la stratégie. Les paramètres de la stratégie Windows peuvent entrer en conflit avec les paramètres de la stratégie de Kaspersky Endpoint Security. Lors du chiffrement d'un disque, des erreurs peuvent se produire.

Paramètres du module Kaspersky Disk Encryption

| Paramètre | Description |
|----------------------------|---|
| Mode de chiffrement | <p>Chiffrer tous les disques durs. Si vous choisissez cette option, l'application chiffre tous les disques durs lors de l'application de la stratégie.</p> <p>Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel l'application est installée peut être lancé après le chiffrement.</p> <p>Déchiffrer tous les disques durs. Si vous choisissez cette option, l'application déchiffre tous les disques durs chiffrés antérieurement lors de l'application de la stratégie.</p> |

| | |
|---|---|
| | <p>Laisser tel quel. Si vous choisissez cette option, l'application ne modifie pas l'état des disques durs lors de l'application de la stratégie. Si le disque était chiffré, il reste chiffré. Si le disque était déchiffré, il reste déchiffré. L'option est sélectionnée par défaut.</p> |
| <p>Pendant le chiffrement, créer automatiquement des comptes de l'Agent d'authentification pour les utilisateurs Windows</p> | <p>Si cette case est cochée, l'application crée des comptes de l'Agent d'authentification en fonction de la liste des comptes d'utilisateurs Windows sur l'ordinateur. Par défaut, Kaspersky Endpoint Security utilise tous les comptes locaux et de domaine avec lesquels l'utilisateur s'est connecté au système d'exploitation au cours des 30 derniers jours.</p> |
| <p>Paramètres de création de comptes utilisateur de l'Agent d'authentification</p> | <p>Tous les comptes de l'ordinateur. Si la case est cochée, lors de l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security crée des comptes utilisateur de l'Agent d'authentification pour tous les comptes utilisateur de l'ordinateur qui étaient actifs à un moment ou à un autre.</p> <p>Tous les comptes de domaine de l'ordinateur. Si la case est cochée, lors de l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security crée des comptes utilisateur de l'Agent d'authentification pour tous les comptes utilisateur de l'ordinateur qui font partie d'un domaine quelconque ou qui étaient actifs à un moment ou à un autre.</p> <p>Tous les comptes locaux de l'ordinateur. Si la case est cochée, lors de l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security crée des comptes utilisateur de l'Agent d'authentification pour tous les comptes utilisateur locaux de l'ordinateur qui étaient actifs à un moment ou à un autre.</p> <p>Administrateur local. Si la case est cochée, Kaspersky Endpoint Security crée un compte administrateur local lors de l'exécution de la tâche de chiffrement du disque.</p> <p>Gestionnaire de l'ordinateur. Si la case est cochée, lors de l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security crée un compte utilisateur de l'Agent d'authentification pour le compte utilisateur dont les propriétés dans Active Directory indiquent qu'il est gestionnaire.</p> <p>Compte actif. Si la case est cochée, lors de l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security crée automatiquement un compte utilisateur de l'Agent d'authentification pour le compte utilisateur de l'ordinateur actif au moment d'exécution de la tâche.</p> |
| <p>Créer automatiquement des comptes de l'Agent d'authentification pour tous les utilisateurs de cet ordinateur lors de la connexion</p> | <p>Si cette case est cochée, l'application vérifie les informations relatives aux comptes utilisateur Windows sur l'ordinateur avant de lancer l'Agent d'authentification. Si Kaspersky Endpoint Security détecte un compte utilisateur Windows qui ne dispose pas de compte d'Agent d'authentification, l'application créera un nouveau compte pour accéder aux disques chiffrés. Le nouveau compte de l'Agent d'authentification présentera les paramètres par défaut suivants : ouverture de session protégée par mot de passe uniquement et changement de mot de passe lors de la première authentification. Par conséquent, vous n'avez pas besoin d'ajouter manuellement des comptes d'Agent d'authentification en utilisant la tâche <i>Gérer les comptes de l'Agent d'authentification</i> pour les ordinateurs avec des disques déjà chiffrés.</p> |
| <p>Enregistrer le nom d'utilisateur saisi dans l'Agent d'authentification</p> | <p>Si la case est cochée, l'application enregistre le nom du compte utilisateur de l'Agent d'authentification. Dès l'authentification suivante dans l'Agent d'authentification, il ne sera plus nécessaire de saisir le nom du compte utilisateur.</p> |
| <p>Chiffrer uniquement l'espace occupé</p> | <p>La case active/désactive la fonction qui limite le secteur de chiffrement aux secteurs occupés du disque dur. Cette restriction permet de réduire la durée du chiffrement.</p> |

L'activation ou la désactivation de la fonctionnalité **Chiffrer uniquement l'espace occupé (réduit la durée du chiffrement)** après le lancement du chiffrement ne modifie pas ce paramètre tant que les disques durs ne sont pas déchiffrés. Il faut cocher ou décocher la case avant le début du chiffrement.

Si la case est cochée, seule la partie du disque dur qui contient des fichiers est chiffrée. Kaspersky Endpoint Security chiffre les nouvelles données automatiquement au fur et à mesure qu'elles sont ajoutées.

Si la case est décochée, tout le disque dur est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant.

Cette fonction est recommandée pour les nouveaux disques durs dont les données n'ont pas été modifiées ou supprimées. Si vous appliquez le chiffrement sur un disque dur déjà utilisé, il est conseillé de chiffrer tout le disque dur. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais qui pourraient être restaurées.

La case est décochée par défaut.

Utiliser le Legacy USB Support

La case active/désactive la fonction Legacy USB Support. *Legacy USB Support* est une fonction BIOS/UEFI qui permet d'utiliser des appareils USB (comme un token) pendant la phase de démarrage d'un ordinateur avant le lancement du système d'exploitation (mode BIOS). La fonction Legacy USB Support n'a pas d'impact sur la prise en charge des appareils USB après le lancement du système d'exploitation.

Si la case est cochée, la prise en charge des appareils USB est activée lors du chargement initial de l'ordinateur.

Lorsque la fonction Legacy USB Support est activée, l'Agent d'authentification en mode BIOS ne prend pas en charge l'utilisation de jetons via USB. Il est recommandé d'utiliser la fonction uniquement en cas de problèmes d'incompatibilités avec le matériel et seulement sur les ordinateurs où le problème est apparu.

Paramètres des mots de passe

Paramètres de sécurité du compte utilisateur de l'Agent d'authentification Vous pouvez également activer l'utilisation de la technologie d'authentification unique (SSO).

La technologie d'authentification unique permet d'utiliser les mêmes identifiants pour accéder aux disques durs chiffrés et pour se connecter au système d'exploitation.

Si la case est cochée, il faudra saisir les identifiants d'accès aux disques chiffrés pour pouvoir accéder aux disques durs chiffrés et se connecter ensuite automatiquement au système d'exploitation.

Si la case est décochée, il faudra saisir séparément les identifiants pour l'accès aux disques durs chiffrés et les identifiants de l'utilisateur dans le système d'exploitation pour pouvoir accéder aux disques durs chiffrés et se connecter ensuite au système d'exploitation.

Textes d'aide

Authentification. Le texte d'aide qui apparaît dans la fenêtre de l'Agent d'authentification à l'étape de saisie des informations d'identification.

Modification du mot de passe. Le texte d'aide qui apparaît dans la fenêtre de l'Agent d'authentification à l'étape de la modification du mot de passe du compte utilisateur de l'Agent d'authentification.

Restauration du mot de passe. Le texte d'aide qui apparaît dans la fenêtre de l'Agent d'authentification pendant la phase de récupération du mot de passe pour le compte utilisateur d'Agent d'authentification.

Paramètres du module Chiffrement de disque BitLocker

| Paramètre | Description |
|--|---|
| Mode de chiffrement | <p>Chiffrer tous les disques durs. Si vous choisissez cette option, l'application chiffre tous les disques durs lors de l'application de la stratégie.</p> <div style="background-color: #f8d7da; padding: 10px;"><p>Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel l'application est installée peut être lancé après le chiffrement.</p></div> <p>Déchiffrer tous les disques durs. Si vous choisissez cette option, l'application déchiffre tous les disques durs chiffrés antérieurement lors de l'application de la stratégie.</p> <p>Laisser tel quel. Si vous choisissez cette option, l'application ne modifie pas l'état des disques durs lors de l'application de la stratégie. Si le disque était chiffré, il reste chiffré. Si le disque était déchiffré, il reste déchiffré. L'option est sélectionnée par défaut.</p> |
| Autoriser l'utilisation de l'authentification BitLocker qui requiert une saisie au clavier avant le démarrage sur les tablettes | <p>La case active ou désactive l'utilisation de l'authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage, même si la plateforme ne dispose pas de cette possibilité (par exemple, claviers tactiles sur les tablettes).</p> <div style="border: 1px solid #ccc; padding: 10px;"><p>Le clavier tactile des tablettes n'est pas accessible dans cet environnement. Pour réaliser une authentification BitLocker sur de telles tablettes, l'utilisateur doit absolument connecter un clavier USB par exemple.</p></div> <p>Si la case est cochée, l'utilisation de l'authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage est autorisée. Il est recommandé d'utiliser ce paramètre uniquement pour les appareils qui, pendant le chargement préalable, disposent de modes alternatifs de saisie de données, par exemple un clavier USB en plus du clavier tactile.</p> <p>Si cette case est décochée, le chiffrement de disque BitLocker n'est pas possible sur les tablettes.</p> |
| Utiliser le chiffrement au niveau matériel | <p>Si la case est cochée, l'application adopte le chiffrement au niveau du matériel. Cela permet d'augmenter la vitesse du chiffrement et de réduire l'utilisation des ressources de l'ordinateur.</p> |
| Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures) | <p>La case active/désactive la fonction qui limite le secteur de chiffrement aux secteurs occupés du disque dur. Cette restriction permet de réduire la durée du chiffrement.</p> <div style="border: 1px solid #ccc; padding: 10px;"><p>L'activation ou la désactivation de la fonctionnalité Chiffrer uniquement l'espace occupé (réduit la durée du chiffrement) après le lancement du chiffrement ne modifie pas ce paramètre tant que les disques durs ne sont pas déchiffrés. Il faut cocher ou décocher la case avant le début du chiffrement.</p></div> |

Si la case est cochée, seule la partie du disque dur qui contient des fichiers est chiffrée. Kaspersky Endpoint Security chiffre les nouvelles données automatiquement au fur et à mesure qu'elles sont ajoutées.

Si la case est décochée, tout le disque dur est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant.

Cette fonction est recommandée pour les nouveaux disques durs dont les données n'ont pas été modifiées ou supprimées. Si vous appliquez le chiffrement sur un disque dur déjà utilisé, il est conseillé de chiffrer tout le disque dur. Cela garantit la protection de toutes les données, même celles qui ont été supprimées mais qui pourraient être restaurées.

La case est décochée par défaut.

Paramètres d'authentification

Utiliser le mot de passe (Windows 8 et versions ultérieures)

Si vous avez choisi cette option, Kaspersky Endpoint Security demande le mot de passe à l'utilisateur lorsque celui-ci souhaite accéder au disque chiffré.

Cette option peut être choisie si la Trusted Platform Module (TPM) n'est pas utilisée.

Utiliser Trusted Platform Module (TPM)

Si vous avez choisi cette option, BitLocker utilise le Trusted Platform Module (TPM).

Module de plateforme sécurisée (en anglais, Trusted Platform Module (TPM)): puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Le Trusted Platform Module s'installe en général sur la carte mère de l'ordinateur et interagit avec les autres modules système via le bus matériel.

Pour les ordinateurs tournant sous les systèmes d'exploitation Windows 7 et Windows Server 2008 R2, seul le chiffrement à l'aide du module TPM est disponible. Si le module TPM n'est pas installé, le chiffrement BitLocker n'est pas possible. L'utilisation d'un mot de passe sur ces ordinateurs n'est pas prise en charge.

L'appareil équipé du Trusted Platform Module peut créer des clés de chiffrement qui peuvent être déchiffrées uniquement à l'aide de celui-ci. Le Trusted Platform Module chiffre les clés de chiffrement à l'aide de la clé racine de stockage correspondante. La clé racine de stockage se trouve à l'intérieur du Trusted Platform Module. Cela offre un niveau de sécurité complémentaire pour les clés de chiffrement contre les tentatives d'attaque.

Cette action est sélectionnée par défaut.

Vous pouvez définir une couche de protection supplémentaire pour l'accès à la clé de chiffrement, et chiffrer la clé à l'aide d'un mot de passe ou d'un code PIN :

- **Utiliser le code PIN pour le TPM.** Quand la case est cochée, l'utilisateur doit saisir un code PIN pour accéder à la clé de chiffrement conservée dans le module de plateforme sécurisée (TPM). Si cette case n'est pas cochée, l'utilisateur n'est pas autorisé à utiliser le code PIN. Pour accéder à la clé de chiffrement, l'utilisateur utilise un mot de passe. Vous pouvez autoriser l'utilisateur à utiliser un code PIN amélioré. Le *code PIN renforcé* permet l'utilisation d'autres caractères en plus des caractères numériques : lettres latines majuscules et minuscules, caractères spéciaux et espaces.

- **Utiliser Trusted Platform Module (TPM) ; s'il n'est pas disponible, utiliser le mot de passe.** Si la case est cochée, l'utilisateur peut accéder aux clés de chiffrement à l'aide d'un mot de passe en l'absence du Trusted Platform Module (TPM).

Si la case n'est pas cochée et que le TPM n'est pas disponible, le chiffrement complet du disque ne démarre pas.

Chiffrement des fichiers

Vous pouvez [former des listes à partir de fichiers](#) selon l'extension ou selon les groupes d'extensions ou de dossiers situés sur les disques locaux de l'ordinateur. Vous pouvez aussi créer des [règles de chiffrement de fichiers créés par des applications distinctes](#). Après l'application de la stratégie, l'application Kaspersky Endpoint Security chiffre et déchiffre les fichiers suivants :

- les fichiers ajoutés séparément aux listes pour le chiffrement et le déchiffrement ;
- les fichiers enregistrés dans les dossiers ajoutés aux listes pour le chiffrement et le déchiffrement ;
- les fichiers créés des applications distinctes.

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Le chiffrement des fichiers présente les caractéristiques suivantes :

- Kaspersky Endpoint Security (dé)chiffre les dossiers standards uniquement pour les profils utilisateur locaux du système d'exploitation. Kaspersky Endpoint Security ne (dé)chiffre pas les dossiers standard pour les profils utilisateur itinérant (roaming user profiles), les profils utilisateur obligatoire (mandatory user profiles), les profils utilisateur temporaires (temporary user profiles) et les redirections de dossiers.
- Kaspersky Endpoint Security ne chiffre pas les fichiers dont la modification peut nuire au fonctionnement du système d'exploitation et des programmes installés. Par exemple, la liste des exclusions du chiffrement inclut les fichiers et les dossiers suivants avec tous les dossiers qui y sont joints :
 - %WINDIR% ;
 - %PROGRAMFILES% et %PROGRAMFILES(X86)% ;
 - les fichiers du registre Windows.

La liste des exclusions du chiffrement ne peut pas être consultée et modifiée. Les fichiers et les dossiers de la liste des exclusions du chiffrement peuvent être ajoutés à la liste pour le chiffrement, mais ils ne seront pas chiffrés lors de l'exécution du chiffrement des fichiers.

Paramètres du module Chiffrement des fichiers

| Paramètre | Description |
|--------------------------------------|---|
| Administration du chiffrement | Laisser tel quel. Si vous choisissez cette option, Kaspersky Endpoint Security laisse les fichiers et les dossiers dans le même état. Il ne les chiffre pas ni ne les déchiffre. |

| | |
|--|---|
| | <p>Chiffrer selon les règles. Si vous choisissez cette option, Kaspersky Endpoint Security chiffre les fichiers et les dossiers conformément à la règle de chiffrement, déchiffre les fichiers et les dossiers conformément à la règle de chiffrement et réglemente l'accès des applications aux fichiers chiffrés conformément aux règles pour les applications.</p> <p>Tout déchiffrer. Si vous choisissez cette option, Kaspersky Endpoint Security déchiffre tous les fichiers et les dossiers chiffrés.</p> |
| Règles de chiffrement | <p>Cet onglet affiche les règles de chiffrement des fichiers enregistrés sur les disques locaux. Vous pouvez ajouter des fichiers comme suit :</p> <ul style="list-style-type: none"> • Dossiers standards. Kaspersky Endpoint Security permet d'ajouter les zones suivantes : <ul style="list-style-type: none"> Documents. Fichiers dans le dossier standard <i>Documents</i> du système d'exploitation, ainsi que dans ses sous-dossiers. Favoris. Fichiers dans le dossier standard <i>Favoris</i> du système d'exploitation, ainsi que dans ses sous-dossiers. Bureau. Fichiers dans le dossier standard <i>Bureau</i> du système d'exploitation, ainsi que dans ses sous-dossiers. Fichiers temporaires. Fichiers temporaires associés au fonctionnement des applications installées sur l'ordinateur. Par exemple, les applications Microsoft Office créent des fichiers temporaires avec les copies de sauvegarde des documents. Fichiers Outlook. Fichiers associés au fonctionnement du client de messagerie Outlook : fichiers de données (.pst), fichiers de données hors ligne (.ost), fichiers du carnet d'adresses en mode hors connexion (.ab) et fichiers du carnet d'adresses personnel (.pab). • Dossiers. Vous pouvez également saisir le chemin d'accès au dossier. Lors de l'ajout d'un chemin de dossier, les règles suivantes doivent être suivies : <ul style="list-style-type: none"> Utilisez une variable d'environnement (par exemple, %FOLDER%\UserFolder\). Vous ne pouvez utiliser la variable d'environnement qu'une seule fois et seulement au début du chemin. N'utilisez pas de chemins relatifs. Vous pouvez utiliser l'ensemble <code>\..\</code> (par exemple, C:\Users\..\UserFolder\). L'ensemble <code>\..\</code> indique la transition vers le dossier parent. N'utilisez pas * et ?. N'utilisez pas de chemins UNC. Utilisez ; ou , en guise de séparateur. • Fichiers selon l'extension. Vous pouvez sélectionner des groupes d'extensions dans la liste, par exemple, le groupe d'extensions <i>Archives</i>. Vous pouvez également ajouter l'extension de fichier manuellement. |
| Règles de déchiffrement | <p>Cet onglet affiche les règles de déchiffrement des fichiers enregistrés sur les disques locaux.</p> |
| Règles pour les applications | <p>L'onglet affiche le tableau qui reprend les règles d'accès des applications aux fichiers chiffrés et les règles de chiffrement des fichiers, créés et modifiés par les applications distinctes.</p> |
| Paramètres du mot de passe des archives chiffrées | <p>Paramètres de complexité des mots de passe lors de la création d'archives chiffrées.</p> |

Ce module est disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs.

Kaspersky Endpoint Security prend en charge le chiffrement des fichiers dans les systèmes de fichiers FAT32 et NTFS. Si un disque amovible doté d'un système de fichiers non pris en charge est connecté à l'ordinateur, le chiffrement de ce disque amovible se solde sur une erreur et Kaspersky Endpoint Security lui attribue l'état d'accès "lecture seule".

Pour protéger les données sur des disques amovibles, vous pouvez utiliser les types de chiffrement suivants :

- Chiffrement de disque (FDE).

Chiffrement de l'intégralité du disque amovible, y compris du système de fichiers.

Il n'est pas possible d'accéder aux données chiffrées en dehors du réseau de l'entreprise. Il est également impossible d'accéder aux données chiffrées au sein du réseau de l'entreprise si l'ordinateur n'est pas connecté à Kaspersky Security Center (ordinateur invité).

- Chiffrement de fichiers (FLE).

Chiffrement uniquement des fichiers sur le disque amovible. Le système de fichiers reste inchangé.

Le chiffrement des fichiers sur des disques amovibles permet d'accéder aux données en dehors du réseau de l'entreprise à l'aide d'un mode spécial baptisé [mode portable](#).

Pendant le chiffrement, Kaspersky Endpoint Security crée une clé principale. Kaspersky Endpoint Security enregistre la clé principale dans les stockages suivants :

- Kaspersky Security Center.

- Ordinateur de l'utilisateur.

La clé principale est chiffrée à l'aide de la clé privée de l'utilisateur.

- Disque amovible.

La clé principale est chiffrée à l'aide de la clé publique de Kaspersky Security Center.

Une fois le chiffrement terminé, les données sur le disque amovible sont accessibles au sein du réseau d'entreprise comme si vous utilisiez un disque amovible classique sans chiffrement.

Obtention de l'accès aux données chiffrées

Lorsqu'un disque amovible contenant des données chiffrées est connecté, Kaspersky Endpoint Security exécute les actions suivantes :

1. Recherche la présence éventuelle d'une clé principale dans le stockage local sur l'ordinateur de l'utilisateur.

Si la clé principale existe, l'utilisateur peut accéder aux données sur le disque amovible.

Si la clé principale est introuvable, Kaspersky Endpoint Security exécute les actions suivantes :

a. Il envoie une demande à Kaspersky Security Center.

Après avoir reçu la demande, Kaspersky Security Center envoie une réponse contenant la clé principale.

b. Kaspersky Endpoint Security enregistre la clé principale dans le stockage local sur l'ordinateur de l'utilisateur pour pouvoir ensuite utiliser le disque amovible chiffré.

2. Il déchiffre les données.

Particularités du chiffrement des disques amovibles

Le chiffrement des disques amovibles présente les caractéristiques suivantes :

- Une stratégie avec les paramètres définis de chiffrement des disques amovibles est composée pour un groupe défini d'ordinateurs administrés. Par conséquent, le résultat de l'application de la stratégie de Kaspersky Security Center avec chiffrement/déchiffrement des disques amovibles dépend de l'ordinateur auquel le disque amovible a été connecté.
- Kaspersky Endpoint Security ne (dé)chiffre pas les fichiers avec l'état d'accès "lecture seule" qui sont enregistrés sur les disques amovibles.
- Les types d'appareils suivants sont pris en charge en guise de disques amovibles :
 - supports branchés via le port USB ;
 - disques durs branchés via le port USB ou FireWire ;
 - disques SSD branchés via le port USB ou FireWire.

Paramètres du module Chiffrement des disques amovibles

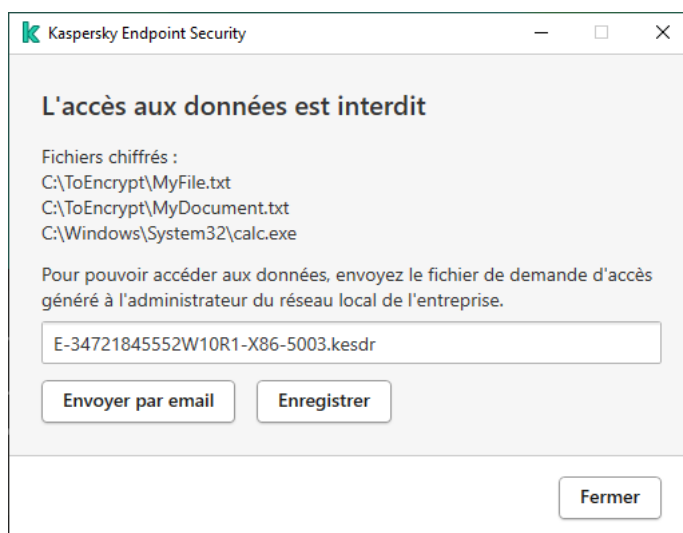
| Paramètre | Description |
|--------------------------------------|--|
| Administration du chiffrement | <p>Chiffrer tout le disque amovible. Si vous choisissez cette option, lors de l'application de la stratégie avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security chiffre les disques amovibles secteur par secteur, y compris leurs systèmes de fichiers.</p> <p>Chiffrer tous les fichiers. Si vous choisissez cette option, lors de l'application de la stratégie avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security chiffre tous les fichiers enregistrés sur les disques amovibles. Kaspersky Endpoint Security ne chiffre pas les fichiers déjà chiffrés. Le contenu du système de fichiers des disques amovibles, y compris les noms des fichiers chiffrés et la structure des dossiers, reste accessible et n'est pas chiffré.</p> <p>Chiffrer uniquement les nouveaux fichiers. Si vous choisissez cette option, lors de l'application de la stratégie avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security chiffre uniquement les fichiers ajoutés aux disques amovibles ou modifiés sur ceux-ci après la dernière application de la stratégie de Kaspersky Security Center. Ce mode de chiffrement s'avère pratique si l'utilisateur utilise ce disque amovible à des fins personnelles et professionnelles. Le mode de chiffrement permet de laisser tous les anciens fichiers inchangés et de chiffrer uniquement les fichiers que l'utilisateur crée sur le poste de travail en utilisant Kaspersky Endpoint Security et la fonction de chiffrement. Ainsi, l'accès aux fichiers personnels est toujours ouvert, que Kaspersky Endpoint Security avec la fonction de chiffrement soit installé ou non sur l'ordinateur.</p> |

| | |
|---|---|
| | <p>Déchiffrer tout le disque amovible. Si vous avez choisi cette option, Kaspersky Endpoint Security, lors de l'application d'une stratégie avec les paramètres définis de chiffrement des disques amovibles, déchiffre tous les fichiers chiffrés qui se trouvent sur les disques amovibles, ainsi que les systèmes de fichiers des disques amovibles s'ils étaient chiffrés.</p> <p>Laisser tel quel. Si vous choisissez cette option, l'application ne modifie pas l'état des disques durs lors de l'application de la stratégie. Si le disque était chiffré, il reste chiffré. Si le disque était déchiffré, il reste déchiffré. L'option est sélectionnée par défaut.</p> |
| <p>Mode portable</p> | <p>La case active ou désactive la préparation du disque amovible qui permet de manipuler les fichiers stockés sur ce disque amovible sur un ordinateur hors du réseau de l'entreprise.</p> <p>Si la case est cochée, lors de l'application d'une stratégie, Kaspersky Endpoint Security requiert la saisie d'un mot de passe avant de lancer le chiffrement des fichiers sur le disque amovible. Le mot de passe est indispensable pour pouvoir accéder aux fichiers chiffrés sur le disque amovible sur des ordinateurs hors du réseau de l'entreprise. Vous pouvez configurer la complexité du mot de passe.</p> <p>Le mode portable est disponible pour les modes Chiffrer tous les fichiers ou Chiffrer uniquement les nouveaux fichiers.</p> |
| <p>Chiffrer uniquement l'espace occupé</p> | <p>La case active ou désactive le mode de chiffrement selon lequel seuls les secteurs occupés du disque sont chiffrés. Ce mode est recommandé pour les nouveaux disques dont les données n'ont pas été modifiées ou supprimées.</p> <p>Si la case est cochée, seule la partie du disque qui contient des fichiers sera chiffrée. Kaspersky Endpoint Security chiffre les nouvelles données automatiquement au fur et à mesure qu'elles sont ajoutées.</p> <p>Si la case est décochée, tout le disque est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant.</p> <p>La fonction de chiffrement réservé à l'espace utilisé est disponible uniquement pour le mode Chiffrer tout le disque amovible.</p> <div data-bbox="427 1256 1493 1413" style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <p>L'activation ou la désactivation de la fonction Chiffrer uniquement l'espace occupé après le lancement du chiffrement ne modifie pas ce paramètre. Il faut cocher ou décocher la case avant le début du chiffrement.</p> </div> |
| <p>Règles de chiffrement des appareils sélectionnés</p> | <p>Tableau des appareils soumis à des règles de chiffrement distinctes. Vous pouvez créer des règles de chiffrement pour des disques amovibles individuels d'une des manières suivantes :</p> <ul style="list-style-type: none"> • Ajoutez un disque amovible à partir de la liste des appareils de confiance du Contrôle des appareils. • Ajoutez un disque amovible manuellement : <ul style="list-style-type: none"> • selon l'identificateur d'appareil (en anglais, Hardware ID - HWID) ; • selon le modèle d'appareil : identifiant de fabricant (en anglais, Vendor ID - VID) et identifiant de produit (en anglais, Product ID - PID). |
| <p>Autoriser le chiffrement des disques amovibles en</p> | <p>Si cette case est cochée, Kaspersky Endpoint Security chiffre les disques amovibles, même en l'absence de connexion à Kaspersky Security Center. Les données nécessaires au déchiffrement des disques amovibles sont alors enregistrées sur le</p> |

| | |
|--|--|
| mode hors ligne | disque dur de l'ordinateur auquel le disque amovible est connecté et ne sont pas transmises à Kaspersky Security Center. Si la case est décochée, Kaspersky Endpoint Security ne chiffre pas les disques amovibles en l'absence de connexion à Kaspersky Security Center. |
| Paramètres du mot de passe du mode portable | Paramètres de sécurité du mot de passe du gestionnaire de fichiers portable |

Modèles (chiffrement des données)

Après le chiffrement des données, Kaspersky Endpoint Security peut interdire l'accès aux données, par exemple, en raison de changements dans l'infrastructure de l'organisation et de changement du Serveur d'administration de Kaspersky Security Center. Si l'utilisateur n'a pas accès aux données chiffrées, il peut solliciter l'accès aux données à l'administrateur. C'est-à-dire que l'utilisateur doit transmettre une requête d'accès au fichier à l'administrateur. Ensuite, l'utilisateur doit télécharger le fichier de réponse fourni par l'administrateur dans Kaspersky Endpoint Security. Kaspersky Endpoint Security vous permet de demander l'accès aux données à l'administrateur par email (cf. ill. ci-dessous).



Demande d'accès aux données chiffrées

Un modèle existe pour signaler l'absence d'accès aux données chiffrées. Pour simplifier la tâche des utilisateurs, il suffit de remplir les champs suivants :

- **À.** Saisissez l'adresse email du groupe d'administrateurs disposant de l'autorisation de chiffrement des données.
- **Objet.** Saisissez l'objet du message avec la demande d'accès aux fichiers chiffrés. Vous pouvez, par exemple, ajouter des balises pour filtrer les messages.
- **Message.** Si nécessaire, modifiez le contenu du message. Vous pouvez utiliser des variables pour obtenir les données nécessaires (par exemple, la variable %USER_NAME%).

Exclusions

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger. Un administrateur peut également autoriser un utilisateur à créer sa propre zone de confiance locale pour un ordinateur particulier. De cette façon, les utilisateurs peuvent créer leurs propres listes locales d'exclusions et d'applications de confiance en plus de la zone de confiance générale proposée par une stratégie.

Exclusions de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Les exclusions de l'analyse permettent d'utiliser des applications légitimes qui pourraient être employées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être exploitées par des individus malintentionnés. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de [l'Encyclopédie de virus de Kaspersky](#).

Kaspersky Endpoint Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des exclusions de l'analyse sur les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque du nom de la menace conformément au classement de l'Encyclopédie des virus de Kaspersky. Par exemple, vous utilisez souvent dans le cadre de votre travail l'application Radmin prévue pour l'administration à distance des ordinateurs. Kaspersky Endpoint Security classe cette activité parmi les activités suspectes et peut la bloquer. Pour exclure le blocage d'une application, il est nécessaire de créer une exclusion de l'analyse dans laquelle vous indiquerez le nom ou le masque du nom selon la classification de l'Encyclopédie des virus de Kaspersky.

Si votre ordinateur est doté d'une application qui récolte et envoie des informations à traiter, Kaspersky Endpoint Security peut la considérer comme une application malveillante. Pour éviter cela, vous pouvez exclure ce programme de l'analyse, en configurant Kaspersky Endpoint Security de manière décrite dans ce document.

Les exclusions de l'analyse peuvent être utilisées pendant le fonctionnement des modules et des tâches suivantes de l'application définis par l'administrateur du système :

- [Détection comportementale](#).
- [Protection contre les Exploits](#).
- [Prévention des intrusions](#).
- [Protection contre les fichiers malicieux](#).
- [Protection contre les menaces Internet](#).
- [Protection contre les menaces par emails](#).
- [Tâches d'analyse](#).

Liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et réseau (y compris l'activité malveillante), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Endpoint Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Cependant, une application qui a été ajoutée à la liste des applications de confiance est exclue des analyses par Kaspersky Endpoint Security.


Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance. L'analyse ignore ensuite les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Endpoint Security considère comme suspectes peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic réseau d'un ordinateur par Kaspersky Endpoint Security et un autre logiciel antivirus) et d'améliorer les performances de l'ordinateur, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autres programmes présentant une menace. Pour exclure entièrement l'application de l'analyse Kaspersky Endpoint Security, il est nécessaire d'utiliser les exclusions de l'analyse.

Paramètres des exclusions

| Paramètre | Description |
|--------------------------------|--|
| Types d'objets détectés | <p>Quelle que soit la configuration des paramètres de Kaspersky Endpoint Security, l'application détecte et bloque toujours les virus, les vers et les chevaux de Troie. Ces programmes peuvent provoquer des dégâts considérables à votre ordinateur.</p> <ul style="list-style-type: none">• Virus, vers  |

Sous-catégorie : virus et vers (Viruses_and_Worms)

Niveau de la menace : élevé

Les virus et les vers classiques exécutent sur l'ordinateur des actions qui n'ont pas été autorisées par l'utilisateur. Ils peuvent créer leurs propres copies qui possèdent la capacité d'auto-reproduction.

Virus classique

Une fois que le virus classique s'est introduit dans un système, il infecte un fichier quelconque, s'y active, exécute son action malveillante, puis ajoute sa copie à d'autres fichiers.

Le virus classique se multiplie uniquement sur les ressources locales de l'ordinateur et il est incapable de s'introduire lui-même dans un autre ordinateur. Il peut pénétrer dans d'autres systèmes uniquement s'il ajoute sa copie dans un fichier enregistré dans un dossier partagé, sur un cédérom d'installation ou si l'utilisateur envoie un email avec le fichier infecté en pièce jointe.

Le code du virus classique peut s'introduire dans divers secteurs de l'ordinateur, du système d'exploitation ou de l'application. En fonction de l'environnement dans lequel ils évoluent, on parle de *virus de fichiers*, *virus de démarrage*, *virus de script* et *virus de macro*.

Les virus peuvent infecter des fichiers de diverses manières. Les virus *écraseurs* (overwriting) remplacent le code du fichier infecté par leur propre code et suppriment ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *parasites* (Parasitic) modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les *virus compagnons* (Companion) ne modifient pas les fichiers mais créent des copies. Lorsque le fichier infecté est exécuté, son double est lancé, à savoir le virus. Il existe également des *virus-liens* (Link), des virus *qui infectent les modules objets* (OBJ), des virus *qui infectent les bibliothèques de compilateur* (LIB), les virus *qui infectent les textes source des programmes* et d'autres.

Ver

Le code du ver, à l'instar de celui du virus classique, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Le ver doit son nom à sa capacité à "ramper" d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

La principale caractéristique qui distingue les vers entre eux est leur mode de diffusion. Le tableau suivant reprend une description des différents types de vers en fonction du mode de diffusion.

Mode de diffusion des vers

| Type | Nom | Description |
|------------|------------|-----------------------------|
| Email-Worm | Email-Worm | Ils se diffusent via email. |

| | | |
|-----------------|--|---|
| | | <p>L'email infecté contient un fichier joint avec la copie du ver ou un lien vers ce fichier sur un site compromis ou créé spécialement à cette fin. Lorsque vous ouvrez le fichier joint, le ver est activé. Lorsque vous cliquez sur le lien, téléchargez le fichier, puis ouvrez celui-ci, le ver commence également à exécuter ses actions malveillantes. Ensuite, il continue à diffuser ses copies après avoir trouvé d'autres adresses email auxquelles il envoie des messages infectés.</p> |
| IRC-Worm | Clients IM | <p>Ils se propagent via les clients IM.</p> <p>En règle générale, ce ver envoie aux contacts un message contenant un lien vers la copie du ver sur un site. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.</p> |
| IRC-Worm | Vers de chats | <p>Ils se diffusent via les canaux IRC (Internet Relay Chats), ces systèmes qui permettent de discuter en temps réel avec d'autres personnes.</p> <p>Ce ver publie un fichier avec sa copie ou un lien vers celle-ci dans le chat. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.</p> |
| Net-Worm | Vers de réseau (vers de réseaux informatiques) | <p>Ils se diffusent via les réseaux informatiques.</p> <p>À la différence des autres types de vers, le ver de réseau se propage sans l'intervention de l'utilisateur. Il recherche une application vulnérable sur les ordinateurs du réseau local. Pour ce faire, il envoie un paquet réseau spécial (un exploit) qui contient le code du ver ou une partie de celui-ci. Si le réseau abrite un ordinateur "vulnérable", celui-ci acceptera le paquet. Une fois qu'il s'est complètement introduit dans cet ordinateur, le ver s'active.</p> |
| P2P-Worm | Vers de réseau d'échange de fichiers | <p>Ils se propagent via les réseaux d'échange de fichiers pair à pair.</p> <p>Afin d'infiltrer le réseau d'échange de fichiers, le ver se copie dans le dossier d'échange de fichiers qui se trouve normalement sur l'ordinateur de l'utilisateur. Le réseau d'échange de fichiers affiche les informations relatives à ce fichier et l'utilisateur peut "trouver" le fichier infecté comme n'importe quel autre fichier, le télécharger puis l'ouvrir.</p> <p>Les vers plus sophistiqués imitent le protocole d'un réseau d'échange de fichiers en particulier : ils répondent positivement aux recherches et proposent leur copie pour le téléchargement.</p> |
| Ver | Autres vers | <p>Parmi ces autres vers, citons :</p> <ul style="list-style-type: none"> • Les vers qui diffusent leur copie via les ressources réseau. À l'aide des fonctions du système d'exploitation, ils consultent les |

répertoires réseau accessibles, se connectent aux ordinateurs du réseau mondial et tentent d'ouvrir leur disque en libre accès. À la différence des types de vers décrits ci-dessus, ces autres vers ne peuvent pas s'activer de manière autonome, mais uniquement lorsque l'utilisateur ouvre le fichier contenant la copie du ver.

- Les vers qui n'adoptent aucun des modes de diffusion décrits dans ce tableau (par exemple, ceux qui se propagent via les téléphones portables).

- [Chevaux de Troie](#) 

Sous-catégories : chevaux de Troie (Trojan_programs)

Niveau de la menace : élevé

À la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie. Ils s'infiltrent sur les ordinateurs via email ou via le navigateur lorsque l'internaute visite un site infecté. Les chevaux de Troie sont exécutés sur intervention de l'utilisateur. Ils entament leur action malveillante directement après l'exécution.

Le comportement des chevaux de Troie sur l'ordinateur infecté varie. Parmi les fonctions principales des chevaux de Troie, citons le blocage, la modification ou la suppression d'informations ainsi que la perturbation du fonctionnement des ordinateurs ou des réseaux. De plus, les chevaux de Troie peuvent recevoir ou envoyer des fichiers, les exécuter, afficher des messages, contacter des pages Internet, télécharger des applications et les installer et redémarrer l'ordinateur.

Les individus malintentionnés utilisent souvent des "sélections" composées de divers chevaux de Troie.

Les types de comportement des chevaux de Troie sont décrits dans le tableau suivant.

Types de comportement des chevaux de Troie sur l'ordinateur infecté

| Type | Nom | Description |
|-----------------------|---|---|
| Trojan-ArcBomb | Chevaux de Troie (bombes dans les archives) | <p>Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur.</p> <p>Lorsque l'utilisateur tente de décompresser une archive de ce genre, l'ordinateur peut commencer à ralentir, voire à s'arrêter et le disque peut se remplir de données "vides". Ces "bombes" sont particulièrement dangereuses pour les serveurs de fichiers et de messagerie. Si le serveur utilise un système de traitement automatique des données entrantes, ce genre de "bombe d'archive" peut entraîner l'arrêt du serveur.</p> |
| Backdoor | Chevaux de Troie pour l'administration à distance | <p>Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs.</p> <p>Ces programmes s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu malintentionné d'administrer l'ordinateur à distance.</p> |
| Trojan | Chevaux de Troie | Cette catégorie reprend les programmes malveillants suivants : |

| | | |
|--------------------------|---|---|
| | | <ul style="list-style-type: none"> • Chevaux de Troie traditionnels. Ils exécutent uniquement les fonctions fondamentales des chevaux de Troie : le blocage, la modification ou la suppression d'informations, la perturbation du fonctionnement des ordinateurs ou des réseaux. Ils ne possèdent pas les fonctions complémentaires caractéristiques d'autres chevaux de Troie décrits dans ce tableau. • Chevaux de Troie "multicibles". Ils possèdent des fonctions complémentaires appartenant à divers types de chevaux de Troie. |
| Trojan-Ransom | Chevaux de Troie exigeant le versement d'une rançon | Ces programmes "prennent en otage" les données de l'ordinateur après les avoir modifiées ou bloquées ou perturbent le fonctionnement de l'ordinateur de telle manière que l'utilisateur n'est plus en mesure d'exploiter les données. L'individu malintentionné exige le versement d'une somme d'argent en échange de l'envoi d'un programme qui rétablira le fonctionnement de l'ordinateur et les données qu'il abrite. |
| Trojan-Clicker | Chevaux de Troie qui cliquent | <p>Ils accèdent à des pages Internet depuis l'ordinateur de la victime : ils envoient des instructions au navigateur ou remplacent les adresses Internet conservées dans les fichiers système.</p> <p>Grâce à ces programmes malveillants, les individus malintentionnés organisent des attaques réseau ou augmentent le nombre de visites sur le site afin d'accroître le nombre d'affichages de bannières publicitaires.</p> |
| Trojan-Downloader | Chevaux de Troie qui téléchargent | Ils accèdent à la page Internet de l'intrus, y téléchargent d'autres applications malveillantes et les installent sur l'ordinateur de l'utilisateur. Ils peuvent contenir le nom du fichier de l'application malveillante à télécharger ou le recevoir à partir de la page Internet consultée. |
| Trojan-Dropper | Chevaux de Troie qui procèdent à des installations | <p>Ils enregistrent sur le disque, puis installent d'autres chevaux de Troie présents dans le corps de ces programmes.</p> <p>Les individus malintentionnés peuvent utiliser ce genre de chevaux de Troie pour :</p> |

| | | |
|------------------------|---|---|
| | | <ul style="list-style-type: none"> • Installer un programme malveillant à l'insu de l'utilisateur : ces chevaux de Troie n'affichent aucun message réel ou fictif (par exemple, messages relatifs à une erreur dans une archive ou à la version incorrecte du système d'exploitation) ; • Protéger un autre programme malveillant connu : tous les antivirus ne sont pas en mesure d'identifier un programme malveillant au sein d'un cheval de Troie qui réalise des installations. |
| Trojan-Notifier | Chevaux de Troie qui envoient des notifications | <p>Ils signalent à l'individu malintentionné que la communication avec l'ordinateur infecté est établie et transmettent des informations relatives à l'ordinateur : adresse IP, numéro du port ouvert ou adresse email. Ils contactent l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens.</p> <p>Ces programmes sont souvent utilisés dans les sélections de différents chevaux de Troie. Ils indiquent à l'individu malintentionné que les autres chevaux de Troie ont bien été installés sur l'ordinateur de l'utilisateur.</p> |
| Trojan-Proxy | Chevaux de Troie faisant office de proxy | Ils permettent à l'individu malintentionné de contacter anonymement des pages Internet via l'ordinateur de la victime ; le plus souvent, ils sont utilisés pour diffuser du spam. |
| Trojan-SMS | Chevaux de Troie qui volent des mots de passe | <p>Il s'agit de chevaux de Troie qui volent des mots de passe (Password Stealing Ware) ; ils volent les données des comptes des utilisateurs, les données d'enregistrement d'un logiciel. Ils recherchent les données confidentielles dans les fichiers système et dans la base de registre et les transmettent à leur "maître" via email ou via FTP sur la page Internet de l'individu malintentionné ou par d'autres méthodes.</p> <p>Certains de ces programmes appartiennent à des groupes particuliers décrits dans ce tableau. Il s'agit des chevaux de Troie qui volent les comptes bancaires (Trojan-Banker), des chevaux de Troie qui volent les données des utilisateurs des clients IM (Trojan-IM) et des chevaux de Troie qui volent les données des adeptes de jeux en ligne (Trojan-GameThief).</p> |
| Trojan-Spy | Chevaux de | Ils espionnent l'utilisateur et collectent |

| | | |
|-------------------------|--|--|
| | Troie espions | des informations sur les actions qu'il effectue lorsqu'il travaille sur son ordinateur. Ils peuvent intercepter les données que l'utilisateur saisit au clavier, faire des captures d'écran ou collecter des listes d'applications actives. Une fois qu'ils ont obtenu ces informations, ils les transmettent à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. |
| Trojan-DDoS | Chevaux de Troie pour attaques réseau | <p>Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). Ces programmes infectent généralement plusieurs ordinateurs pour attaquer simultanément un serveur.</p> <p>Les programmes de type DoS lancent l'attaque depuis un ordinateur avec l'accord de l'utilisateur. Les programmes de type DDoS (Distributed DoS) lancent des attaques distribuées depuis plusieurs ordinateurs, à l'insu de l'utilisateur de l'ordinateur infecté.</p> |
| Trojan-IM | Chevaux de Troie qui volent les données des utilisateurs de clients IM | Ils volent les numéros et les mots de passe des utilisateurs des clients IM. Ils transmettent ces informations à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. |
| Rootkit | Rootkits | Ils masquent d'autres applications malveillantes et leur activité, et prolongent ainsi la persistance de ces applications dans le système d'exploitation. Ils peuvent également dissimuler des fichiers, des processus dans la mémoire d'un ordinateur infecté ou des clés de registre qui exécutent des applications malveillantes. Les rootkits peuvent masquer l'échange de données entre les applications sur l'ordinateur de l'utilisateur et les autres ordinateurs du réseau. |
| Trojan-SMS | Chevaux de Troie qui envoient des messages SMS | Ils infectent des téléphones mobiles et les utilisent pour envoyer des messages SMS vers des numéros payants. |
| Trojan-GameThief | Chevaux de Troie qui volent les données des | Ils volent les comptes des adeptes de jeux en ligne ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. |

| | adeptes de jeux en ligne | |
|---|---|---|
| Trojan-Banker | Chevaux de Troie qui volent les données de comptes bancaires. | Ils volent les données des comptes bancaires ou les données des comptes de système de porte-monnaie électronique ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. |
| Trojan-Mailfinder des adresses email | Chevaux de Troie qui récoltent des adresses email | Ils recueillent les adresses email sur l'ordinateur et les envoient à l'individu malintentionné par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. Les individus malintentionnés utilisent ensuite ces adresses pour diffuser du spam. |

- [Outils malveillants](#) 

Sous-catégories : outils malveillants (Malicious_tools)

Niveau de danger : moyen

Contrairement aux autres types de logiciels malveillants, les outils malveillants n'exécutent pas leurs actions immédiatement après leur démarrage. Elles peuvent être stockées et lancées en toute sécurité sur l'ordinateur de l'utilisateur. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants, s'introduire dans des ordinateurs ou exécuter d'autres actions malveillantes.

Les différentes fonctionnalités des outils malveillants sont regroupées en types présentés dans le tableau suivant.

Fonctionnalités des outils malveillants

| Type | Nom | Description |
|--------------------|-----------------|---|
| Constructor | Constructeurs | Ils permettent de créer de nouveaux virus, vers ou chevaux de Troie. Certains constructeurs sont dotés d'une interface standard à base de fenêtres qui permet, à l'aide de menus, de sélectionner le type de programme malveillant à créer, son mode de résistance face aux débogueurs ainsi que d'autres propriétés. |
| Dos | Attaques réseau | Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). |
| Exploit | Exploits | L'exploit est un ensemble de données ou de code qui exploite une vulnérabilité de l'application dans laquelle il est exécuté afin de réaliser une action malveillante quelconque sur l'ordinateur. Par exemple, un exploit peut écrire ou lire des fichiers ou contacter des pages Internet "infectées". |

| | | |
|--------------------|-------------------------------------|--|
| | | <p>Divers exploits exploitent les vulnérabilités de diverses applications et services réseau. L'exploit sous la forme d'un paquet réseau se transmet via le réseau vers de nombreux ordinateurs à la recherche d'ordinateurs possédant des services réseau vulnérables.</p> <p>L'exploit d'un fichier DOC utilise la vulnérabilité de l'éditeur de test. Il peut commencer à exécuter les fonctions intégrées par l'individu malintentionné lorsque l'utilisateur ouvre le fichier infecté. L'exploit intégré à un email recherche les vulnérabilités dans un client de messagerie quelconque. Il peut commencer à exécuter l'action malveillante dès que l'utilisateur ouvre le message infecté dans le client de messagerie.</p> <p>Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploites de type <i>Nuker</i> sont des paquets réseau qui mettent l'ordinateur hors service.</p> |
| FileCryptor | Encodeurs | Ils encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus. |
| Flooder | Programmes de "pollution" du réseau | <p>Ils envoient une multitude de messages via les canaux réseau. Les programmes utilisés pour polluer les canaux IRC (Internet Relay Chats) appartiennent à cette catégorie.</p> <p>La catégorie Flooder ne reprend pas les applications qui "polluent" l'email, les clients IM et les systèmes mobiles. Ces programmes sont regroupés dans des catégories distinctes décrites dans ce tableau (Email-Flooder, IM-Flooder et SMS-Flooder).</p> |
| HackTool | Outils de piratage | Ils permettent de s'emparer de l'ordinateur sur lequel ils sont installés ou d'attaquer un autre ordinateur (par exemple, ajout d'autres utilisateurs au système sans l'autorisation de la victime ; purge des journaux du système afin de dissimuler les traces de leur présence dans le système). Il s'agit de quelques sniffers qui possèdent des fonctions malveillantes telles que l'interception des mots de passe. Les sniffers sont des programmes qui permettent de consulter le trafic réseau. |
| Hoax | Canulars | Ils effraient l'utilisateur à l'aide de messages semblables à ceux que pourrait produire un virus : ils peuvent |

| | | |
|----------------------|--|---|
| | | découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu. |
| Spoofers | Utilitaires d'imitation | Ils envoient des messages et des requêtes réseau au départ d'adresses fictives. Les individus malintentionnés les utilisent pour se faire passer pour l'expéditeur. |
| VirTool | Instruments pour la modification des programmes malveillants | Ils permettent de modifier d'autres programmes malveillants afin de les rendre invisibles pour les logiciels antivirus. |
| Email-Flooder | Programmes qui "inondent" l'email. | Ils envoient de nombreux messages aux adresses email du carnet d'adresses ("pollution du courrier"). Ce flux important de messages empêche l'utilisateur de lire le courrier utile. |
| SMS-Flooder | Programmes de "pollution" des clients IM | Ils envoient de nombreux messages aux utilisateurs de clients IM. Ce flux important de messages empêche l'utilisateur de lire les messages utiles. |
| SMS-Flooder | Programmes de "pollution" des messages SMS | Ils envoient de nombreux messages SMS vers les téléphones portables. |

- [Applications publicitaires](#) ⓘ

Sous-catégorie : applications publicitaires (Adware)

Niveau de la menace : moyen

Les applications publicitaires montrent des publicités à l'utilisateur. Elles affichent des bannières publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. Certains d'entre elles recueillent également des informations marketing sur l'utilisateur qu'elles renvoient à l'auteur : par exemple, catégorie de sites Internet visités, mots clés utilisés dans les recherches. À la différence des chevaux de Troie espions, elles transmettent ces informations avec l'autorisation de l'utilisateur.

- [Numéroteurs automatiques](#) ⓘ

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

| Type | Nom | Description |
|--------------------|--|---|
| Client-IRC | Clients de chats | Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants. |
| Dialer | Numéroteurs automatiques | Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur. |
| Downloader | Programmes de téléchargement | Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché. |
| Monitor | Programmes de surveillance | Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs). |
| PSWTool | Récupérateur de mots de passe | Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs. |
| RemoteAdmin | Programmes d'administration à distance | Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les |

| | | |
|----------------------|--|--|
| | | ordinateurs distants et de les administrer. Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions. |
| Server-FTP | Serveurs FTP | Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP. |
| Server-Proxy | Serveurs proxy | Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| Server-Telnet | Serveurs Telnet | Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet. |
| Server-Web | Serveurs Internet | Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP. |
| RiskTool | Outils utilisés sur l'ordinateur local | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs. |
| NetTool | Outils réseau | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs. |
| Client-P2P | Clients de réseaux d'échange de fichiers | Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants. |
| Client-SMTP | Clients SMTP | Envient les emails en mode caché. Les individus malintentionnés les |

| | | |
|-------------------|-------------------------|---|
| | | introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| WebToolbar | Barre d'outils Internet | Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche. |
| FraudTool | Pseudo-programmes | Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien. |

- Détecter d'autres applications qui peuvent être utilisées par des individus malintentionnés afin de nuire à l'ordinateur ou aux données de l'utilisateur ²

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

| Type | Nom | Description |
|--------------------|--|---|
| Client-IRC | Clients de chats | Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants. |
| Dialer | Numéroteurs automatiques | Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur. |
| Downloader | Programmes de téléchargement | Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché. |
| Monitor | Programmes de surveillance | Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs). |
| PSWTool | Récupérateur de mots de passe | Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs. |
| RemoteAdmin | Programmes d'administration à distance | Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les |

| | | |
|----------------------|--|--|
| | | ordinateurs distants et de les administrer. Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions. |
| Server-FTP | Serveurs FTP | Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP. |
| Server-Proxy | Serveurs proxy | Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| Server-Telnet | Serveurs Telnet | Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet. |
| Server-Web | Serveurs Internet | Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP. |
| RiskTool | Outils utilisés sur l'ordinateur local | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs. |
| NetTool | Outils réseau | Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs. |
| Client-P2P | Clients de réseaux d'échange de fichiers | Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants. |
| Client-SMTP | Clients SMTP | Envient les emails en mode caché. Les individus malintentionnés les |

| | | |
|-------------------|-------------------------|---|
| | | introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom. |
| WebToolbar | Barre d'outils Internet | Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche. |
| FraudTool | Pseudo-programmes | Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien. |

- [Fichiers compressés pouvant dissimuler un programme malveillant](#)

Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX.

Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois.

Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Kaspersky Endpoint Security identifie les programmes suivants :

- *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie.
- *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.

- [Fichiers compressés à plusieurs reprises](#)

Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX.

Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois.

Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Kaspersky Endpoint Security identifie les programmes suivants :

- *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie.
- *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.

Exclusions

Tableau contenant les informations relatives aux exclusions de l'analyse.

Vous pouvez exclure de l'analyse des objets à l'aide des méthodes suivantes :

- Indiquez le chemin d'accès au fichier ou au dossier.
- Saisissez l'hachage de l'objet.
- Utilisez des masques :
 - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:**.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
 - Deux caractères `**` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier***.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:***.txt` n'est pas un masque valide.
 - Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

| | |
|--|---|
| | <ul style="list-style-type: none"> • Saisissez le nom du type d'objet en fonction de la classification de l'Encyclopédie Kaspersky (par exemple, Vers de courrier, Rootkit ou RemoteAdmin). Vous pouvez utiliser des masques avec le caractère ? (remplace n'importe quel caractère unique) et le caractère * (remplace n'importe quel nombre de caractères). Par exemple, si le masque Client* est spécifié, Kaspersky Endpoint Security exclut les objets Client-IRC, Client-P2P et Client-SMTP des analyses. |
| Applications de confiance | <p>Tableau des applications de confiance dont l'activité n'est pas analysée par Kaspersky Endpoint Security.</p> <p>Le module Contrôle des applications régit le lancement de chacune des applications, que cette application figure ou pas dans le table des applications de confiance.</p> |
| Regrouper les valeurs après l'héritage <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | <p>Ce paramètre permet de fusionner la liste des exclusions d'analyse et des applications de confiance dans les stratégies parents et enfant de Kaspersky Security Center. Pour fusionner des listes, la stratégie enfant doit être configurée de manière à hériter les paramètres de la stratégie parente de Kaspersky Security Center.</p> <p>Si la case est cochée, la liste des éléments de la stratégie parente de Kaspersky Security Center est affichée dans les stratégies enfant. Ainsi, vous pouvez, par exemple, créer une liste d'applications de confiance commune pour l'ensemble de l'organisation.</p> <p>Les éléments de liste hérités dans une stratégie enfant ne peuvent pas être supprimés ni modifiés. Les éléments de la liste des exclusions d'analyse et de la liste des applications de confiance qui sont fusionnés lors de l'héritage ne peuvent pas être supprimés ni modifiés, sauf dans la stratégie parente. Vous pouvez ajouter, modifier ou supprimer des éléments de la liste dans les stratégies de niveau inférieur.</p> <p>Si des éléments des listes de la stratégie enfant et de la stratégie parente correspondent, ces éléments sont affichés comme étant le même élément de la stratégie parente.</p> <p>Si la case n'est pas cochée, les éléments des listes ne sont pas fusionnés lors de l'héritage des paramètres des stratégies de Kaspersky Security Center.</p> |
| Autoriser l'utilisation d'exclusions locales/Autoriser l'utilisation d'applications locales de confiance <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | <p><i>Exclusions locales et applications locales de confiance (zone locale de confiance)</i> : liste d'objets et d'applications définie par l'utilisateur dans Kaspersky Endpoint Security pour un ordinateur particulier. Kaspersky Endpoint Security ne surveille pas les objets ni les applications de la zone de confiance locale. De cette façon, les utilisateurs peuvent créer leurs propres listes locales d'exclusions et d'applications de confiance en plus de la zone de confiance générale d'une stratégie.</p> <p>Si la case est cochée, un utilisateur peut créer une liste locale d'exclusions d'analyse et une liste locale d'applications de confiance. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.</p> <p>Si la case est décochée, un utilisateur ne peut accéder qu'aux listes générales des exclusions d'analyse et des applications de confiance créées dans le cadre de la stratégie. Si des listes locales ont été créées, une fois cette fonctionnalité a été désactivée, Kaspersky Endpoint Security continue d'exclure des analyses les objets figurant dans la liste.</p> |
| Stockage système sécurisé des certificats | <p>Si l'une des boutiques de certificats système de confiance est sélectionnée, Kaspersky Endpoint Security exclut les applications signées avec une signature de confiance numérique des analyses. Kaspersky Endpoint Security attribue automatiquement ces applications au groupe <i>De confiance</i></p> |

Si **Ne pas utiliser** est sélectionné, Kaspersky Endpoint Security analyse les applications, qu'elles aient ou non une signature numérique. Kaspersky Endpoint Security place l'application dans un groupe de confiance en fonction du niveau de danger que cette application peut représenter pour l'ordinateur.

Paramètres de l'application

Vous pouvez configurer les paramètres généraux de l'application suivants :

- mode de fonctionnement ;
- autodéfense ;
- performances ;
- données pour le débogage ;
- État de l'ordinateur à l'application des paramètres

Paramètres de l'application

| Paramètre | Description |
|--|---|
| Lancer Kaspersky Endpoint Security au démarrage de l'ordinateur | <p>Si la case est cochée, Kaspersky Endpoint Security se lance après le démarrage du système d'exploitation et protège l'ordinateur de l'utilisateur tout au long de la session d'utilisation.</p> <p>Lorsque la case est décochée, Kaspersky Endpoint Security ne démarre pas après le chargement du système d'exploitation, tant que l'utilisateur ne le démarre pas manuellement. La protection de l'ordinateur est désactivée et les données des utilisateurs peuvent être exposées à des menaces.</p> |
| Appliquer la technologie de désinfection de l'infection active | <p>Si la case est cochée, une notification contextuelle apparaît à l'écran lorsqu'une activité malveillante est détectée dans le système d'exploitation. Dans sa notification, Kaspersky Endpoint Security propose à l'utilisateur d'effectuer une réparation de l'infection active. Une fois que l'utilisateur a approuvé cette procédure, Kaspersky Endpoint Security neutralise la menace. Une fois la procédure de désinfection avancée terminée, Kaspersky Endpoint Security redémarre l'ordinateur. La technologie de désinfection avancée utilise des ressources informatiques considérables, ce qui peut ralentir d'autres applications.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p>Si Kaspersky Endpoint Security est installé sur un ordinateur fonctionnant sous Windows for Servers, Kaspersky Endpoint Security n'affiche pas la notification. Par conséquent, l'utilisateur ne peut pas sélectionner une action pour désinfecter une menace active. Pour désinfecter une menace, vous devez activer la technologie de désinfection active dans les paramètres de l'application et lancer immédiatement la désinfection active dans les paramètres de la tâche <i>Recherche de virus</i>. Ensuite, vous devez démarrer la tâche <i>Recherche de virus</i>.</p></div> |
| Utiliser Kaspersky Security Center en guise de | <p>Si la case est cochée, le Serveur d'administration de Kaspersky Security Center est utilisé en tant que serveur proxy pour activer l'application.</p> |

| | |
|--|--|
| <p>serveur proxy pour l'activation</p> <p>(disponible uniquement dans Kaspersky Security Center Console)</p> | |
| <p>Activer l'autodéfense</p> | <p>Lorsque cette case est cochée, Kaspersky Endpoint Security empêche la modification ou la suppression des fichiers d'application sur le disque dur, les processus de mémoire et les entrées dans le registre système.</p> |
| <p>Autoriser la gestion des paramètres de Kaspersky Endpoint Security via les applications de contrôle à distance</p> | <p>Si la case est cochée, les applications d'administration à distance de confiance (telles que TeamViewer, LogMeIn Pro et Remotely Anywhere) peuvent modifier les paramètres de Kaspersky Endpoint Security.</p> <p>Les applications d'administration à distance douteuses ne peuvent pas modifier les paramètres de Kaspersky Endpoint Security, même si la case est cochée.</p> |
| <p>Activer le contrôle de service externe</p> | <p>Si la case est cochée, Kaspersky Endpoint Security permet l'administration des services d'application à partir d'un ordinateur à distance. Lorsqu'une tentative est faite pour gérer les services d'application à distance, une notification s'affiche dans la barre des tâches de Microsoft Windows, au-dessus de l'icône de l'application (sauf si le service de notification a été désactivé par l'utilisateur).</p> |
| <p>Reporter les tâches planifiées en cas d'alimentation par batterie</p> | <p>Si la case est cochée, le mode d'économie d'énergie est activé. Kaspersky Endpoint Security reporte les tâches planifiées. Vous pouvez démarrer manuellement les tâches d'analyse et de mise à jour, si nécessaire.</p> |
| <p>Céder les ressources aux autres applications</p> | <p>Quand Kaspersky Endpoint Security exécute des tâches planifiées, la charge sur le processeur et les sous-systèmes de disque peut augmenter, ce qui ralentit les autres programmes.</p> <p>Si la case est cochée, quand la charge augmente, Kaspersky Security suspend l'exécution des tâches programmées et libère des ressources du système d'exploitation pour les autres programmes.</p> |
| <p>Activer l'enregistrement des fichiers de vidage</p> | <p>Si la case est cochée, Kaspersky Endpoint Security écrit des vidages en cas de panne.</p> <p>Si la case est cochée, Kaspersky Endpoint Security n'écrit pas de vidage. L'application supprime également les fichiers de vidage existants du disque dur de l'ordinateur.</p> |
| <p>Activer la protection des fichiers de vidage et des fichiers de traçage</p> | <p>Si la case est cochée, l'accès aux fichiers de vidage est accordé à l'administrateur système et à l'administrateur local ainsi qu'à l'utilisateur qui a activé l'écriture de vidage. Seuls les administrateurs système et locaux peuvent accéder aux fichiers de traçage.</p> <p>Si la case est décochée, tout utilisateur peut accéder aux fichiers de vidage et aux fichiers de traçage.</p> |
| <p>État de l'ordinateur à l'application des paramètres</p> | <p>Les paramètres de l'affichage des états des ordinateurs client doté de l'application Kaspersky Endpoint Security dans Web Console en cas d'erreur d'application de la stratégie ou d'exécution de la tâche. Les états <i>OK</i>, <i>Avertissement</i> et <i>Critique</i> sont disponibles.</p> |

(disponible
uniquement dans
Kaspersky
Security Center
Console)

Rapports et stockage

Rapports

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'exécution de chaque tâche d'analyse, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans des rapports.

Les rapports se trouvent dans le dossier C:\ProgramData\Kaspersky Lab\KES\Report.

Sauvegarde et restauration

La *Sauvegarde* est le stockage qui contient les copies de sauvegarde des objets qui ont été modifiés ou supprimés lors de la désinfection. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier C:\ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès total à ce dossier sont accordées aux utilisateurs du groupe Administrateurs. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Kaspersky Endpoint Security n'offre pas la possibilité de configurer les autorisations d'accès des utilisateurs aux copies de sauvegarde des fichiers.

Paramètres des rapports et du stockage

| Paramètre | Description |
|--|---|
| Supprimer les rapports après X jours | Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des rapports est de 30 jours. À l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport. |
| Limiter la taille du fichier de rapports à X Mo | Si la case est cochée, la taille maximale du fichier de rapport est limitée par la valeur renseignée. Par défaut, la taille maximale du fichier est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale. |
| Supprimer les objets après X jours | Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens de la sauvegarde. |

| | |
|---|--|
| Limiter la taille de la sauvegarde à X Mo | Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 100 Mo. Une fois que la Sauvegarde a atteint sa taille maximale, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens dans afin que le volume de la Sauvegarde ne dépasse plus la valeur maximale. |
| Transfert des données au Serveur d'administration <i>(disponible uniquement dans Kaspersky Security Center)</i> | Les catégories des événements survenus sur les ordinateurs client dont les données doivent être transmises au Serveur d'administration. |

Paramètres du réseau

Vous pouvez configurer les paramètres du serveur proxy pour la connexion à Internet et la mise à jour des bases antivirus, sélectionner le mode de surveillance des ports réseau et configurer l'analyse des connexions protégées.

Options du réseau

| Paramètre | Description |
|---|--|
| Limiter le trafic lors de la connexion limitée | <p>Si la case est cochée, l'application limite son propre trafic réseau si la connexion à Internet est limitée. Kaspersky Endpoint Security définit la connexion mobile à Internet à haut débit comme limitée, la connexion via Wi-Fi comme illimitée.</p> <p>Le Contrôle du trafic Internet fonctionne sur les ordinateurs exécutant Windows 8 ou une version ultérieure.</p> |
| Planter un script dans le trafic Internet pour interagir avec les pages Internet | <p>Si la case est cochée, Kaspersky Endpoint Security plante dans le trafic le script d'interaction avec les pages Internet. Ce script permet de s'assurer que le module Contrôle Internet peut fonctionner correctement. Le script permet l'enregistrement des événements du Contrôle Internet. Sans ce script, il est impossible d'activer la surveillance de l'activité des utilisateurs sur Internet.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Les experts de Kaspersky recommandent d'injecter ce script d'interaction avec les pages Internet dans le trafic pour assurer le bon fonctionnement du Contrôle Internet.</p> </div> |
| Serveur proxy | <p>Paramètres du serveur proxy utilisé pour l'accès à Internet des utilisateurs des ordinateurs clients. Kaspersky Endpoint Security utilise ces paramètres pour certains modules de la protection, notamment pour la mise à jour des bases de données et des modules de l'application.</p> <p>Pour la configuration automatique du serveur proxy, Kaspersky Endpoint Security utilise le protocole WPAD (Web Proxy Auto-Discovery Protocol). Si l'adresse IP du serveur proxy ne peut pas être déterminée à l'aide de ce protocole, Kaspersky Endpoint Security utilise l'adresse du serveur proxy spécifiée dans les paramètres du navigateur Microsoft Internet Explorer.</p> |
| Ne pas utiliser de serveur proxy pour les adresses locales | Si cette case est cochée, Kaspersky Endpoint Security n'utilise pas de serveur proxy lors d'une mise à jour à partir d'un dossier partagé. |

| | |
|---|--|
| <p>Ports contrôlés</p> | <p>Contrôler tous les ports réseau. Le mode de contrôle des ports de réseau via lesquels les modules de la protection (Protection contre les fichiers malicieux, Protection contre les menaces Internet, Protection contre les menaces par emails) contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur.</p> <p>Surveiller uniquement les ports réseau sélectionnés. Dans ce mode de surveillance des ports réseau, les modules de la protection surveillent les ports sélectionnés de l'ordinateur ainsi que l'activité réseau des applications sélectionnées. La liste des ports qui sont normalement utilisés pour le transfert des messages électroniques et le trafic réseau, configurée conformément aux recommandations des experts de Kaspersky.</p> <p>Contrôler tous les ports pour les applications de la liste recommandée par Kaspersky. Ce mode utilise une liste prédéfinie d'applications dont les ports réseau sont surveillés par Kaspersky Endpoint Security. Par exemple, cette liste comprend Google Chrome, Adobe Reader, Java et d'autres applications.</p> <p>Contrôler tous les ports pour les applications indiquées. Ce mode utilise une liste d'applications dont les ports réseau sont surveillés par Kaspersky Endpoint Security.</p> |
| <p>Analyse des connexions chiffrées</p> | <p>Kaspersky Endpoint Security analyse le trafic réseau chiffré transmis via les protocoles suivants :</p> <ul style="list-style-type: none"> • SSL 3.0 ; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. <p>Kaspersky Endpoint Security prend en charge les modes d'analyse des connexions chiffrées suivants :</p> <ul style="list-style-type: none"> • Ne pas analyser les connexions chiffrées Kaspersky Endpoint Security n'aura pas accès au contenu des sites Internet dont l'adresse commence par <code>https://</code>. • Analyser les connexions chiffrées à la demande des modules de la protection. Kaspersky Endpoint Security analysera le trafic chiffré uniquement à la demande des modules Protection contre les fichiers malicieux, Protection contre les menaces par emails et Contrôle Internet. • Toujours analyser les connexions chiffrées Kaspersky Endpoint Security analysera le trafic réseau chiffré même si les modules de la protection sont désactivés. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security n'analyse pas les connexions chiffrées qui ont été établies par des applications de confiance pour lesquelles l'analyse du trafic est désactivée. Kaspersky Endpoint Security n'analyse pas les connexions chiffrées provenant de la liste prédéfinie de sites Internet de confiance. La liste prédéfinie des sites Internet de confiance est créée par les experts de Kaspersky. Cette liste est mise à jour avec les bases antivirus de l'application. Vous pouvez consulter la liste prédéfinie des sites Internet de confiance uniquement dans l'interface de Kaspersky Endpoint Security. Il est impossible de consulter la liste dans Kaspersky Security Center Console.</p> </div> |
| <p>Lors de l'accès à un domaine avec un certificat douteux</p> | <ul style="list-style-type: none"> • Autoriser. Si vous choisissez cette option, Kaspersky Endpoint Security autorise l'établissement d'une connexions réseau lors de l'accès à un domaine avec un certificat douteux. |

| | |
|--|---|
| | <p>Si vous accédez à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui reprend un avertissement et la raison pour laquelle il est déconseillé de visiter ce domaine. Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé. Après que vous avez cliqué sur le lien, Kaspersky Endpoint Security n'affiche plus d'avertissements sur le certificat douteux pendant une heure quand vous accédez à d'autres ressources dans le même domaine.</p> <ul style="list-style-type: none"> • Bloquer la connexion. Si vous choisissez cette option, Kaspersky Endpoint Security bloque l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. <p>Lors de l'accès à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui indique la raison pour laquelle l'accès à ce domaine est bloqué.</p> |
| <p>En cas d'erreur lors de l'analyse des connexions sécurisées</p> | <ul style="list-style-type: none"> • Bloquer la connexion. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée. • Ajouter un domaine aux exclusions. Si vous choisissez cette option, en cas d'erreur lors de l'analyse d'une connexion sécurisée, Kaspersky Endpoint Security ajoute le domaine dont l'accès est à l'origine de l'erreur à la liste des domaines avec erreurs d'analyse et il n'analyse pas le trafic réseau chiffré lors de l'accès à ce domaine. Vous pouvez consulter la liste des domaines contenant des erreurs d'analyse des connexions chiffrées uniquement dans l'interface locale de l'application. Pour réinitialiser le contenu de la liste, sélectionnez l'élément Bloquer la connexion. |
| <p>Bloquer la connexions selon le protocole SSL 2.0</p> | <p>Si cette case est cochée, Kaspersky Endpoint Security bloque les connexions réseau établies via le protocole SSL 2.0.</p> <p>Si cette case est désactivée, Kaspersky Endpoint Security ne bloque pas les connexions réseau établies via le protocole SSL 2.0 et ne surveille pas le trafic réseau transmis via ces connexions.</p> |
| <p>Déchiffrer les connexions chiffrées avec un site à l'aide d'un certificat EV</p> | <p>Les certificats EV (Extended Validation Certificates) confirment l'authenticité des sites Internet et améliorent la sécurité de la connexion. Les navigateurs signalent la présence du certificat EV sur le site à l'aide de l'icône du cadenas dans la ligne d'adresse du navigateur. Les navigateurs peuvent aussi colorer en vert la ligne d'adresse entièrement ou partiellement.</p> <p>Si cette case est cochée, Kaspersky Endpoint Security déchiffre et surveille les connexions chiffrées avec les sites Internet qui utilisent un certificat EV.</p> <p>Si la case est décochée, Kaspersky Endpoint Security n'a pas accès au contenu du trafic HTTPS. Pour cette raison, l'application surveille le trafic HTTPS uniquement en fonction de l'adresse du site Internet, par exemple, <code>https://facebook.com</code>.</p> <p>Si vous ouvrez le site avec le certificat EV pour la première fois, la connexion sécurisée sera déchiffrée peu importe le statut de la case.</p> |
| <p>Adresses de confiance</p> | <p>Ce mode utilise une liste d'adresses Internet pour lesquels Kaspersky Endpoint Security n'analyse pas les connexions réseau. Vous pouvez saisir un nom de domaine ou une adresse IP. Kaspersky Endpoint Security prend en charge le caractère <code>*</code> dans la saisie d'un masque d'identifiant de l'appareil.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security ne prend pas en charge les masques des adresses IP.</p> </div> |



| | |
|---|---|
| | <p>Exemples :</p> <ul style="list-style-type: none"> • <code>domain.com</code> : cette entrée comprend les adresses suivantes : <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. Cette entrée exclut des sous-domaines (par exemple, <code>subdomain.domain.com</code>). • <code>subdomain.domain.com</code> : cette entrée comprend les adresses suivantes : <code>https://subdomain.domain.com</code>, <code>https://subdomain.domain.com/page123</code>. Cette entrée exclut le domaine <code>domain.com</code>. • <code>*.domain.com</code> : cette entrée comprend les adresses suivantes : <code>https://movies.domain.com</code>, <code>https://images.domain.com/page123</code>. Cette entrée exclut le domaine <code>domain.com</code>. |
| <p>Applications de confiance</p> | <p>Liste des applications dont l'activité n'est pas surveillée par Kaspersky Endpoint Security pendant son fonctionnement. Vous pouvez sélectionner les types d'activité de l'application que Kaspersky Endpoint Security ne surveillera pas (par exemple, ne pas analyser le trafic réseau). Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères <code>*</code> et <code>?</code> lors de la saisie d'un masque.</p> |
| <p>Vérifier le trafic sécurisé dans les applications Mozilla</p> <p><i>(disponible uniquement dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Si cette case est cochée, Kaspersky Endpoint Security analyse le trafic chiffré dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird. L'accès à certains sites via le protocole HTTPS peut être bloqué.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Pour analyser le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird, vous devez activer l'analyse des connexions chiffrées. Si l'Analyse des connexions chiffrées est désactivée, Kaspersky Endpoint Security n'analyse pas le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird.</p> </div> <p>Kaspersky Endpoint Security utilise le certificat racine de Kaspersky pour déchiffrer et analyser le trafic chiffré. Vous pouvez sélectionner la boutique de certificats qui contiendra le certificat racine de Kaspersky.</p> <ul style="list-style-type: none"> • Utiliser la boutique des certificats Windows. Le certificat racine de Kaspersky est ajouté à cette boutique lors de l'installation de Kaspersky Endpoint Security. • Utiliser la liste de certificats Mozilla. Mozilla Firefox et Thunderbird utilisent leurs propres boutiques de certificats. Si la boutique de certificats Mozilla est sélectionnée, vous devez ajouter manuellement le certificat racine de Kaspersky à cette boutique via les propriétés du navigateur. |

Interface

Vous pouvez configurer les paramètres de l'interface de l'application.

Paramètres de l'interface

| Paramètre | Description |
|--|---|
| <p>Interaction avec l'utilisateur</p> | <p>Avec interface simplifiée. La fenêtre principale de l'application n'est pas disponible sur l'ordinateur client. Seule l'icône de la zone de notification Windows est disponible. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer une série limitée d'opérations avec Kaspersky Endpoint Security. Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.</p> |

| | |
|--|---|
| <p><i>(disponible uniquement dans Kaspersky Security Center Console)</i></p> | <p>Avec interface complète. La fenêtre principale de Kaspersky Endpoint Security et l'icône de la zone de notification Windows sont disponibles sur l'ordinateur client. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer des opérations avec Kaspersky Endpoint Security. Kaspersky Endpoint Security affiche également des notifications au-dessus de l'icône de l'application.</p> <p>Sans interface. L'ordinateur client n'affiche aucun élément pouvant indiquer le fonctionnement de Kaspersky Endpoint Security. De même, l'icône dans la zone de notification Windows et les notifications ne sont pas disponibles.</p> |
| <p>Paramètres des notifications</p> | <p>Tableau contenant les paramètres de notifications sur les événements de divers niveaux d'importance qui peuvent survenir pendant le fonctionnement d'un module ou de l'application dans son ensemble ou lors de l'exécution d'une tâche. Kaspersky Endpoint Security affiche les notifications relatives à ces événements sur l'écran, les remet par email ou les enregistre dans les journaux.</p> |
| <p>Paramètres des notifications par email</p> | <p>Paramètres du serveur SMTP pour l'envoi de notifications relatives aux événements enregistrés pendant le fonctionnement de l'application.</p> |
| <p>Afficher l'état de l'application dans la zone de notifications</p> | <p>Catégories d'événements de l'application dont l'apparition entraîne la modification de l'icône de Kaspersky Endpoint Security dans la zone de notifications de la barre de tâches de Microsoft Windows ( ou ).</p> |
| <p>Notifications sur l'état des bases antivirus locales</p> | <p>Paramètres de notification sur le caractère dépassé des bases antivirus que l'application utilise.</p> |
| <p>Protection par mot de passe</p> | <p>Si le commutateur est activé, Kaspersky Endpoint Security impose la saisie d'un mot de passe à l'utilisateur tente d'effectuer une opération couverte par la protection par mot de passe. La protection par mot de passe porte sur les opération interdites (par exemple, la désactivation de modules de la protection) et les comptes utilisateur repris dans la zone d'action de la protection par mot de passe.</p> <p>Une fois la Protection par mot de passe activée, Kaspersky Endpoint Security propose de définir un mot de passe pour les opérations.</p> |
| <p>Ressources Internet du Support Technique <i>(disponible uniquement dans Kaspersky Security Center Console)</i></p> | <p>Liste des liens vers les sites Internet contenant des informations sur le Support Technique de l'application Kaspersky Endpoint Security. Les liens ajoutés apparaissent dans la fenêtre Assistance de l'interface locale de Kaspersky Endpoint Security aux côtés des liens standard.</p> |
| <p>Message pour l'utilisateur</p> | <p>Message qui apparaît dans la fenêtre Assistance de l'interface locale de Kaspersky Endpoint Security.</p> |

(disponible
uniquement
dans
Kaspersky
Security
Center
Console)

Gestion des paramètres

Vous pouvez enregistrer les paramètres actuels de Kaspersky Endpoint Security dans un fichier et les utiliser pour configurer rapidement l'application sur un autre ordinateur. Vous pouvez également utiliser un fichier de configuration lorsque vous déployez l'application via Kaspersky Security Center 12 avec un [paquet d'installation](#). Vous pourrez rétablir les paramètres par défaut à tout moment.

Les paramètres d'administration de la configuration des applications ne sont disponibles que dans l'interface de Kaspersky Endpoint Security.

Paramètres d'administration de la configuration des applications

| Paramètres | Description |
|------------------|--|
| Importer | Extraire les paramètres de fonctionnement de l'application depuis un fichier au format CFG et les appliquer. |
| Exporter | Sauvegarder les paramètres actuels de fonctionnement de l'application dans un fichier au format CFG. |
| Restaurer | Vous pouvez à tout moment restaurer les paramètres recommandés de Kaspersky Endpoint Security. Lorsque les paramètres sont restaurés, le niveau de protection Recommandé sera sélectionné pour tous les modules de la protection. |

Gestion de la tâche

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration ;
- des tâches pour la sélection d'ordinateurs.

Vous pouvez créer n'importe quelle quantité de tâches de groupe, de tâches pour une sélection d'ordinateurs et de tâches locales. Pour en savoir plus sur l'utilisation des groupes d'administration et des sélections d'ordinateurs, consultez l'[aide de Kaspersky Security Center](#).

Paramètres de gestion des tâches

| Paramètre | Description |
|------------------------------------|---|
| Autoriser l'utilisation des | Si la case est cochée, les tâches locales sont affichées dans l'interface locale de Kaspersky Endpoint Security. L'utilisateur, en l'absence de restrictions complémentaires de la stratégie, |

| | |
|---|--|
| tâches locales | <p>peut configurer les tâches et les lancer. Cependant, la configuration de la planification de l'exécution des tâches reste indisponible pour l'utilisateur. L'utilisateur ne peut exécuter des tâches que manuellement.</p> <p>Si la case est décochée, l'utilisation des tâches locales est interrompue. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. Les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de Kaspersky Endpoint Security ou via la ligne de commande.</p> <p>L'utilisateur peut toujours lancer la recherche de virus dans un fichier ou un dossier en choisissant l'option Rechercher d'éventuels virus dans le menu contextuel du fichier ou le dossier. Dans ce cas, la tâche d'analyse sera lancée selon les valeurs de paramètres définies par défaut pour la tâche d'analyse personnalisée.</p> |
| Autoriser l'affichage des tâches de groupe | <p>Si la case est cochée, les tâches de groupe sont affichées dans l'interface locale de Kaspersky Endpoint Security. L'utilisateur peut consulter la liste complète des tâches dans l'interface de l'application.</p> <p>Si cette case n'est pas cochée, Kaspersky Endpoint Security affiche une liste de tâches vide.</p> |
| Autoriser la gestion des tâches de groupe | <p>Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans Kaspersky Security Center. L'utilisateur peut lancer et arrêter des tâches dans l'interface de l'application ou dans l'interface simplifiée de l'application.</p> <p>Si cette case n'est pas cochée, Kaspersky Endpoint Security lance automatiquement les tâches selon la planification ou l'administrateur les lance manuellement dans Kaspersky Security Center.</p> |

Analyse de l'ordinateur

La recherche de virus est un élément important dans la protection de l'ordinateur. Elle doit être réalisée régulièrement pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de la protection en raison, par exemple, d'un niveau de sécurité faible ou pour toute autre raison.

Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive et crée des entrées de journal indiquant que ces fichiers n'ont pas été analysés.

Analyse complète

Analyse minutieuse de tout le système. Kaspersky Internet Endpoint analyse les objets suivants :

- Mémoire du noyau
- Objets chargés au lancement du système d'exploitation
- Secteurs d'amorçage
- Sauvegarde du système d'exploitation
- Tous les disques durs et amovibles

Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse de la tâche *Analyse complète*.

Pour économiser les ressources de l'ordinateur, il est conseillé de lancer la tâche d'analyse en arrière-plan au lieu de la tâche d'analyse complète. Le niveau de sécurité de l'ordinateur ne change pas.

Analyse des zones critiques

Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse de la tâche *Analyse des zones critiques*.

Analyse personnalisée

Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :

- Mémoire du noyau
- Objets chargés au lancement du système d'exploitation
- Sauvegarde du système d'exploitation
- Boîte aux lettres Microsoft Outlook
- Disques durs, disques amovibles et disques réseau
- N'importe quel fichier sélectionné

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage, le secteur d'amorçage, la mémoire du système et la partition du système.

Vérification de l'intégrité

Kaspersky Endpoint Security vérifie si les modules de l'application ont été endommagés ou modifiés.

Paramètres d'analyse

| Paramètre | Description |
|---------------------------|--|
| Niveau de sécurité | <p>Kaspersky Endpoint Security peut utiliser différents groupes de paramètres pour lancer une analyse. Ces groupes de paramètres stockés dans l'application sont appelés <i>niveaux de sécurité</i> :</p> <ul style="list-style-type: none">• Élevé. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse de fichiers composés, Kaspersky Endpoint Security analyse également les fichiers au format de messagerie. |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Recommandé. Kaspersky Endpoint Security analyse uniquement les fichiers de formats déterminés sur tous les disques durs, les disques amovibles et les disques réseau de l'ordinateur ainsi que les objets OLE intégrés. Kaspersky Endpoint Security n'analyse pas les archives et les fichiers d'installation. • Faible. Kaspersky Endpoint Security analyse uniquement les nouveaux fichiers et les fichiers modifiés aux extensions définies sur tous les disques durs, amovibles ou réseau de votre ordinateur. Kaspersky Endpoint Security n'analyse pas les fichiers composés. |
| Action en cas de détection d'une menace | <p>Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime.</p> <p>Désinfecter ; bloquer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.</p> <p>Informé. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Avant de tenter de désinfecter ou de supprimer un fichier infecté, Kaspersky Endpoint Security crée une copie de sauvegarde du fichier au cas où vous auriez besoin de restaurer le fichier ou au cas où il pourrait être désinfecté à l'avenir.</p> </div> |
| Zone de protection | Liste des objets analysés par Kaspersky Endpoint Security pendant l'exécution de l'analyse. Les objets analysés peuvent comprendre la mémoire du noyau, les processus en cours d'exécution, les secteurs d'amorçage, le stockage des sauvegardes système, les bases de données de messagerie, le disque dur, le disque amovible ou le disque, dossier ou fichier réseau. |
| Planification de l'analyse | <p>Manuellement. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment.</p> <p>Selon l'horaire. Le mode d'exécution de la tâche d'analyse où Kaspersky Endpoint Security exécute la tâche d'analyse selon la planification que vous avez créée. Si ce mode d'exécution de la tâche d'analyse est sélectionné, vous pouvez également lancer la tâche d'analyse manuellement.</p> |
| Lancer les tâches ignorées <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | <p>Si la case est cochée, Kaspersky Endpoint Security exécute la tâche d'analyse manquée dès que cela est possible. La tâche d'analyse peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche d'analyse.</p> <p>Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches d'analyse ignorées. Au lieu de cela, il effectue la prochaine tâche d'analyse conformément à la planification en cours.</p> |
| Exécuter lorsque l'ordinateur est inactif | Début différé de la tâche d'analyse lorsque les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security lance la tâche d'analyse si l'ordinateur est verrouillé ou si l'écran de veille est activé. |
| Lancer | Par défaut, la tâche d'analyse est exécutée au nom de l'utilisateur avec les droits duquel |

| | |
|--|---|
| <p>l'analyse en tant que</p> | <p>vous êtes enregistré dans le système d'exploitation. La protection étendue peut inclure des lecteurs réseau ou d'autres objets spéciaux qui nécessitent des droits d'accès. Vous pouvez définir un utilisateur qui possède les droits requis dans les paramètres de Kaspersky Endpoint Security et exécuter la tâche d'analyse sous le compte de cet utilisateur.</p> |
| <p>Types de fichiers</p> | <div data-bbox="384 315 1493 472" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Les fichiers sans extension sont considérés par Kaspersky Endpoint Security comme des fichiers exécutables. Kaspersky Endpoint Security analyse toujours les fichiers exécutables, quel que soit le type de fichiers que vous avez sélectionné pour l'analyse.</p> </div> <p>Tous les fichiers. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension).</p> <p>Fichiers analysés par format. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables. Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Pendant l'analyse, l'extension du fichier est également prise en compte.</p> <p>Fichiers analysés selon l'extension. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables. Le format du fichier sera déterminé sur la base de son extension.</p> |
| <p>Analyser uniquement les nouveaux fichiers et les fichiers modifiés</p> | <p>Analyse uniquement les nouveaux fichiers et les fichiers qui ont été modifiés depuis la dernière fois qu'ils ont été analysés. Cela permettra de réduire la durée de l'analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.</p> |
| <p>Ignorer les fichiers si l'analyse dure plus de X secondes</p> | <p>Limite la durée de numérisation d'un seul objet. À l'issue du temps indiqué, Kaspersky Endpoint Security termine l'analyse du fichier. Cela permettra de réduire la durée de l'analyse.</p> |
| <p>Analyser les archives</p> | <p>Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE.</p> |
| <p>Analyser les paquets de distribution</p> | <p>La case active/désactive l'analyse des paquets de distribution des logiciels tiers.</p> |
| <p>Analyser les fichiers aux formats Microsoft Office</p> | <p>Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE.</p> |
| <p>Analyser les fichiers au format de messagerie</p> | <p>La case active/désactive la fonction à l'aide de laquelle Kaspersky Endpoint Security analyse les fichiers au format de messagerie, ainsi que les bases de données de messagerie.</p> <p>L'application ne scanne que les formats de fichiers de messagerie MS Outlook, Windows Mail/Outlook Express et EML et seulement si l'ordinateur possède le client de messagerie MS Outlook x86.</p> <p>Si la case est cochée, Kaspersky Endpoint Security décompose le fichier au format de messagerie (en-tête, corps, pièces jointes) et effectue la recherche des menaces éventuelles.</p> |

| | |
|---|---|
| | Si la case est décochée, Kaspersky Endpoint Security analyse le fichier au format de messagerie comme un fichier unique. |
| Analyser les archives protégées par un mot de passe | <p>Si la case est cochée, Kaspersky Endpoint Security analyse les archives protégées par un mot de passe. Avant l'analyse des fichiers stockés dans une archive, l'écran affiche la demande du mot de passe.</p> <p>Si la case est décochée, Kaspersky Endpoint Security exclut de l'analyse les archives protégées par un mot de passe.</p> |
| Ne pas décompresser les fichiers composés de grande taille | <p>Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie.</p> <p>Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille.</p> <p>Kaspersky Endpoint Security analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.</p> |
| Machine learning et analyse sur la base de signature | <p>Machine learning et l'analyse sur la base de signatures utilisent les bases de Kaspersky Endpoint Security qui contiennent les descriptions des menaces connues et les méthodes de désinfection. La protection à l'aide de cette méthode d'analyse garantit le niveau de sécurité minimal admissible.</p> <p>Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.</p> |
| Analyse heuristique | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| Technologie iSwift | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS. |
| Technologie iChecker | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage, le secteur d'amorçage, la mémoire du système et la partition du système. L'Analyse en arrière-plan est lancée dans les cas suivants :

- après la mise à jour des bases antivirus ;
- trente minutes après le lancement de Kaspersky Endpoint Security ;
- toutes les six heures ;
- lorsque l'ordinateur est inactif pendant cinq minutes ou plus (l'ordinateur est verrouillé ou l'écran de veille est allumé).

L'analyse en arrière-plan réalisée quand l'ordinateur est en veille est interrompue lorsque l'une des conditions suivantes est remplie :

- L'ordinateur est réactivé.

Si l'analyse en arrière-plan n'a pas été réalisée depuis plus de dix jours, l'analyse n'est pas interrompue.

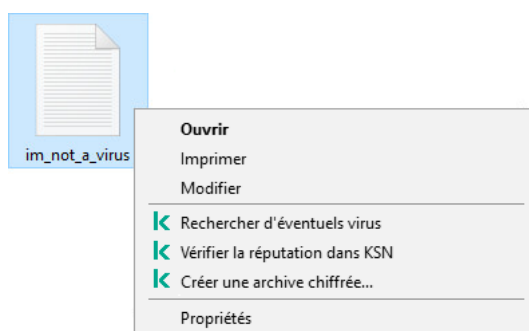
- L'ordinateur (ordinateur portable) est passé en mode batterie.

Lors de l'analyse en arrière-plan, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.

Analyse depuis le menu contextuel

Kaspersky Endpoint Security vous permet d'analyser des fichiers individuels à la recherche de virus et autres programmes constituant une menace via le menu contextuel (cf. ill. ci-dessous).

Lors de l'exécution de l'analyse depuis le menu contextuel, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.



Analyse depuis le menu contextuel

Paramètres de la tâche Analyse depuis le menu contextuel

| Paramètre | Description |
|--|---|
| Action en cas de détection d'une menace | Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. |

| | |
|---|---|
| | <p>Désinfecter ; bloquer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.</p> <p>Informé. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.</p> |
| Analyser uniquement les nouveaux fichiers et les fichiers modifiés | Analyse uniquement les nouveaux fichiers et les fichiers qui ont été modifiés depuis la dernière fois qu'ils ont été analysés. Cela permettra de réduire la durée de l'analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. |
| Ignorer les fichiers si l'analyse dure plus de X s. | Limite la durée de numérisation d'un seul objet. À l'issue du temps indiqué, Kaspersky Endpoint Security termine l'analyse du fichier. Cela permettra de réduire la durée de l'analyse. |
| Analyser les archives | Analyse les archives dans les formats suivants : RAR, ARJ, ZIP, CAB, LHA, JAR et ICE. |
| Analyser les paquets de distribution | La case active/désactive l'analyse des paquets de distribution. |
| Analyser les fichiers aux formats Microsoft Office | Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. |
| Ne pas décompresser les fichiers composés de grande taille | Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. |
| Machine learning et analyse sur la base de signatures | <p>Machine learning et l'analyse sur la base de signatures utilisent les bases de Kaspersky Endpoint Security qui contiennent les descriptions des menaces connues et les méthodes de désinfection. La protection à l'aide de cette méthode d'analyse garantit le niveau de sécurité minimal admissible.</p> <p>Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.</p> |
| Analyse heuristique | <p>Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.</p> <p>Lors de l'analyse de fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions qui sont exécutées par l'analyseur heuristique dépend du niveau spécifié pour l'analyseur heuristique. Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge des ressources du système d'exploitation et la durée de l'analyse heuristique.</p> |
| Technologie iSwift | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure |

| | |
|-----------------------------|---|
| | de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS. |
| Technologie iChecker | La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus des analyses à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux fichiers dont la structure est connue de l'application (exemple : aux fichiers du format EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR). |

Analyse des disques amovibles

Kaspersky Endpoint Security prend en charge la recherche de virus et d'autres programmes présentant une menace sur les disques amovibles lors de leur connexion à l'ordinateur.

Paramètres de la tâche Analyse des disques amovibles

| Paramètre | Description |
|--|---|
| Action à exécuter lors de la connexion d'un disque amovible | <ul style="list-style-type: none"> • Ne pas analyser. • Analyse approfondie Si vous choisissez cette option, Kaspersky Endpoint Security analyse tous les fichiers situés sur le disque amovible, y compris les fichiers joints à l'intérieur des objets composés, dès que le disque amovible a été connecté. • Analyse rapide Si vous choisissez cette option, Kaspersky Endpoint Security analyse uniquement les fichiers de certains formats les plus exposés à l'infection et il ne décompacte pas les objets composés dès que le disque amovible a été connecté. |
| Taille maximale du disque amovible | <p>Si la case est cochée, Kaspersky Endpoint Security exécute l'action sélectionnée dans la liste déroulante Action à exécuter lors de la connexion d'un disque amovible sur les disques amovibles dont la taille est inférieure à la taille maximale définie.</p> <p>Si cette case est décochée, Kaspersky Endpoint Security exécute l'action sélectionnée dans la liste déroulante Action à exécuter lors de la connexion d'un disque amovible sur tous les disques amovibles quelle que soit leur taille.</p> |
| Afficher la progression de l'analyse | <p>Si la case est cochée, Kaspersky Endpoint Security affiche la progression de l'analyse des disques amovibles dans une nouvelle fenêtre et dans la fenêtre Tâches.</p> <p>Si la case est décochée, Kaspersky Endpoint Security exécute l'analyse des disques amovibles en arrière-plan.</p> |
| Interdire l'arrêt de la tâche d'analyse | <p>Si la case est cochée, le bouton Arrêter de la fenêtre Tâches et le bouton Arrêter de la fenêtre Recherche de virus ne sont pas disponibles dans l'interface locale de Kaspersky Endpoint Security pour la tâche d'analyse des disques amovibles.</p> |

Vérification de l'intégrité

Kaspersky Endpoint Security vérifie si les fichiers de l'application, situés dans le dossier d'installation de l'application, ont été endommagés ou modifiés. Par exemple, si la bibliothèque de l'application possède une signature numérique incorrecte, cette bibliothèque est considérée comme endommagée. La tâche *Vérification de l'intégrité* sert à l'analyse des fichiers de l'application. Exécutez la tâche *Vérification de l'intégrité* si Kaspersky Endpoint Security a détecté un objet malveillant et ne l'a pas neutralisé.

Vous pouvez créer la tâche *Vérification de l'intégrité* dans Kaspersky Security Center 12 Web Console et dans la Console d'administration. Il est impossible de créer une tâche dans Kaspersky Security Center Cloud Console.

L'intégrité de l'application peut être compromise par exemple dans les cas suivants :

- Un objet malveillant a modifié les fichiers de Kaspersky Endpoint Security. Dans ce cas, lancez la procédure de récupération pour Kaspersky Endpoint Security à l'aide des outils du système d'exploitation. Après la récupération, exécutez une analyse complète de l'ordinateur et répétez la vérification de l'intégrité.
- La signature numérique a expiré. Dans ce cas, mettez à jour Kaspersky Endpoint Security.

Paramètres de la tâche de vérification de l'intégrité

| Paramètre | Description |
|--|---|
| Planification de l'analyse | <p>Manuelle. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment.</p> <p>Selon l'horaire. Le mode d'exécution de la tâche d'analyse où Kaspersky Endpoint Security exécute la tâche d'analyse selon la planification que vous avez créée. Si ce mode d'exécution de la tâche d'analyse est sélectionné, vous pouvez également lancer la tâche d'analyse manuellement.</p> |
| Lancer les tâches non exécutées | <p>Si la case est cochée, Kaspersky Endpoint Security exécute la tâche d'analyse manquée dès que cela est possible. La tâche d'analyse peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche d'analyse.</p> <p>Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches d'analyse ignorées. Au lieu de cela, il effectue la prochaine tâche d'analyse conformément à la planification en cours.</p> |
| Exécuter lorsque l'ordinateur est inactif | <p>Début différé de la tâche d'analyse lorsque les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security lance la tâche d'analyse si l'ordinateur est verrouillé ou si l'écran de veille est activé.</p> |
| Lancer en tant que <i>(disponible uniquement dans Kaspersky Security Center Console)</i> | <p>Par défaut, la tâche d'analyse est exécutée au nom de l'utilisateur avec les droits duquel vous êtes enregistré dans le système d'exploitation. Il se peut que des autorisations spéciales soient exigées pour accéder au dossier d'installation de l'application. Vous pouvez définir un utilisateur qui possède les droits requis dans les paramètres de Kaspersky Endpoint Security et exécuter la tâche d'analyse sous le compte de cet utilisateur.</p> |

Mise à jour des bases de données et des modules de l'application

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

Pour une mise à jour régulière, il faut une licence valide de l'application. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Les serveurs de mise à jour de Kaspersky sont la principale source de mise à jour pour Kaspersky Endpoint Security.

Pour réussir le téléchargement du paquet de mise à jour depuis les serveurs de mise à jour de Kaspersky, l'ordinateur doit être connecté à l'Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, vous devez configurer les paramètres du serveur proxy.

Le téléchargement des mises à jour s'opère selon le protocole HTTPS. Le téléchargement selon le protocole HTTP est possible quand le téléchargement des mises à jour selon le protocole HTTPS est impossible.

Lors de la mise à jour, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Les bases de Kaspersky Endpoint Security. La protection de l'ordinateur est garantie par l'utilisation de bases de données qui contiennent les signatures des virus et autres programmes présentant une menace ainsi que les informations sur les moyens de lutter contre elles. Ces informations sont utilisées par les modules de la protection pour rechercher sur votre ordinateur les objets dangereux et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des menaces qui apparaissent et les moyens de lutter contre celles-ci. Pour cette raison, il est recommandé d'actualiser régulièrement les bases.

En plus des bases de Kaspersky Endpoint Security, la mise à jour concerne également les pilotes réseau qui assurent l'interception du trafic réseau par les modules de la protection.

- Modules de l'application. Outre les bases de Kaspersky Endpoint Security, il est possible d'actualiser les modules de l'application. Les mises à jour des modules de l'application permettent de supprimer les vulnérabilités de Kaspersky Endpoint Security, ajoutent de nouvelles fonctionnalités ou améliorent les fonctionnalités existantes.

Pendant la mise à jour, les bases et les modules de l'application installés sur votre ordinateur sont comparés à la dernière version stockée à la source des mises à jour. Si les bases et les modules de l'application actuels diffèrent de la dernière version, la partie manquante sera installée sur l'ordinateur.

La mise à jour des modules de l'application peut s'accompagner de la mise à jour de l'aide contextuelle de l'application.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Les informations sur l'état actuel des bases de Kaspersky Endpoint Security s'affichent dans le groupe **Mise à jour** de la fenêtre **Tâches**.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le [rapport de Kaspersky Endpoint Security](#).

| Paramètre | Description |
|--|--|
| Mode d'exécution | <p>Automatique. Le mode d'exécution de la tâche de mise à jour où Kaspersky Endpoint Security vérifie la présence du paquet des mises à jour dans la source des mises à jour avec la fréquence indiquée. L'intervalle de vérification de la présence du paquet des mises à jour est augmenté en cas d'épidémie et réduit en situation normale. Dès qu'il détecte un nouveau paquet de mise à jour, Kaspersky Endpoint Security le télécharge et l'installe sur l'ordinateur.</p> <p>Manuelle. Ce mode d'exécution de la tâche de mise à jour permet de lancer la tâche de mise à jour manuellement.</p> <p>Selon l'horaire. Le mode d'exécution de la tâche de mise à jour où Kaspersky Endpoint Security exécute la tâche de mise à jour selon la planification que vous avez créée. Si ce mode d'exécution de la tâche de mise à jour est sélectionné, vous pouvez également lancer la tâche de mise à jour de Kaspersky Endpoint Security manuellement.</p> |
| Lancer les tâches non exécutées | <p>Si la case est cochée, Kaspersky Endpoint Security exécute la tâche de mise à jour manquée dès que cela est possible. La tâche de mise à jour peut être manquée si, par exemple, l'ordinateur était éteint à l'heure indiquée.</p> <p>Si la case est décochée, Kaspersky Endpoint Security ne lance pas les tâches de mise à jour non effectuées. Au lieu de cela, il exécute la tâche de mise à jour suivante conformément à la planification en cours.</p> |
| Source des mises à jour | <p><i>La source des mises à jour</i> est une ressource qui contient les mises à jour des bases et des modules de l'application de Kaspersky Endpoint Security.</p> <p>La source des mises à jour inclut le serveur Kaspersky Security Center, les serveurs de mises à jour de Kaspersky et des dossiers locaux ou réseau.</p> <p>La liste des sources des mises à jour contient par défaut le serveur Kaspersky Security Center et les serveurs de mises à jour de Kaspersky. Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés.</p> <div data-bbox="352 1216 1493 1339" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security ne prend pas en charge les mises à jour des serveurs HTTPS sauf s'il s'agit des serveurs de mise à jour de Kaspersky.</p> </div> <p>Si plusieurs ressources ont été sélectionnées en tant que sources des mises à jour, Kaspersky Endpoint Security les consultera pendant la mise à jour dans l'ordre de la liste et exécute la tâche de mise à jour en utilisant le paquet de mise à jour de la première source de mise à jour disponible.</p> |
| Lancer la tâche avec les privilèges de l'utilisateur | <p>Par défaut, la tâche de mise à jour de Kaspersky Endpoint Security est lancée au nom de l'utilisateur que vous avez utilisé pour ouvrir votre session dans le système d'exploitation. Cependant, la mise à jour de Kaspersky Endpoint Security peut se dérouler depuis une source à laquelle l'utilisateur n'a pas accès (par exemple, depuis un dossier partagé contenant le paquet des mises à jour) ou pour laquelle l'utilisation de l'authentification sur le serveur proxy n'a pas été configurée. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de Kaspersky Endpoint Security et lancer la tâche de mise à jour de Kaspersky Endpoint Security au nom de cet utilisateur.</p> |
| Télécharger les mises à jour des modules de l'application | <p>La case active ou désactive le téléchargement des mises à jour des modules de l'application en même temps que les mises à jour des bases de données de l'application.</p> <p>Si la case est cochée, Kaspersky Endpoint Security signale à l'utilisateur l'existence de mises à jour disponibles pour les modules de l'application et, pendant l'exécution de la tâche de mise à jour, il inclut les mises à jour des modules de l'application dans le paquet de mises à jour. Ainsi, l'application des mises à jour des modules est définie par les paramètres suivants :</p> <ul style="list-style-type: none"> • Installer les mises à jour critiques et approuvées. Si cette option est sélectionnée et que des mises à jour des modules de l'application sont disponibles, Kaspersky Endpoint |

| | |
|---|---|
| | <p>Security installe les mises à jour critiques automatiquement tandis qu'il installera les autres mises à jour uniquement après approbation de leur installation locale via l'interface de l'application ou le Kaspersky Security Center.</p> <ul style="list-style-type: none"> • Installer uniquement les mises à jour approuvées. Si cette option est sélectionnée et que des mises à jour des modules sont disponibles, Kaspersky Endpoint Security les installe après approbation de leur application, localement via l'interface de l'application ou depuis le Kaspersky Security Center. Cette option est sélectionnée par défaut. <p>Si la case n'est pas cochée, Kaspersky Endpoint Security ne signale pas à l'utilisateur la présence de mises à jour disponibles pour l'application et pendant l'exécution de la tâche, il n'inclut pas les mises à jour des modules de l'application dans le paquet de mises à jour.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Si la mise à jour des modules de l'application implique la lecture et l'acceptation de dispositions du Contrat de licence utilisateur final, l'application installera ces mises à jour après l'acceptation de ces dispositions.</p> </div> <p>La case est cochée par défaut.</p> |
| <p>Copier les mises à jour dans le dossier</p> | <p>Si la case est cochée, Kaspersky Endpoint Security copie le paquet de mises à jour dans le dossier partagé indiqué sous la case. Après, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé. Ceci permet de limiter le trafic Internet, car il suffit de télécharger le paquet de mise à jour une seule fois. Le dossier suivant est repris par défaut : C:\ProgramData\Kaspersky Lab\KES\Update distribution\.</p> |
| <p>Serveur proxy pour les mises à jour <i>(disponible uniquement dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Paramètres du serveur proxy pour l'accès Internet des utilisateurs des postes clients permettant de mettre à jour les modules d'application ainsi que les bases de données.</p> <p>Pour la configuration automatique du serveur proxy, Kaspersky Endpoint Security utilise le protocole WPAD (Web Proxy Auto-Discovery Protocol). Si l'adresse IP du serveur proxy ne peut pas être déterminée à l'aide de ce protocole, Kaspersky Endpoint Security utilise l'adresse du serveur proxy spécifiée dans les paramètres du navigateur Microsoft Internet Explorer.</p> |
| <p>Ne pas utiliser de serveur proxy pour les adresses locales <i>(disponible uniquement dans l'interface de Kaspersky Endpoint Security)</i></p> | <p>Si cette case est cochée, Kaspersky Endpoint Security n'utilise pas de serveur proxy lors d'une mise à jour à partir d'un dossier partagé.</p> |

Annexe 2. Groupes de confiance d'applications

Kaspersky Endpoint Security répartit toutes les applications lancées sur l'ordinateur en groupes de confiance. Les applications sont réparties en groupes de confiance selon le degré de menace que ces applications peuvent représenter pour le système d'exploitation.

Les zones de confiances suivantes sont :

- **De confiance.** Ce groupe reprend les applications qui satisfont à une ou plusieurs des conditions suivantes :
 - Les applications sont dotées de la signature numérique d'un éditeur de confiance.
 - La base des applications de confiance de Kaspersky Security Network contient des enregistrements relatifs à ces applications.
 - L'utilisateur a placé les applications dans le groupe "De confiance".

Il n'existe aucune opération interdite pour ces applications.

- **Restrictions faibles.** Ce groupe reprend les applications qui satisfont aux conditions suivantes :
 - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
 - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
 - L'utilisateur a placé les applications dans le groupe "Restrictions faibles".

Il existe des restrictions minimales sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.

- **Restrictions élevées.** Ce groupe reprend les applications qui satisfont aux conditions suivantes :
 - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
 - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
 - L'utilisateur a placé les applications dans le groupe "Restrictions élevées".

Il existe des restrictions considérables sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.

- **Douteuses.** Ce groupe reprend les applications qui satisfont aux conditions suivantes :
 - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
 - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
 - L'utilisateur a placé les applications dans le groupe "Douteuses".

Pour ces applications, toutes les opérations sont interdites.

Annexe 3. Extensions de fichiers pour l'analyse rapide des disques amovibles

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64 Ko ;

exe : fichier exécutable, archive autoextractible ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase™, Clipper ou Microsoft Visual FoxPro®, programme de la suite WAVmaker ;

bin : fichier binaire ;

bat : fichier de paquet ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compressée ;

dll : bibliothèque dynamique ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme qui fonctionne en mode de partage du temps ;

drv : pilote d'un appareil quelconque ;

vxd : pilote d'un appareil virtuel Microsoft Windows ;

pif : fichier contenant des informations sur un logiciel ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registre de Microsoft Windows ;

ini : fichier de configuration qui contient les données des paramètres pour Microsoft Windows, Windows NT et pour certaines applications ;

cla : classe Java ;

vbs : script Visual Basic® ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer® ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

eml : email de Microsoft Outlook Express ;

nws : nouvel email de Microsoft Outlook Express ;

msg : email de Microsoft Mail ;

plg : email ;

mbx : email Microsoft Office Outlook enregistré ;

doc* : documents Microsoft Office Word, par exemple, doc : document Microsoft Office Word, docx : document Microsoft Office Word 2007 compatible avec XML, docm : document Microsoft Office Word 2007 compatible avec les macros ;

dot* : modèles de document Microsoft Office Word, par exemple, dot : modèle de document Microsoft Office Word, dotx : modèle de document Microsoft Office Word 2007, dotm : modèle de document Microsoft Office Word 2007 compatible avec les macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Windows Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD® ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave® Flash ;

jpg, jpeg : fichier graphique de conservation de données compressées ;

emf : fichier au format Enhanced Metafile ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutables Microsoft Office Word ;

xl* : les documents et les fichiers de Microsoft Office Excel, tels que, xla : extension Microsoft Excel, xlc : schéma, xlt : modèle des documents, xlsx : feuille de calcul Microsoft Office Excel 2007, xlsm : feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, xlsb : feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), xltx : modèle Microsoft Office Excel 2007, xlsx : modèle Microsoft Office Excel 2007 compatible avec les macros, xlam : modèle externe Microsoft Office Excel 2007 compatible avec les macros ;

pp* : les documents et les fichiers de Microsoft Office PowerPoint®, tels que, pps : diaporama Microsoft Office PowerPoint, ppt : présentation, pptx : présentation Microsoft Office PowerPoint 2007, pptm : présentation Microsoft Office PowerPoint 2007 compatible avec les macros, potx : modèle de présentation Microsoft Office PowerPoint 2007, potm : modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, ppsx : diaporama Microsoft Office PowerPoint 2007, ppsm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, ppam : module externe Microsoft Office PowerPoint 2007 compatible avec les macros ;

md* : documents et fichiers de Microsoft Office Access® tels que, mda : groupe de travail de Microsoft Office Access, mdb : base de données ;

sldx : diaporama Microsoft Office PowerPoint 2007 ;

sldm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros ;

thmx : thème Microsoft Office 2007.

Annexe 4. Types de fichiers pour le filtre de pièces jointes de Protection contre les menaces par emails

N'oubliez pas que le format réel du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

Si vous avez activé le filtrage des pièces jointes dans les messages électroniques, le module Protection contre les menaces par emails peut, à l'issue de celui-ci, renommer ou supprimer les fichiers portant les extensions suivantes :

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64 Ko ;

exe : fichier exécutable, archive autoextractible ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase™, Clipper ou Microsoft Visual FoxPro®, programme de la suite WAVmaker ;

bin : fichier binaire ;

bat : fichier de paquet ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compressée ;

dll : bibliothèque dynamique ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme qui fonctionne en mode de partage du temps ;

drv : pilote d'un appareil quelconque ;

vxd : pilote d'un appareil virtuel Microsoft Windows ;

pif : fichier contenant des informations sur un logiciel ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registre de Microsoft Windows ;

ini : fichier de configuration qui contient les données des paramètres pour Microsoft Windows, Windows NT et pour certaines applications ;

cla : classe Java ;

vbs : script Visual Basic® ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer® ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

eml : email de Microsoft Outlook Express ;

nws : nouvel email de Microsoft Outlook Express ;

msg : email de Microsoft Mail ;

plg : email ;

mbx : email Microsoft Office Outlook enregistré ;

doc* : documents Microsoft Office Word, par exemple, doc : document Microsoft Office Word, docx : document Microsoft Office Word 2007 compatible avec XML, docm : document Microsoft Office Word 2007 compatible avec les macros ;

dot* : modèles de document Microsoft Office Word, par exemple, dot : modèle de document Microsoft Office Word, dotx : modèle de document Microsoft Office Word 2007, dotm : modèle de document Microsoft Office Word 2007 compatible avec les macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Windows Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD® ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave® Flash ;

jpg, jpeg : fichier graphique de conservation de données compressées ;

emf : fichier au format Enhanced Metafile ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutables Microsoft Office Word ;

xl* : les documents et les fichiers de Microsoft Office Excel, tels que, xla : extension Microsoft Excel, xlc : schéma, xlt : modèle des documents, xlsx : feuille de calcul Microsoft Office Excel 2007, xlsm : feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, xlsb : feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), xltx : modèle Microsoft Office Excel 2007, xlsx : modèle Microsoft Office Excel 2007 compatible avec les macros, xlam : modèle externe Microsoft Office Excel 2007 compatible avec les macros ;

pp* : les documents et les fichiers de Microsoft Office PowerPoint®, tels que, pps : diaporama Microsoft Office PowerPoint, ppt : présentation, pptx : présentation Microsoft Office PowerPoint 2007, pptm : présentation Microsoft Office PowerPoint 2007 compatible avec les macros, potx : modèle de présentation Microsoft Office PowerPoint 2007, potm : modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, ppsx : diaporama Microsoft Office PowerPoint 2007, ppsm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, ppam : module externe Microsoft Office PowerPoint 2007 compatible avec les macros ;

md* : documents et fichiers de Microsoft Office Access® tels que, mda : groupe de travail de Microsoft Office Access, mdb : base de données ;

sldx : diaporama Microsoft Office PowerPoint 2007 ;

sldm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros ;

thmx : thème Microsoft Office 2007.

Annexe 5. Paramètres de réseau pour l'interaction avec les services externes

Kaspersky Endpoint Security utilise les paramètres réseau suivants pour interagir avec les services externes.

Paramètres du réseau

| Adresse | Description |
|---|---|
| activation- v2.kaspersky.com/activation-service/activation-service.svc Protocole : HTTPS Port : 443 | Activation de l'application |
| s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com | Mise à jour des bases et des modules d'application en cours |

s17.upd.kaspersky.com
s18.upd.kaspersky.com
s19.upd.kaspersky.com
cm.k.kaspersky-labs.com

Protocole : HTTPS

Port : 443

downloads.upd.kaspersky.com

Protocole : HTTPS

Port : 443

- Mise à jour des bases et des modules d'application en cours
- Vérification de l'accessibilité des serveurs Kaspersky. Si l'accès aux serveurs à l'aide du DNS du système n'est pas possible, l'application utilise le DNS public. Cette mesure est nécessaire pour s'assurer que les bases de données antivirus sont mises à jour et que le niveau de sécurité de l'ordinateur est maintenu. Kaspersky Endpoint Security utilise la liste suivante de serveurs DNS publics dans l'ordre suivant :

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).

| | |
|--|---|
| | <p>Les requêtes émises par l'application peuvent contenir des adresses de domaines et l'adresse IP publique de l'utilisateur parce que l'application établit une connexion TCP/UDP avec le serveur DNS. Ces informations sont nécessaires, par exemple, pour valider le certificat d'une ressource Internet lors de l'utilisation du protocole HTTPS. Si Kaspersky Endpoint Security utilise un serveur DNS public, le traitement des données est régi par la politique de confidentialité du service concerné. Si vous voulez empêcher Kaspersky Endpoint Security d'utiliser un serveur DNS public, contactez le Support Technique pour obtenir un correctif privé.</p> |
| <p>touch.kaspersky.com Protocole : HTTP</p> | <ul style="list-style-type: none"> • Réception du temps de confiance pour vérifier la période de validité du certificat (connexion TLS). • Avertissement concernant le refus d'accès à une ressource Internet dans le navigateur (Protection contre les menaces Internet et Contrôle Internet) |
| <p>p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com</p> | <p>Mise à jour des bases et des modules d'application en cours</p> |

| | |
|--|---|
| <p>p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com</p> <p>Protocole : HTTP Port : 80</p> | |
| <p>ds.kaspersky.com</p> <p>Protocole : HTTPS Port : 443</p> | Utilisation de Kaspersky Security Network |
| <p>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</p> <p>Protocole : Quelconque Port : 443, 1443</p> | Utilisation de Kaspersky Security Network |
| <p>click.kaspersky.com redirect.kaspersky.com</p> <p>Protocole : HTTPS</p> | Suivez les liens de l'interface |
| <p>cr1.kaspersky.com ocsp.kaspersky.com</p> <p>Protocole : HTTP Port : 80</p> | Infrastructure à clés publiques (ICP) |

Annexe 6. Événements relatifs à l'application dans le journal des événements Windows

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'exécution de chaque tâche d'analyse, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans le journal des événements Windows.

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|---|-------------------|
| 201 | Le Contrat de licence utilisateur final n'a pas été respecté | ✓ |
| 203 | La durée de validité de la licence expire bientôt | – |
| 204 | La licence expire bientôt | – |
| 206 | Les bases sont endommagées ou manquantes | – |
| 207 | Les bases sont fortement dépassées | – |
| 208 | Les bases sont dépassées | – |
| 209 | Le lancement automatique de l'application est désactivé | – |
| 210 | La mise à jour automatique est désactivée | – |
| 211 | L'Autodéfense est désactivée | – |
| 212 | Impossible d'exécuter la tâche | – |
| 213 | L'action sur les ressources de l'application est bloquée par l'Autodéfense | – |
| 214 | Les modules de protection sont désactivés | – |
| 215 | L'ordinateur fonctionne en mode sans échec | – |
| 216 | Il y a des fichiers non traités | – |
| 217 | Le rapport a été purgé | ✓ |
| 218 | Les paramètres de l'application ont été modifiés | ✓ |
| 219 | Une stratégie de groupe a été appliquée | ✓ |
| 220 | La stratégie de groupe est désactivée | – |
| 221 | La tâche a été lancée | – |
| 222 | La tâche a été interrompue | – |
| 223 | La tâche est terminée | – |
| 224 | Le redémarrage de l'application est requis pour terminer la mise à jour | – |
| 225 | Le redémarrage de l'ordinateur est requis | ✓ |
| 226 | Certains des modules de l'application autorisés par la licence ne sont pas installés | – |
| 227 | Les modules installés correspondent à la licence | – |
| 229 | Erreur d'activation | ✓ |
| 230 | Le code d'activation de réserve est incorrect | – |
| 231 | Une menace active a été détectée, la procédure de désinfection de l'infection active doit être lancée | – |
| 232 | La procédure de désinfection de l'infection active a été lancée | – |
| 233 | La procédure de désinfection de l'infection active est terminée | – |
| 235 | L'application a été lancée | ✓ |

| | | |
|------|--|---|
| 236 | L'application a été arrêtée | ✓ |
| 237 | Une panne de la session antérieure de l'application a été détectée | ✓ |
| 240 | La licence expire bientôt | ✓ |
| 238 | Les paramètres de l'abonnement ont été modifiés | ✓ |
| 239 | L'abonnement a été renouvelé | ✓ |
| 335 | L'objet a été restauré à partir de la Sauvegarde | ✓ |
| 336 | Impossible de restaurer l'objet à partir de la Sauvegarde | ✓ |
| 245 | Le traitement par l'application de certaines fonctions du système d'exploitation est désactivé | ✓ |
| 250 | Une connexion chiffrée a été interrompue | ✓ |
| 708 | Les paramètres de la tâche ont bien été appliqués | – |
| 335 | L'objet a été restauré à partir de la Sauvegarde | ✓ |
| 2000 | Saisissez un nom d'utilisateur et un mot de passe | – |
| 2001 | Une activité réseau suspecte a été détectée | – |
| 2020 | La participation à KSN est activée | – |
| 2021 | La participation à KSN est désactivée | – |
| 2022 | Les serveurs de KSN sont disponibles | – |
| 2023 | Les serveurs de KSN sont indisponibles | – |
| 2024 | L'application fonctionne conformément à la législation locale et utilise l'infrastructure locale | ✓ |
| 227 | Tous les modules de l'application, admis par la licence, sont installés et fonctionnent en mode normal | – |

Détection comportementale

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |
| 307 | L'objet a été supprimé | – |
| 308 | Une copie de sauvegarde de l'objet a été créée | – |
| 311 | Impossible de créer la copie de sauvegarde de l'objet | – |
| 313 | Suppression impossible | – |
| 323 | L'objet sera supprimé au redémarrage | – |
| 329 | L'objet a été renommé | – |
| 331 | Interdit | – |
| 452 | Le processus est terminé | – |
| 453 | Impossible de terminer le processus | – |
| 455 | Le retour à l'état antérieur a été exécuté | – |
| 458 | La valeur du registre a été restaurée | – |
| 459 | La valeur du registre a été supprimée | – |
| 453 | L'exécution du fichier/code est interdite | – |

Protection contre les Exploits 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 302 | Un objet malveillant a été détecté | – |
| 331 | Interdit | – |
| 455 | Le retour à l'état antérieur a été exécuté | – |
| 323 | L'objet sera supprimé au redémarrage | – |
| 307 | L'objet a été supprimé | – |
| 329 | L'objet a été renommé | – |
| 457 | Le fichier a été restauré | – |
| 458 | La valeur du registre a été restaurée | – |
| 459 | La valeur du registre a été supprimée | – |

Prévention des intrusions 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 301 | Un objet a été traité | – |
| 302 | Un objet malveillant a été détecté | – |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |
| 306 | L'objet a été désinfecté | – |
| 307 | L'objet a été supprimé | – |
| 308 | Une copie de sauvegarde de l'objet a été créée | – |
| 310 | Impossible de créer la copie de sauvegarde de l'objet | – |
| 312 | Désinfection impossible | – |
| 313 | Suppression impossible | – |
| 314 | L'objet n'a pas été traité | – |
| 315 | L'objet a été ignoré | – |
| 317 | Erreur de traitement | ✓ |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 320 | L'objet est chiffré | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 323 | L'objet sera supprimé au redémarrage | – |
| 324 | L'objet sera désinfecté au redémarrage | – |
| 327 | L'objet a été écrasé par une copie désinfectée auparavant | – |
| 332 | Informations relatives à l'objet détecté | – |
| 335 | L'objet a été restauré à partir de la Sauvegarde | – |
| 336 | Impossible de restaurer l'objet à partir de la Sauvegarde | ✓ |
| 340 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 401 | L'application est placée dans le groupe des applications de confiance | – |
| 402 | L'application a été placée dans un groupe à privilèges restreints | – |
| 403 | Déclenchement du module Prévention des intrusions | – |
| 452 | Le processus est terminé | – |
| 453 | Impossible de terminer le processus | – |

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 302 | Un objet malveillant a été détecté | ✓ |
| 317 | Erreur de traitement | ✓ |
| 336 | Impossible de restaurer l'objet à partir de la Sauvegarde | ✓ |
| 340 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 301 | Un objet a été traité | – |
| 306 | L'objet a été désinfecté | – |
| 307 | L'objet a été supprimé | – |
| 308 | Une copie de sauvegarde de l'objet a été créée | – |
| 310 | Impossible de créer la copie de sauvegarde de l'objet | – |
| 312 | Désinfection impossible | – |
| 313 | Suppression impossible | – |
| 314 | L'objet n'a pas été traité | – |
| 315 | L'objet a été ignoré | – |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 320 | L'objet est chiffré | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 323 | L'objet sera supprimé au redémarrage | – |
| 324 | L'objet sera désinfecté au redémarrage | – |
| 325 | L'objet a été écrasé par une copie désinfectée auparavant | – |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |
| 329 | L'objet a été renommé | – |
| 335 | L'objet a été restauré à partir de la Sauvegarde | – |
| 452 | Le processus est terminé | – |
| 453 | Impossible de terminer le processus | – |
| 332 | Informations relatives à l'objet détecté | – |

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 301 | Un objet a été traité | – |
| 302 | Un objet malveillant a été détecté | ✓ |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |
| 317 | Erreur de traitement | ✓ |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 329 | L'objet a été renommé | – |
| 362 | Un lien dangereux a été bloqué | ✓ |
| 1201 | Un lien dangereux ouvert précédemment a été détecté | ✓ |
| 1211 | Un lien malveillant ouvert précédemment a été détecté | ✓ |
| 363 | Un lien dangereux a été ouvert | ✓ |
| 341 | Le téléchargement de l'objet est interdit | – |
| 370 | Le lien se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 370 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 332 | Informations relatives à l'objet détecté | – |

[Protection contre les menaces par emails](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 301 | Un objet a été traité | – |
| 306 | L'objet a été désinfecté | – |
| 302 | Un objet malveillant a été détecté | ✓ |
| 317 | Erreur de traitement | ✓ |
| 340 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 307 | L'objet a été supprimé | – |
| 308 | Une copie de sauvegarde de l'objet a été créée | – |
| 312 | Désinfection impossible | – |
| 314 | L'objet n'a pas été traité | – |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 329 | L'objet a été renommé | – |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ont été détectés | – |
| 332 | Informations relatives à l'objet détecté | – |

Firewall ⓘ

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|---------------------------------|-------------------|
| 601 | L'activité réseau est autorisée | – |
| 602 | L'activité réseau est interdite | – |

Protection contre les menaces réseau ⓘ

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|-----------------------------------|-------------------|
| 651 | Une attaque réseau a été détectée | – |

Protection BadUSB ⓘ

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|----------------------------------|-------------------|
| 2050 | Le clavier a été autorisé | – |
| 2051 | Le clavier n'est pas autorisé | ✓ |
| 2052 | Erreur d'autorisation du clavier | ✓ |

[Protection AMSI](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 301 | Un objet a été traité | – |
| 302 | Un objet malveillant a été détecté | ✓ |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |
| 314 | L'objet n'a pas été traité | – |
| 315 | L'objet a été ignoré | – |
| 317 | Erreur de traitement | ✓ |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 320 | L'objet est chiffré | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 1512 | Le résultat de l'analyse de l'objet a été transmis à une application tierce | – |
| 329 | L'objet a été renommé | – |
| 332 | Informations relatives à l'objet détecté | – |
| 340 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 2200 | Une requête AMSI a été bloquée | ✓ |

[Contrôle des applications](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|---|-------------------|
| 701 | Le lancement de l'application est autorisé | – |
| 702 | Le lancement de l'application est interdit | – |
| 703 | Le lancement de l'application est interdit en mode test | – |
| 704 | Le lancement de l'application est autorisé en mode test | – |
| 707 | Erreur dans le paramétrage des tâches. Les paramètres des tâches ne sont pas appliqués | – |
| 710 | Le processus interdit a été lancé avant le démarrage de Kaspersky Endpoint Security for Windows | – |
| 708 | Les paramètres de la tâche ont bien été appliqués | – |

[Contrôle des appareils ?](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|---|-------------------|
| 801 | L'opération sur l'appareil est autorisée | – |
| 802 | L'opération sur l'appareil est interdite | – |
| 803 | L'accès temporaire à l'appareil est activé | ✓ |
| 808 | Une opération a été exécutée sur un fichier | – |
| 809 | La connexion réseau est interdite | – |

[Contrôle Internet ?](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 751 | L'accès est autorisé | – |
| 752 | L'accès est interdit | – |
| 753 | Avertissement sur le contenu indésirable | – |
| 754 | Le contenu indésirable a été consulté après un avertissement | – |
| 751 | La page autorisée est ouverte | – |

[Contrôle évolutif des anomalies ?](#)

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 501 | Plainte concernant le blocage de l'activité de l'application | – |
| 2201 | L'action du processus a été ignorée | – |
| 2200 | L'action du processus a été bloquée | ✓ |

[Chiffrement des données](#) 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 904 | Erreur d'application des règles de chiffrement/déchiffrement des fichiers | ✓ |
| 912 | Erreur de chiffrement/déchiffrement des fichiers | ✓ |
| 1305 | Erreur de chiffrement/déchiffrement de l'appareil | ✓ |
| 931 | Erreur de création de l'archive chiffrée | ✓ |
| 951 | Erreur d'activation du mode portable | ✓ |
| 953 | Erreur de désactivation du mode portable | ✓ |
| 1311 | Échec du chargement du module de chiffrement | ✓ |
| 1340 | La tâche de gestion des comptes utilisateur de l'Agent d'authentification a échoué | ✓ |
| 1312 | La stratégie ne peut pas être appliquée | ✓ |
| 1342 | La mise à jour de la fonction de chiffrement s'est soldée par une erreur | ✓ |
| 1343 | La restauration de la mise à jour de la fonction de chiffrement a réussi | ✓ |
| 1345 | Échec de l'installation ou de la mise à jour des pilotes de Kaspersky Disk Encryption dans l'image WinRE | ✓ |
| 1346 | Échec de la désinstallation des pilotes de Kaspersky Disk Encryption dans l'image WinRE | ✓ |
| 1370 | La clé de récupération BitLocker a été modifiée | ✓ |
| 901 | L'application des règles de chiffrement/déchiffrement des fichiers est en cours | – |
| 902 | L'application des règles de chiffrement/déchiffrement des fichiers est terminée | – |
| 903 | L'application des règles de chiffrement/déchiffrement des fichiers a été interrompue | – |
| 905 | L'application des règles de chiffrement/déchiffrement des fichiers a été reprise | – |
| 910 | L'opération de chiffrement/déchiffrement du fichier a été lancée | – |
| 911 | L'opération de chiffrement/déchiffrement du fichier est terminée | – |
| 913 | Le fichier n'a pas été chiffré, car il s'agit d'une exclusion | – |
| 914 | L'opération de chiffrement/déchiffrement du fichier a été interrompue | – |
| 1301 | Lancement de l'opération de chiffrement/déchiffrement de l'appareil | – |
| 1302 | L'opération de chiffrement/déchiffrement de l'appareil est terminée | – |
| 1307 | L'appareil n'est pas chiffré | – |
| 1303 | Le chiffrement/déchiffrement de l'appareil a été interrompu | – |
| 1304 | Le chiffrement/déchiffrement de l'appareil a été repris | – |
| 1309 | Le processus de chiffrement/déchiffrement du disque est passé en mode passif | – |

| | | |
|------|---|---|
| 1308 | Le processus de chiffrement/déchiffrement de l'appareil est passé en mode actif | - |
| 1306 | L'utilisateur a refusé la stratégie de chiffrement | - |
| 940 | L'accès au fichier est bloqué | ✓ |
| 950 | Le mode portable est activé | - |
| 952 | Le mode portable est désactivé | - |
| 1330 | Un compte utilisateur de l'Agent d'authentification a été créé | - |
| 1337 | Le compte n'a pas été ajouté. Ce compte existe déjà | - |
| 1338 | Le compte n'a pas été modifié. Ce compte n'existe pas | - |
| 1339 | Le compte n'a pas été supprimé. Ce compte n'existe pas | - |
| 1331 | Un compte utilisateur de l'Agent d'authentification a été supprimé | - |
| 1332 | Le mot de passe du compte utilisateur de l'Agent d'authentification a été modifié | - |
| 1334 | L'authentification dans l'Agent d'authentification s'est soldée par une erreur | - |
| 1333 | L'authentification dans l'Agent d'authentification a réussi | - |
| 1335 | L'accès au disque dur a été obtenu à l'aide de la procédure de demande d'accès aux appareils chiffrés | - |
| 1336 | La tentative d'accès au disque dur à l'aide de la procédure de demande d'accès aux appareils chiffrés s'est soldée par une erreur | - |
| 1310 | Le module de chiffrement a été chargé | - |
| 1344 | Échec de la restauration de la mise à jour de la fonctionnalité de chiffrement | ✓ |
| 1341 | La mise à jour de la fonction de chiffrement a réussi | ✓ |
| 1332 | Le mot de passe du compte utilisateur de l'Agent d'authentification a été modifié | - |

[Endpoint Sensor](#) 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 2100 | Le serveur Kaspersky Anti Targeted Attack Platform est inaccessible | – |
| 2105 | Le lancement de l'application a été bloqué | ✓ |
| 2106 | L'ouverture du document a été bloquée | ✓ |
| 2104 | Les tâches à partir du serveur Kaspersky Anti Targeted Attack Platform sont en cours de traitement | – |
| 2103 | Les tâches à partir du serveur Kaspersky Anti Targeted Attack Platform ne sont pas traitées | – |
| 2101 | Endpoint Sensor est connecté au serveur | – |
| 2102 | La connexion au serveur Kaspersky Anti Targeted Attack Platform a été rétablie | – |
| 2112 | Tous les processus lancés depuis le fichier image ou le flux ont été arrêtés | ✓ |
| 2113 | L'application a été lancée | ✓ |
| 2111 | Un fichier ou un flux a été supprimé par l'administrateur du serveur de Kaspersky Anti Targeted Attack Platform | ✓ |
| 2110 | Un fichier a été restauré par l'administrateur à partir de la quarantaine du serveur Kaspersky Anti Targeted Attack Platform | ✓ |
| 2109 | Un fichier est mis en quarantaine par l'administrateur sur le serveur de Kaspersky Anti Targeted Attack Platform | ✓ |
| 2107 | L'activité réseau des applications d'éditeurs tiers est bloquée | ✓ |
| 2108 | L'activité réseau des applications d'éditeurs tiers est débloquée | ✓ |

[Analyse de l'ordinateur](#) 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 302 | Un objet malveillant a été détecté | ✓ |
| 335 | L'objet a été restauré à partir de la Sauvegarde | ✓ |
| 336 | Impossible de restaurer l'objet à partir de la Sauvegarde | ✓ |
| 340 | L'objet se trouve dans la liste d'autorisation dans le KSN privé | ✓ |
| 301 | Un objet a été traité | – |
| 329 | L'objet a été renommé | – |
| 306 | L'objet a été désinfecté | – |
| 307 | L'objet a été supprimé | – |
| 308 | Une copie de sauvegarde de l'objet a été créée | – |
| 310 | Impossible de créer la copie de sauvegarde de l'objet | – |
| 312 | Désinfection impossible | – |
| 313 | Suppression impossible | – |
| 314 | L'objet n'a pas été traité | – |
| 315 | L'objet a été ignoré | – |
| 317 | Erreur de traitement | – |
| 318 | Une archive a été détectée | – |
| 319 | Un objet compressé a été détecté | – |
| 320 | L'objet est chiffré | – |
| 321 | L'objet est endommagé | – |
| 322 | Une archive protégée par un mot de passe a été détectée | – |
| 323 | L'objet sera supprimé au redémarrage | – |
| 324 | L'objet sera désinfecté au redémarrage | – |
| 327 | L'objet a été écrasé par une copie désinfectée auparavant | – |
| 303 | Des logiciels légitimes que des attaquants pourraient exploiter pour nuire à votre ordinateur ou à vos données personnelles ont été détectés | – |

Vérification de l'intégrité 

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 2002 | Échec de la vérification de la signature du module système | – |

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|--|-------------------|
| 101 | Une erreur interne est survenue | ✓ |
| 1001 | La source de mises à jour a été sélectionnée | – |
| 1002 | Le serveur proxy a été sélectionné | – |
| 1003 | Téléchargement du fichier | – |
| 1004 | Le fichier a été téléchargé | – |
| 1005 | Le fichier a été installé | – |
| 1006 | Le fichier a été mis à jour | – |
| 1007 | Le fichier a été remis à l'état antérieur en raison d'une erreur de mise à jour | – |
| 1008 | Mise à jour des fichiers | – |
| 1009 | Copie des mises à jour | – |
| 1010 | Remise à l'état antérieur des fichiers | – |
| 1011 | Erreur de mise à jour du module | – |
| 1012 | Erreur de copie des mises à jour du module | – |
| 1013 | Création de la liste des fichiers à télécharger | – |
| 1014 | Erreur locale de mise à jour | – |
| 1016 | L'utilisateur a annulé l'opération | – |
| 1017 | Impossible de lancer deux tâches simultanément | – |
| 1018 | Erreur d'analyse des bases et des modules de l'application | – |
| 1019 | Erreur d'interaction avec Kaspersky Security Center | – |
| 1020 | Aucune mise à jour n'est disponible | – |
| 1021 | Certains modules n'ont pas été mis à jour | – |
| 1022 | La copie des mises à jour a réussi | – |
| 1023 | La mise à jour a réussi tandis que la copie des mises à jour s'est soldée par un échec | – |
| 2153 | Erreur d'installation du correctif | – |
| 2156 | Erreur d'annulation du correctif | – |
| 2150 | Téléchargement des correctifs | – |
| 2151 | Installation des correctifs | – |
| 2152 | Un correctif a été installé | – |
| 2154 | Annulation du correctif | – |
| 2155 | Annulation du correctif terminée | – |

Suppression des données

Codes des événements

| Identifiant de l'événement | Description | Activé par défaut |
|----------------------------|---|-------------------|
| 223 | La tâche est terminée | – |
| 221 | La tâche a été lancée | – |
| 222 | La tâche a été interrompue | – |
| 2252 | Impossible de supprimer l'objet | – |
| 2253 | Statistiques de la tâche de suppression | – |
| 2251 | L'objet a été supprimé | – |

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier `legal_notices.txt` situé dans le dossier d'installation de l'application.

Notice sur les marques de commerce

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash, Reader et Shockwave sont des marques ou des marques déposées d'Adobe Systems Incorporated enregistrées aux États-Unis et/ou dans d'autres pays.

Apple, FireWire, iTunes et Safari sont des marques d'Apple Inc. déposées aux États-Unis et dans d'autres pays.

AutoCAD est une marque ou une marque déposée aux États-Unis et/ou dans d'autres pays qui appartient à Autodesk, Inc. et/ou à ses filiales.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Borland est une marque ou une marque déposée de Borland Software Corporation.

Android et Google Chrome sont des marques de commerce de Google, Inc.

Citrix, Citrix Provisioning Services et XenDesktop sont des marques de Citrix Systems, Inc. et/ou de ses filiales déposées à l'office des brevets des États-Unis et d'autres pays.

Dell est une marque de commerce de Dell, Inc. ou de ses filiales.

dBase est une marque de dataBased Intelligence, Inc.

EMC est une marque de commerce ou une marque déposée d'EMC Corporation aux États-Unis et/ou dans d'autres pays.

Radmin est une marque déposée de Famatech.

IBM est une marque d'International Business Machines Corporation déposées dans plusieurs juridictions à travers le monde.

ICQ est une marque ou une marque de service de ICQ LLC.

Intel est une marque d'Intel Corporation déposée aux États-Unis et dans d'autres pays.

IOS est une marque déposée de Cisco Systems, Inc. et/ou de ses filiales déposées aux États-Unis et dans d'autres pays.

Lenovo et ThinkPad sont des marques commerciales de Lenovo aux États-Unis et/ou dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux États-Unis et dans d'autres pays.

Logitech est une marque ou une marque déposée de Logitech aux États-Unis et/ou dans d'autres pays.

LogMeIn Pro et Remotely Anywhere sont des marques déposées de LogMeIn, Inc.

Mail.ru est une marque déposée de Mail.Ru, LLC.

McAfee est une marque de commerce ou une marque déposée de McAfee, Inc. aux États-Unis et dans d'autres pays.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface et Hyper-V sont des marques de commerce de Microsoft Corporation déposées aux États-Unis et dans d'autres pays.

Mozilla, Firefox et Thunderbird sont des marques de Mozilla Foundation.

Java et JavaScript sont des marques déposées de la société Oracle et/ou de ses filiales.

VERISIGN est une marque déposée aux États-Unis et dans d'autres pays ou une marque non déposée de VeriSign, Inc. et de ses filiales.

VMware et VMware ESXi sont des marques de VMware, Inc. ou des marques déposées de VMware, Inc. aux États-Unis ou dans d'autres juridictions

Thawte est une marque de commerce ou une marque déposée de Symantec Corporation ou de ses filiales aux États-Unis et dans d'autres pays.

SAMSUNG est une marque de commerce de SAMSUNG aux États-Unis et dans d'autres pays.