kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

Contenu

Aide de Kaspersky Endpoint Security for Windows
- Nouveautés
- Problèmes résolus
- Foire aux questions

Kaspersky Endpoint Security for Windows
- Modes de l'application : Standard, EDR Agent, Light Agent
- 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
  - Installation standard de l'application
  - Création du fichier d'installation
  - Mise à jour des bases dans le fichier d'installation
  - Création de la tâche d'installation à distance
- Installation locale de l'application à l'aide de l'Assistant
- Installation à distance de l'application à l'aide de System Center Configuration Manager
- Description des paramètres d'installation dans le fichier setup.ini
- Processus de Kaspersky Endpoint Security for Windows
- Modification de la sélection des modules de l'application
- Mise à jour à partir de la version précédente de l'application
  - Mise à jour de l'application sans redémarrage
  - Mise à jour SMU de l'application
- Suppression de l'application

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
- Comparaison des fonctionnalités des applications en fonction du type de licence pour les postes de travail
- Comparaison des fonctionnalités des applications en fonction du type de licence pour les serveurs
- Activation de l'application
- Suppression d'une clé de licence
- Consultation des informations relatives à la licence
- Achat d'une licence
- Renouvellement de l'abonnement

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
Préparation de l'application pour utilisation
Administration des stratégies
Création d'une stratégie
Exportation et importation d'une stratégie
Indicateur du niveau de protection
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
Création et utilisation d'un fichier de configuration
Restauration des paramètres par défaut de l'application
Performances de Kaspersky Endpoint Security et compatibilité avec d'autres applications
Activation et désactivation du mode d'économie d'énergie
Activation et désactivation du mode de transfert des ressources vers d'autres applications
Pratiques exemplaires pour optimiser les performances de Kaspersky Endpoint Security
Analyse des logiciels malveillants
Analyse de l'ordinateur
Analyse des disques amovibles lors de leur connexion à l'ordinateur
Analyse en arrière-plan
Analyse depuis le menu contextuel
Vérification de l'intégrité de l'application
Modification de la zone d'analyse
Exécution d'une analyse programmée
Exécution d'une analyse en tant qu'utilisateur différent
Optimisation de l'analyse
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
Mise à jour des modules d'application
Utilisation du serveur proxy lors de la mise à jour
Restauration de la dernière mise à jour

Technologie de désinfection avancée
Désinfection des menaces actives sur les postes de travail
Désinfection des menaces actives sur les serveurs
Élimination des menaces non traitées
Protection de l'ordinateur
État de la Protection en temps réel
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
Analyser les conteneurs.
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
Protection BadUSB
Activation et désactivation de la Protection BadUSB
Utilisation d'un clavier virtuel pour l'autorisation des appareils USB
Autorisation d'utilisation du lecteur de code-barres
Protection AMSI
Activation et désactivation de la protection AMSI
Optimisation de l'analyse des fichiers par la Protection AMSI
Protection contre les menaces Internet
Activation et désactivation de la Protection contre les menaces Internet
Configuration des méthodes de détection des adresses Internet malveillantes
Anti-phishing
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 aux emails
Exportation et importation d'extensions pour le filtrage des pièces jointes
Analyse du courrier dans Microsoft Office Outlook
Analyse des emails dans Thunderbird, MyOffice et R7-Office
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 menaces réseau par type
Pare-feu
Activation et désactivation du Pare-feu
Modification du type de 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
Définition de règles pour les paquets réseau au format XML
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 contre les Exploits
Activation et désactivation de la Protection contre les Exploits
Protection de la mémoire des processus système
Détection comportementale
Protection contre le chiffrement
Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe
Configuration de la période de blocage d'un ordinateur non fiable
Modification de la zone de protection
Ajout d'ordinateurs de confiance pour le chiffrement externe des données
Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe
Réparation des actions malicieuses
Kaspersky Security Network
Activation et désactivation de l'utilisation de Kaspersky Security Network
Limitations de Kaspersky Private Security Network
Activation et désactivation du mode Cloud pour les modules de la protection
Paramètres du proxy KSN
Vérification de la réputation d'un fichier dans Kaspersky Security Network
Analyse des connexions chiffrées
Activation de l'analyse des connexions chiffrées
Installation de certificats racine de confiance

Analyse des connexions chiffrées utilisant un certificat douteux
Ajout d'un certificat de Kaspersky dans la propre liste de certificats
Exclusion des connexions chiffrées de l'analyse
Blocage de l'accès aux domaines dotés de certificats non fiables
Suppression des données
Contrôle de l'ordinateur
Contrôle Internet
Ajout d'une règle d'accès aux ressources Internet
Filtrage selon les adresses des ressources Internet
Filtrage selon le contenu des ressources Internet
Vérification du fonctionnement des règles d'accès aux sites Internet
Exportation et importation de règles du Contrôle Internet
Exportation et importation des adresses des ressources Internet de la règle du Contrôle 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
Contrôle Internet pour les machines virtuelles
Variables dans les modèles de message du Contrôle Internet
Contrôle des appareils
À propos des règles d'accès
Obtention d'informations sur les appareils installés
Gestion de l'accès aux appareils par type
Gestion de l'accès aux appareils par bus de connexion
Distinction des droits d'accès des utilisateurs aux appareils
Gestion de l'accès aux appareils mobiles
Gestion de l'accès aux appareils Bluetooth
Contrôle de l'impression
Contrôle des connexions Wi-Fi
Surveillance de l'utilisation des disques amovibles
Modification de la durée de mise en cache
Actions avec les appareils de confiance
Ajout d'un appareil à la liste des appareils de confiance
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
Apprentissage 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
Surveillance des opérations du Contrôle évolutif des anomalies
Contrôle des applications
Restrictions sur le fonctionnement du Contrôle des applications
Obtention d'informations sur les applications installées
Comment activer le mode Applications bloquées
Contrôle des applications à partir d'un ordinateur de référence
Administration des règles du Contrôle des applications
Ajout d'une condition de déclenchement de la règle de Contrôle des 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 d'une règle du Contrôle des applications
Modification de l'état de la règle de Contrôle des applications via Kaspersky Security Center
Exportation et importation de règles du Contrôle des applications
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
Activation et désactivation des tests de règles du Contrôle des applications
Consultation du rapport sur les applications interdites en mode d'essai
Consultation des événements à l'issue du fonctionnement d'essai du module 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
Variables dans les modèles de message du Contrôle des applications
Bonnes pratiques relatives à l'inventaire des fichiers exécutables
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
Inspection des journaux
Configuration des règles prédéfinies
Ajout des règles personnalisées
Contrôle de l'intégrité du système
À propos des règles du Contrôle de l'intégrité du système
Contrôle de l'intégrité du système en temps réel
Vérification de l'intégrité du système sur demande
Exportation et importation des règles du Contrôle de l'intégrité du système
Affichage des rapports du Contrôle de l'intégrité du système
Réinitialisation de l'état de l'intégrité du système
Cloud Discovery

Exclusions de l'analyse pour l'application
Définition de l'exclusion de l'analyse
Création d'une exclusion par type d'objets détectés
Composition de la liste des applications de confiance
Création d'une zone de confiance locale
Exportation et importation de la zone de confiance
Gestion des applications dotées d'une signature numérique de confiance
Application. Exclusions d'analyse prédéfinies et applications de confiance
Microsoft SQL Server
Serveur Microsoft Exchange
Microsoft System Center Configuration Manager
Citrix
VMware
Déduplication des données dans Microsoft Windows Server
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
Échange de messages entre utilisateur et administrateur
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
Protection des services d'application contre l'administration externe
Assurance de fonctionnement des applications de l'administration à distance
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
Révocation du mot de passe temporaire
Particularités des autorisations de la Protection par mot de passe
Réinitialisation du mot de passe KLAdmin
Protection de la connexion au Serveur d'administration
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
Lancement de 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 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
Connexion avec le compte de service de l'Agent d'authentification
Mise à jour du système d'exploitation
Élimination des erreurs lors de la mise à jour de la fonctionnalité de chiffrement
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
Interruption de la protection BitLocker pour mettre à jour un logiciel
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

Solutions Detection and Response
Licences MDR et EDR Optimum
Compatibilité avec des solutions EDR tierces
Kaspersky Endpoint Agent
Migration de la configuration [KES+KEA] vers la configuration [KES+agent intégré]
Migration des stratégies et des tâches pour Kaspersky Endpoint Agent
Endpoint Detection and Response Agent (EDR Agent)
Installation d'EDR Agent
Intégration d'EDR Agent avec MDR
Intégration d'EDR Agent avec EDR (KATA)
Intégration d'EDR Agent avec NDR (KATA)
Intégration d'EDR Agent avec EDR Expert (on-premises)
Compatibilité avec les applications PPE tierces
Managed Detection and Response
Intégration de l'agent intégré avec MDR
Guide de migration KEA vers KES pour MDR
Endpoint Detection and Response
Intégration de l'agent intégré avec EDR Optimum / EDR Expert
Recherche d'indicateurs de compromission (tâche standard)
Télémétrie étendue pour l'analyse IOC
Placer le fichier en quarantaine
Obtenir le fichier
Supprimer le fichier
Démarrage du processus
Terminer le processus
Prévention de l'exécution
Isolation du réseau pour l'ordinateur
Cloud Sandbox
Guide de migration KEA vers KES pour EDR Optimum
Kaspersky Sandbox
Intégration de l'agent intégré avec Kaspersky Sandbox
Recherche d'indicateurs de compromission (tâche autonome)
Guide de migration KEA vers KES pour Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform
Intégration de l'agent intégré avec EDR / NDR (KATA)
Configuration de la télémétrie EDR (KATA)
Exclusions de télémétrie EDR (KATA)
Exemple 1. Processus exclus
Exemple 2. Communications des réseaux exclus
Exemple 3. Opérations sur les fichiers exclus
Exemple 4. Modifications du registre exclues
KATA Sandbox
Intégration de l'agent intégré avec KATA Sandbox
Configuration des actions de réponse aux menaces
Guide de migration KEA vers KES pour EDR (KATA)

Endpoint Detection and Response Expert (on-premises)
Intégration de l'agent intégré avec EDR Expert (on-premises)
Configuration des paramètres de la télémétrie EDR Expert (on-premises)
Exclusions de la télémétrie EDR Expert (on-premises)
Exportation et importation de filtres d'événements EDR Expert (on-premises)
Points à prendre en compte lors de l'utilisation de profils de stratégie pour configurer l'intégration avec EDR Expert (on-premises) et EDR (KATA)
Endpoint Detection and Response Expert (cloud)
Intégration de l'agent intégré avec EDR Expert (cloud)
Configuration des paramètres de la télémétrie EDR Expert (cloud)
Exclusions de la télémétrie EDR Expert (cloud)
Comment exporter ou importer les filtres d'événements EDR Expert (cloud)
Gestion de la quarantaine
Configuration de la taille maximale de la quarantaine
Envoi de données concernant les fichiers en quarantaine à Kaspersky Security Center
Restauration des fichiers depuis la quarantaine
Surveillance des actions EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Intégration de Kaspersky Endpoint Security à KUMA
Préparation de l'intégration de KES à KUMA
Connexion de KES à KUMA
Filtrage des événements à envoyer à KUMA
Exportation et importation de filtres d'événements KUMA
Guide de migration de KSWS vers KES
Correspondance des modules de KSWS et de KES
Correspondance des paramètres de KSWS et de KES
Migration des modules de KSWS
Migration des tâches et des stratégies de KSWS
Migration de la zone de confiance de KSWS
Migration des règles du Contrôle du lancement des applications de KSWS
Installation de KES à la place de KSWS
Migration de la configuration [KSWS+KEA] vers la configuration [KES+agent intégré]
Vérification que Kaspersky Security for Windows Server a bien été supprimé
Activation de KES avec une clé KSWS
Particularités relatives à la migration de serveurs à forte charge
Administration de l'application sur un serveur en mode Server Core
Migration de [KSWS+KEA] vers [KES+agent intégré]
Mode Light Agent pour protéger les machines virtuelles
Considérations particulières pour le mode Light Agent
Préconfiguration de la machine virtuelle
Compatibilité avec la technologie Citrix App Layering
Compatibilité avec la technologie Citrix Provisioning (Citrix Provisioning Services)
Compatibilité avec la technologie Omnissa App Volumes
Installation de Light Agent
À propos de la connexion Light Agent à la SVM
Recherche de SVM
Configuration de l'algorithme de sélection de la SVM pour le Light Agent

Répartition des connexions des Light Agents aux SVM (tags)
Protection de la connexion entre Light Agent et une SVM
Activation du Light Agent
Guide de migration de KSVLA Light Agent vers KES Light Agent
Installation de KES Light Agent à la place de KSVLA Light Agent
Correspondance des modules KSVLA Light Agent et KES Light Agent
Migration des tâches et des stratégies de KSVLA Light Agent
Migration de la configuration [KSVLA Light Agent+KEA] vers la configuration [KES Light Agent+agent intégré]
Administration de l'application via la ligne de commande
Setup. Installation de l'application
Setup /x. Suppression de l'application
msiexec /i. Restauration de l'application
Commandes AVP
SCAN. Analyse des logiciels malveillants
UPDATE. Mise à jour des bases de données et des modules de l'application
ROLLBACK. Restauration de la dernière mise à jour
TRACES. Traçage
START. Création d'un profil
STOP. Désactivation du profil
STATUS. État du profil
STATISTICS. Statistiques de l'exécution du profil
RESTORE. Restauration des fichiers depuis la sauvegarde
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. Réinitialisation des 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
KSN. Basculement entre KSN / KPSN
SERVERBINDINGDISABLE. Désactivation de la protection de la connexion au serveur
Commandes KESCLI
Scan. Analyse des logiciels malveillants
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. Définition de la date et de l'heure de la dernière mise à jour des bases de données
EnableRTP. Activation de la protection
GetRealTimeProtectionState. États de la Protection contre les fichiers malicieux
GetEncryptionState. État de chiffrement des disques
Version. Identification de la version de l'application

Commandes d'administration de Detection and Response
SANDBOX. Gestion de Sandbox
PREVENTION. Gestion de la prévention de l'exécution
ISOLATION. Administration de l'isolation du réseau
RESTORE. Restauration des fichiers depuis la quarantaine
IOCSCAN. Rechercher d'indicateurs de compromission (IOC)
MDRLICENSE. Activation MDR
EDRKATA. Intégration d'EDR (KATA)
EDRExpertOnPrem. Intégration d'EDR Expert (on-premises)
KUMA. Intégration de KUMA
YARA. Exécution de l'analyse YARA
TELEMETRYFILTERS. Filtrage des événements à envoyer à KUMA
Commandes d'administration du Light Agent
KSVLAINFO. Définition du mode Light Agent
VIISINFO. État de la connexion du Light Agent au Serveur d'intégration
SVMINFO. État de la connexion du Light Agent au Serveur de protection
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 des opérations de l'application
Trace des performances de l'application
Enregistrement des fichiers dump
Protection des fichiers dump et de traçage
Obtention des données relatives au système d'exploitation (Kaspersky Get System Info)
Restrictions et avertissements
Glossaire
Agent d'administration
Agent d'authentification
Archive
Authentification Kerberos
Base des URL de phishing
Base des URL malveillantes
Bases antivirus
Certificat de licence
Clé active
Cloud Discovery
Émetteur de certificat
Faux positif
Fichier infectable
Fichier infecté
Fichier IOC
Forme normalisée de l'adresse du site Internet

Gestionnaire de fichiers portable
Groupe d'administration
IOC
Light Agent
Masque
Objet OLE
OpenIOC
Réparation d'objets
Serveur d'intégration.
SVM
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
Pare-feu
Protection BadUSB
Protection AMSI
Protection contre les Exploits
Détection comportementale
Prévention des intrusions
Réparation des actions malicieuses
Kaspersky Security Network
Inspection des journaux
Protection contre le chiffrement
Contrôle Internet
Contrôle des appareils
Contrôle des applications
Contrôle évolutif des anomalies
Contrôle de l'intégrité du système
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Intégration de KUMA
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
Administration des paramètres
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 du réseau pour l'interaction avec les services externes
Annexe 6. Événements relatifs aux applications
Critique
Erreur de fonctionnement
Avertissement
Messages d'information
Annexe 7. Extensions de fichier prises en charge pour Prévention de l'exécution
Annexe 8. Interpréteurs de script pris en charge pour la prévention de l'exécution
Annexe 9. Zone de l'analyse IOC dans le registre (RegistryItem)
Annexe 10. Exigences relatives aux fichiers IOC
Annexe 11. API pour la réponse aux menaces EDR
Annexe 12. Comptes utilisateurs dans les règles des modules d'application
Informations légales
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
Collecte des données lors de l'utilisation de solutions Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Intégration à Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Respect de la législation de l'Union européenne (RGPD)
Notice sur les marques de commerce
Informations sur le code tiers

Aide de Kaspersky Endpoint Security for Windows

Nouveautés de la version 14.2

Ajout de la prise en charge de l'authentification par jeton pour la Protection par mot de passe

Nouveautés de chaque version de Kaspersky Endpoint Security for Windows

Guide de démarrage

Déploiement de Kaspersky Endpoint Security for Windows

Configuration initiale de Kaspersky Endpoint Security for Windows

Licences de Kaspersky Endpoint Security for Windows

À propos des données

En vertu du Contrat de licence utilisateur final

Lorsque vous utilisez KSN

RGPD

Élimination des menaces

Sur les postes de travail

Sur les serveurs

Réagir à la détection d'un indicateur de compromission (Isolation du réseau → Quarantaine → Prévention de l'exécution)

Bonnes pratiques

Optimisation des performances des applications

Implémentation du mode de refus par défaut dans le Contrôle des applications

Migration de KEA vers KES avec agent intégré

Utilisation de KES dans le cadre d'autres solutions

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Nouveautés

Mise à jour 14.2

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 14.2 for Windows :

1. L'ensemble des modules installés par défaut a été modifié. La configuration par défaut de l'application inclut désormais la Protection BadUSB, l'administration de BitLocker et l'agent EDR Optimum intégré.

2. Ajout de la prise en charge de l'authentification par jeton (Protection par mot de passe). Désormais, pour accéder à l'application, vous pouvez utiliser soit votre nom d'utilisateur et votre mot de passe, soit un mot de passe temporaire fourni par l'administrateur, soit un jeton. L'authentification par jeton peut être utilisée, par exemple, pour les comptes utilisateur de service qui ne nécessitent pas de mot de passe.

3. Ajout d'un nouveau critère de robustesse du mot de passe pour BitLocker : la vérification de l'historique des mots de passe. L'application empêche les utilisateurs de définir un mot de passe qu'ils ont déjà utilisé.

4. Ajout de la possibilité de modifier la langue de l'interface de Kaspersky Endpoint Security lors de la mise à jour de l'application à l'aide de la tâche *Installer l'application à distance*. Désormais, vous n'avez plus besoin de réinstaller l'application si vous avez choisi une langue d'interface incorrecte.

5. Ajout de nouveaux événements de télémétrie pour les utilisateurs des solutions Kaspersky Endpoint Detection and Response : GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Ces nouveaux événements améliorent les capacités de détection des menaces des solutions EDR.

6. Ajout de la prise en charge d'une nouvelle action de réponse aux menaces, *Placer le fichier*, pour les utilisateurs de Kaspersky Endpoint Detection and Response Expert (on-premises). Cette tâche permet de transférer vers les ordinateurs des fichiers de configuration, des scripts de réponse aux menaces, des utilitaires visant à atténuer les conséquences des attaques, etc. La tâche *Placer le fichier* est disponible dans la console OSMP lorsque la solution Kaspersky EDR Expert (on-premises) version 9.0 est déployée.

7. Amélioration du comportement des actions de réponse aux menaces pour les utilisateurs de Kaspersky Endpoint Detection and Response Optimum. Désormais, avant d'exécuter l'action (*Supprimer le fichier*, *Déplacer le fichier vers la quarantaine* ou *Prévention de l'exécution*), l'application vérifie si l'objet est critique pour le système (System Critical Object, SCO) et vous avertit de l'impact potentiel sur la stabilité du système. Il est déconseillé d'appliquer ces actions aux fichiers d'objets critiques pour le système (SCO).

8. Ajout de la possibilité pour les utilisateurs de Kaspersky Security for Virtualization Light Agent d'utiliser l'application au sein d'un cluster de Serveurs d'intégration à haute disponibilité. Un cluster haute disponibilité de Serveurs d'intégration assure une protection ininterrompue de l'environnement virtuel grâce au basculement des SVM et des Light Agents vers un Serveur d'intégration de sauvegarde en cas de défaillance du Serveur d'intégration principal.

9. Lors du développement de cette version de Kaspersky Endpoint Security, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Mise à jour 14.1

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 14.1 for Windows :

1. La prise en charge du système d'exploitation Windows Server 2025 a été ajoutée.

2. La limite du nombre de règles de filtrage des événements de télémétrie pour Endpoint Detection and Response Expert (on-premises) et Kaspersky Endpoint Detection and Response Expert (cloud) a été augmentée. Kaspersky Endpoint Security prend désormais en charge jusqu'à 10 000 règles de filtrage incluses et exclusives au total.

3. Vous pouvez désormais configurer les tâches pour qu'elles s'exécutent uniquement certains jours de la semaine, à un intervalle donné en semaines. La planification est disponible à partir de la version 16.1 de Kaspersky Security Center.

4. Pour la tâche *Analyse des logiciels malveillants*, vous pouvez désormais définir un intervalle de temps pendant lequel la tâche sera mise en pause, par exemple afin de minimiser l'impact sur les performances de l'ordinateur pendant les périodes de charge élevée.

5. Les performances du sous-système de disque dur sur l'ordinateur protégé ont été optimisées en réduisant le nombre d'opérations d'E/S.

6. Lors du développement de cette version de Kaspersky Endpoint Security, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Mise à jour 14.0

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 14.0 for Windows :

1. Les ordinateurs équipés d'un processeur ARM sont désormais pris en charge. Vous pouvez installer l'application soit en mode standard, soit en mode EDR Agent. Cependant, l'application présente plusieurs limitations (par exemple, parmi les technologies de chiffrement des données, seul BitLocker est pris en charge).

2. L'audit étendu des stratégies est pris en charge dans Kaspersky Security Center Web Console version 15.0 ou toute version ultérieure. Vous pouvez désormais consulter les modifications apportées aux stratégies et les enregistrer dans un fichier. Une *révision* est un ensemble de paramètres modifiés enregistrés par l'utilisateur. Les révisions vous permettent de comparer et d'annuler les modifications apportées aux paramètres de la stratégie.

3. De nouveaux événements de télémétrie sont désormais disponibles pour les utilisateurs de Kaspersky Endpoint Detection and Response. Ces nouveaux événements améliorent les capacités de détection des menaces à l'aide des solutions EDR de Kaspersky.

4. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Mise à jour 12.12

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.12 for Windows :

1. La protection des dossiers partagés contre le chiffrement externe, qui faisait auparavant partie du module Détection comportementale, est désormais un module distinct, appelé Protection contre le chiffrement.

2. Ajout de la prise en charge du protocole Kerberos pour l'authentification de l'application via un serveur proxy pour l'accès à Internet.

3. Vous pouvez maintenant indiquer un hachage de fichier pour une application de confiance et pas seulement un chemin d'accès complet.

4. Davantage de fonctionnalités de la tâche *Analyse IOC* sont disponibles pour les utilisateurs des solutions Endpoint Detection and Response (EDR). La fonctionnalité Analyse IOC rétrospective est désormais disponible. *Analyse IOC rétrospective* est un mode de la tâche *Analyse IOC* dans laquelle Kaspersky Endpoint Security recherche des indicateurs de compromission à l'aide des données pendant une certaine période. Ce mode est destiné à détecter les indicateurs de compromission dans les données relatives à l'activité réseau de l'ordinateur. Kaspersky Endpoint Security analyse les données contenues dans les journaux du système d'exploitation et les journaux du navigateur sur l'ordinateur.

5. Les utilisateurs de Kaspersky Endpoint Detection and Response (EDR) peuvent supprimer la limite de taille de la quarantaine. Cette option peut être nécessaire pour l'analyse YARA, car l'application peut enregistrer un fichier de vidage mémoire volumineux. Vous pouvez désormais réserver tout votre espace disque disponible pour la quarantaine.

6. La compression HTTPS est désormais prise en charge pour optimiser l'exportation des événements vers la plateforme Kaspersky Unified Monitoring and Analysis Platform (KUMA). Cette mesure permet de réduire le trafic sortant.

7. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Mise à jour 12.11

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.11 for Windows :

1. L'application vérifie la configuration des modules de contrôle avant d'enregistrer les paramètres. La vérification a été ajoutée pour les modules Contrôle des applications, Contrôle des appareils et Contrôle de l'intégrité du système. L'application affiche désormais un avertissement si les paramètres actuels du module de contrôle sont susceptibles d'augmenter la charge sur l'ordinateur ou de provoquer des défaillances du système. Par exemple, dans le cas du Contrôle des applications, si vous avez sélectionné le mode qui bloque toutes les applications sauf celles autorisées et que vous n'avez ajouté aucune règle d'autorisation, l'application affiche un avertissement, car une telle configuration peut entraîner des défaillances du système.

2. Ajout de la prise en charge de l'envoi automatique de fichiers à KATA Sandbox pour examen. *KATA Sandbox* est un module de Kaspersky Anti Targeted Attack Platform qui exécute les fichiers sur les images virtuelles des systèmes d'exploitation. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour que KATA Sandbox fonctionne en mode automatique, Kaspersky Anti Targeted Attack Platform 8.0 ou une version ultérieure doit être déployée.

3. Optimisation de l'envoi de données télémétriques EDR. Vous pouvez maintenant spécifier la longueur maximale des paquets.

4. Amélioration du diagnostic de connexion à Kaspersky Security Network. Amélioration des détails de l'erreur de connexion de Kaspersky Security Network afin de résoudre les problèmes potentiels.

5. Ajout de la prise en charge de la configuration des listes d'événements à envoyer à Kaspersky Unified Monitoring and Analysis Platform (KUMA). Désormais, en plus des listes d'événements prédéfinies dans KUMA, vous pouvez ajouter manuellement des événements à la télémétrie ou exclure des événements par leur ID dans le journal des événements Windows.

6. Mise à jour de l'interface des stratégies dans Web Console. La disposition des sections consacrées aux stratégies a été modifiée afin de permettre un accès plus rapide aux fonctionnalités essentielles.

7. Prise en charge de Windows 11 25H2.

8. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Mise à jour 12.10

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.10 for Windows :

1. Pour le module Protection BadUSB, il est désormais possible d'autoriser les lecteurs de code-barres en lisant un code-barres à l'écran. Désormais, il n'est plus nécessaire de saisir un code à l'aide du clavier à l'écran pour autoriser les lecteurs de code-barres.

2. Les fonctionnalités et améliorations suivantes sont disponibles pour les utilisateurs des solutions Endpoint Detection and Response (EDR) de Kaspersky :

   - Vous pouvez désormais gérer l'isolement du réseau de l'ordinateur dans les détails de l'alerte. De plus, vous pouvez indiquer dans les détails de l'alerte la période d'isolement du réseau de l'ordinateur et ajouter des exclusions.

   - Ajout de nouvelles données aux détails de l'alerte. Désormais, les détails de l'alerte contiennent plus d'informations à propos de la menace, notamment comment l'application réagit aux menaces EDR.

   - Le traitement des fichiers IOC a été amélioré. Désormais, vous pouvez visualiser et modifier le contenu des fichiers IOC dans l'interface de Kaspersky Security Center Web Console. Une fois que vous aurez chargé un fichier IOC, l'application affichera un rapport sur l'application des conditions IOC.

   - Amélioration de la réponse aux IOC détectés. Vous pouvez désormais mettre en quarantaine les fichiers détectés par la tâche *Analyse IOC* directement dans les résultats de la détection IOC dans les propriétés de la tâche. Vous pouvez également isoler les ordinateurs du réseau dans les propriétés de la tâche.

   - Vous pouvez désormais créer des fichiers IOC directement dans les propriétés de la tâche *Analyse IOC* à partir de listes de hachages de fichiers, d'adresses IP ou de noms DNS générés dans un fichier TXT.

   - Zone d'analyse étendue pour la tâche *Analyse IOC*. Vous pouvez maintenant définir une zone pour l'analyse IOC du registre (**Registre Windows – RegistryItem**). Dans les versions antérieures de l'application, vous ne pouviez utiliser qu'une zone d'analyse IOC prédéfinie dans le registre.

3. Nouvelle autorisation de protection par mot de passe ajoutée, *Paramètres d'exportation*. Par défaut, seul l'utilisateur KLAdmin peut créer un fichier de configuration avec les paramètres de Kaspersky Endpoint Security dans l'interface de l'application. Pour accorder l'accès à d'autres utilisateurs, vous devez leur donner l'autorisation correspondante.

4. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Mise à jour 12.9

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.9 for Windows :

1. La nouvelle fonctionnalité de *gestion des mots de passe temporaires* a été ajoutée. Le mot de passe temporaire vous permet d'octroyer l'accès à Kaspersky Endpoint Security avec la protection par mot de passe activée pour un ordinateur distinct. La gestion des mots de passe temporaires permet d'enregistrer l'historique des mots de passe (jusqu'à 30 jours), de surveiller l'état du mot de passe temporaire (*Active*, *Expirée*, *Révoquée*) et révoquer les mots de passe temporaires.

2. Ajout de la possibilité de mettre fin à la connexion aux ressources Internet interdites par les règles du Contrôle Internet immédiatement après l'application de la stratégie. Dans les versions précédentes de l'application, le Contrôle Internet limitait uniquement les nouvelles connexions aux ressources Internet interdites.

3. Pour les utilisateurs de Kaspersky Anti Targeted Attack Platform, la possibilité d'exécuter une vérification YARA localement sur l'ordinateur a été ajoutée. Pour ce faire, vous devez télécharger le fichier avec les règles YARA et exécuter la commande dans CMD.

4. Correction du comportement de l'application lorsque BitLocker était activé sur les ordinateurs dont les disques sont déjà protégés par BitLocker à l'aide d'outils tiers. Kaspersky Endpoint Security lance la procédure de récupération pour envoyer la clé de récupération à Kaspersky Security Center. Ainsi, l'administration de BitLocker est reportée sur la console de Kaspersky Security Center.

5. Une nouvelle section, **Historique des réponses**, est accessible aux utilisateurs des solutions Detection and Response de Kaspersky. Cette section contient des informations sur les actions de réponse aux menaces exécutées sur l'ordinateur. Ces actions incluent, par exemple, l'exécution de la tâche *Fin du processus* ou l'isolement de l'ordinateur du réseau. L'historique des réponses est disponible uniquement pour les utilisateurs des solutions de Kaspersky suivantes : MDR, EDR, KATA.

6. Pour les utilisateurs de Kaspersky Unified Monitoring and Analysis Platform, la prise en charge des actions EDR de réponse aux menaces est désormais disponible. Lorsqu'il répond aux menaces, KUMA exécute des scripts qui créent les tâches EDR correspondantes. Pour exécuter des tâches EDR, vous devez créer une règle de réponse pour le script personnalisé dans la console KUMA et sélectionner des événements.

7. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020 et PF20021.

Mise à jour 12.8

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.8 for Windows :

1. L'application prend désormais en charge le Mode Light Agent pour la protection des environnements virtuels. Vous pouvez maintenant déployer l'application en tant que Light Agent dans le cadre de la solution Kaspersky Security for Virtualization Light Agent 6.2.

2. L'interception des opérations sur les fichiers dans les conteneurs Docker sur les serveurs est désormais prise en charge. Un *conteneur* est un environnement isolé dans lequel une application peut s'exécuter sans interagir directement avec le système d'exploitation. Kaspersky Endpoint Security analyse les fichiers dans les conteneurs auxquels l'utilisateur a accès. Lorsqu'une menace est détectée, l'application la bloque et tente de désinfecter le fichier à l'intérieur du conteneur. Si le fichier ne peut pas être désinfecté, l'application arrête le conteneur.

3. Vous pouvez désormais définir une zone de protection pour la protection des dossiers partagés contre le chiffrement externe (module Détection comportementale). Vous pouvez maintenant spécifier les dossiers partagés dont l'application doit surveiller l'activité liée aux fichiers. Vous pouvez également exclure des fichiers de la zone de protection. Dans les versions précédentes de l'application, le module Détection comportementale surveillait tous les dossiers partagés pour détecter l'activité des fichiers.

4. Vous pouvez désormais configurer différents ensembles de modules pour différents types de systèmes d'exploitation dans le paquet d'installation. Autrement dit, vous pouvez déployer l'application sur les postes de travail et les serveurs à l'aide du même paquet d'installation. Les modules non disponibles pour un certain type de système d'exploitation sont automatiquement exclus des propriétés du paquet d'installation.

5. L'option permettant de sélectionner les exclusions d'analyse et les applications de confiance prédéfinies a été ajoutée. Les exclusions d'analyse et les applications de confiance prédéfinies permettent de configurer rapidement la zone de confiance de l'application dans un environnement virtuel (Citrix, Vmware). Ces exclusions comprennent, par exemple, les fichiers de machine virtuelle VHD et VHDX. Les exclusions peuvent être ajoutées lors de la création d'un paquet d'installation d'application, de la création d'une stratégie ou de l'installation de Kaspersky Endpoint Security.

6. Les données télémétriques EDR incluent désormais les événements pour les opérations avec les appareils connectés par USB. Vous pouvez également ajouter ces événements aux exclusions des données télémétriques EDR.

7. Ajout de la possibilité de bloquer les connexions réseau via le protocole obsolète TLS 1.0. Le protocole TLS 1.0 a un niveau de sécurité faible, il est donc recommandé de désactiver ce protocole et d'utiliser les versions plus récentes TLS 1.2 ou TLS 1.3. Par défaut, Kaspersky Endpoint Security bloque les connexions TLS 1.0. Après la mise à jour de la version de l'application, le fonctionnement des services tiers qui utilisent le protocole TLS 1.0 peut échouer. Pour éviter tout problème lors du fonctionnement des services tiers, vous pouvez autoriser l'utilisation du protocole TLS 1.0 dans la stratégie de groupe avant la mise à jour de la version de l'application.

8. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016 et PF19018.

Mise à jour 12.7

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.7 for Windows :

1. Vous pouvez désormais limiter l'utilisation des ressources du processeur pour la tâche *Analyse des logiciels malveillants*. Pour ce faire, dans les paramètres de l'application, précisez le pourcentage de charge maximale du processeur pour tous les cœurs qui peuvent être utilisés lors de l'analyse de l'ordinateur.

2. Désormais, vous pouvez manuellement envoyer des fichiers à analyser dans KATA Sandbox. *KATA Sandbox* est un module de Kaspersky Anti Targeted Attack Platform qui exécute les fichiers sur les images virtuelles des systèmes d'exploitation. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour envoyer un fichier pour analyse à KATA Sandbox, sélectionnez la commande correspondante dans le menu contextuel du fichier.

3. Vous pouvez maintenant configurer l'intégration à la solution qui protège le réseau local de l'entreprise, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) fait partie de Kaspersky Anti Targeted Attack Platform. Vous pouvez configurer l'interaction avec NDR en mode standard ainsi qu'en mode EDR Agent.

4. La prise en charge du client de messagerie Microsoft Office Outlook version 2021 a été ajoutée à l'extension Protection contre les menaces par emails. L'extension permet d'analyser les messages au niveau d'un client de messagerie plutôt qu'au niveau du protocole. En plus des messages, l'extension vous permet d'analyser les objets reçus via l'interface MAPI à partir des stockages Microsoft Exchange (par exemple, les objets du calendrier). Cette analyse a lieu dans le client de messagerie.

5. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006 et PF18007.

Mise à jour 12.6

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.6 for Windows :

1. La fonctionnalité d'intégration avec la solution Kaspersky SIEM (*Kaspersky Unified Monitoring and Analysis Platform ; KUMA*) a été ajoutée. Il est désormais possible d'envoyer des événements depuis les journaux des événements Windows au collecteur KUMA. Cette fonction permet à KUMA de recevoir des événements Windows (un ensemble limité d'identifiants EventID est pris en charge) de tous les ordinateurs sur lesquels Kaspersky Endpoint Security est installé, sans installer d'agents KUMA sur ces ordinateurs.

2. Le nouveau module *Contrôle de l'intégrité du système* a été ajouté pour remplacer le module Contrôle de l'intégrité des fichiers. Le module Contrôle de l'intégrité du système inclut toutes les fonctionnalités du Contrôle de l'intégrité des fichiers et permet également de surveiller les modifications apportées au registre et la connexion d'appareils externes. Le module Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Endpoint Security génère les événements correspondants et en informe l'administrateur. Le Contrôle de l'intégrité des fichiers ne fait plus partie de l'application. Les paramètres du Contrôle de l'intégrité des fichiers migrent automatiquement vers le Contrôle de l'intégrité du système lorsque vous mettez à jour l'application. Pour garantir le bon fonctionnement du Contrôle de l'intégrité du système, l'application et le plug-in d'administration Kaspersky Endpoint Security doivent être mis à jour vers la version 12.6.

3. L'état d'EDR Agent (KATA) intégré installé est ajouté dans les propriétés de l'ordinateur dans la console de Kaspersky Security Center. Maintenant, si vous avez installé un EDR Agent (KATA) intégré, la colonne **État de Endpoint Sensor** affiche l'état actuel du module (p. ex., *En cours*, *Arrêté*, *Non pris en charge par la licence*, etc.).

4. L'option permettant de sélectionner les exclusions d'analyse et les applications de confiance prédéfinies a été ajoutée. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement la zone de confiance lors de l'utilisation de l'application sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Ces exclusions comprennent, par exemple, les fichiers de base de données MDF et LDF. Les exclusions peuvent être ajoutées lors de la création d'une nouvelle stratégie, de la modification d'une stratégie existante ou de l'installation de Kaspersky Endpoint Security.

5. L'affichage des détails des alertes pour Kaspersky Endpoint Detection and Response Optimum a été déplacé du plug-in d'administration de Kaspersky Endpoint Security vers un plug-in d'administration distinct de Kaspersky Endpoint Detection and Response. Le plug-in d'administration EDR est un plug-in unique conçu pour fonctionner avec des agents sous les systèmes d'exploitation Windows, Mac et Linux. Désormais, lorsque vous utiliserez EDR Optimum, vous aurez besoin du plug-in d'administration de Kaspersky Endpoint Security pour créer des tâches de réponse aux menaces et du plug-in d'administration EDR pour consulter les détails des alertes.

6. Prise en charge de Windows 11 24H2.

7. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029 et pf17002.

Mise à jour 12.5

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.5 for Windows :

1. La possibilité de configurer des exclusions de télémétrie a été ajoutée. *Télémétrie* est une liste d'événements qui se sont produits sur l'ordinateur protégé. Les données de télémétrie sont utilisées par Kaspersky Anti Targeted Attack Platform (EDR) pour surveiller et protéger l'infrastructure informatique de l'entreprise. La configuration des exclusions de télémétrie permet d'améliorer les performances de l'ordinateur et d'optimiser la transmission des données vers le serveur de collecte de données télémétriques.

2. L'interface de la zone de confiance de l'application a été améliorée. Kaspersky Endpoint Security masque désormais les objets de la zone de confiance à l'utilisateur si l'administrateur a interdit à l'utilisateur d'ajouter ses propres exclusions d'analyse (locales) et applications de confiance. Cette mesure empêche tout accès non autorisé à la zone de confiance par un intrus, ce qui accroît le niveau de sécurité de l'ordinateur.

3. L'option d'analyse du trafic pour les clients de messagerie MyOffice Mail et R7-Office Organizer a été ajoutée. Le module Protection contre les menaces par emails analyse désormais non seulement les pièces jointes lors de leur téléchargement, mais également les messages envoyés et reçus.

4. Une nouvelle catégorie de ressources Internet *Outils d'IA générative* a été ajoutée. Vous pouvez configurer l'accès aux sites Internet de la nouvelle catégorie par le Contrôle Internet.

5. Maintenant, vous pouvez sélectionner l'emplacement d'une règle pour les paquets réseau dans la liste Pare-feu. L'emplacement d'une règle pour les paquets réseau dans la liste détermine sa priorité. Dans les versions précédentes de l'application, une nouvelle règle ne pouvait être ajoutée qu'à la fin de la liste, après quoi il fallait déplacer manuellement la règle dans la liste pour la classer par ordre de priorité. Désormais, lors de l'ajout d'une règle, vous pouvez choisir si la règle doit être placée au début, à la fin de la liste ou à côté de la règle sélectionnée.

6. Dans les règles des modules de Kaspersky Endpoint Security, vous pouvez désormais sélectionner des utilisateurs non seulement dans Active Directory, mais également dans la liste des utilisateurs de Kaspersky Security Center. Vous pouvez également saisir les données du compte utilisateur local manuellement. Cette possibilité a été ajoutée pour les règles des modules suivants : Contrôle des applications, Contrôle des appareils, Contrôle Internet, Contrôle évolutif des anomalies et Inspection des journaux.

7. Le rapport de détection des attaques réseau comprend désormais une colonne avec l'adresse MAC de l'ordinateur attaquant (le module Protection contre les menaces réseau). Vous pouvez désormais voir l'adresse MAC de l'ordinateur attaquant dans le rapport en plus de son adresse IP. Ces informations sont utiles dans le cadre d'une enquête sur un incident. Les rapports, qui contiennent l'adresse MAC de l'ordinateur attaquant, seront également disponibles à partir de la version 15.1 de la console de Kaspersky Security Center Linux.

8. Le niveau d'exigences en matière de protection informatique a été augmenté. Le niveau de protection élevé requiert l'activation de la Protection des services de l'application contre l'administration externe. Vérifiez l'indicateur du niveau de sécurité dans la partie supérieure de la fenêtre de la stratégie. Si vous disposez d'un niveau de sécurité moyen ou faible, vous pouvez activer l'option Administration des applications contre l'administration externe dans la fenêtre de recommandation de l'indicateur de niveau de sécurité.

9. Ajout de la prise en charge des nouveaux événements de détection d'objets lors du fonctionnement de l'application dans la configuration d'Endpoint Detection and Response Agent (EDR Agent). Ces événements étaient déjà pris en charge dans la configuration [KES+agent intégré].

10. Lors du développement de cette version de Kaspersky Endpoint Security for Windows, nous avons intégré les modifications incluses dans les correctifs privés suivants : pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028 et pf16013.

Mise à jour 12.4

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.4 for Windows :

1. Ajout d'une nouvelle fonctionnalité pour protéger la connexion de l'ordinateur à Kaspersky Security Center. La nouvelle tâche *Protection de la connexion au Serveur d'administration* permet de définir un mot de passe pour la connexion à un serveur de confiance. Cela signifie qu'il n'est pas possible de reconnecter l'ordinateur et d'exécuter des commandes à partir d'un autre serveur sans ce mot de passe.

2. Pour le module Protection par mot de passe, la possibilité de sélectionner les utilisateurs manuellement et pas seulement depuis Active Directory a été ajoutée. C'est-à-dire que vous pouvez définir manuellement un nom d'utilisateur et un mot de passe et attribuer des droits d'accès à Kaspersky Endpoint Security pour ce compte. Vous n'avez donc pas besoin de partager votre mot de passe KLAdmin avec d'autres utilisateurs ni de créer différents comptes Active Directory pour contrôler l'accès à l'application.

3. Prise en charge de Windows 11 23H2.

Mise à jour 12.3

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.3 for Windows :

1. Vous pouvez maintenant installer l'application dans la configuration Endpoint Detection and Response Agent. Cette configuration permet d'installer l'application avec un ensemble de modules requis par les solutions Detection and Response de Kaspersky : Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform (EDR). Vous pouvez installer l'application dans cette configuration aux côtés de solutions tierces (par exemple, Dr.Web, Dallas Lock ou ESET). Vous pouvez ainsi utiliser des outils de sécurité d'infrastructure tiers ainsi que la solution Detection and Response de Kaspersky.

2. Le fonctionnement de Kaspersky Endpoint Security avec les appareils Bluetooth a été amélioré. Vous pouvez désormais configurer des exclusions et restreindre l'accès à tous les appareils Bluetooth, à l'exception des appareils de saisie (claviers sans fil, souris, etc.).

3. Le fonctionnement du module Contrôle des applications avec la base de données des fichiers exécutables a été optimisé. Kaspersky Endpoint Security supprime désormais automatiquement les informations sur les fichiers de la base de données si le fichier est supprimé de l'ordinateur. Cela permet de maintenir la base de données à jour et d'économiser les ressources de Kaspersky Security Center.

4. Le niveau d'exigences en matière de protection informatique a été augmenté. Le niveau de protection élevé exige désormais l'activation de la protection par mot de passe. Vérifiez l'indicateur du niveau de sécurité dans la partie supérieure de la fenêtre de la stratégie. Si vous disposez d'un niveau de protection moyen ou faible, vous pouvez activer la Protection par mot de passe dans la fenêtre de recommandation de l'indicateur de niveau de sécurité.

5. La prise en charge du protocole HTTPS a été ajoutée pour permettre à l'application de fonctionner avec Kaspersky Security Network. Activez l'utilisation du protocole HTTPS dans les propriétés du Serveur d'administration dans les paramètres du serveur proxy KSN.

Mise à jour 12.2

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.2 for Windows :

1. La prise en charge du protocole WPA3 a été ajoutée pour contrôler les connexions aux réseaux Wi-Fi (Contrôle des appareils). Vous pouvez désormais sélectionner le protocole WPA3 dans les paramètres du réseau Wi-Fi de confiance et refuser la connexion au réseau à l'aide d'un protocole moins sécurisé.

2. Vous pouvez désormais choisir un protocole et des ports pour les exclusions de protection contre les menaces réseau. Désormais, en plus d'indiquer les adresses IP des appareils de confiance, vous pouvez également sélectionner un port et un protocole. Cela vous permet d'exclure des flux de données individuels et d'empêcher les attaques réseau à partir d'adresses IP de confiance.

3. Ordre différent des sources de mise à jour pour la *tâche locale Mise à jour des bases et des modules d'application* si une stratégie est appliquée à l'ordinateur. Le serveur Kaspersky Security Center est désormais utilisé par défaut comme première source de mise à jour au lieu des serveurs Kaspersky. Cette mesure permet d'économiser du trafic lorsque l'utilisateur exécute la tâche locale *Mise à jour des bases et des modules d'application*.

Mise à jour 12.1

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 12.1 for Windows :

1. Un agent intégré pour la solution Kaspersky Anti Targeted Attack Platform a été ajouté. Vous n'avez plus besoin de Kaspersky Endpoint Agent pour utiliser EDR (KATA). Toutes les fonctions de Kaspersky Endpoint Agent seront exécutées par Kaspersky Endpoint Security. Pour migrer les stratégies de Kaspersky Endpoint Agent, utilisez l'Assistant de migration. Après que l'application a été mise à jour, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. Kaspersky Endpoint Agent a été ajouté à la liste des logiciels incompatibles. Kaspersky Endpoint Security dispose d'agents intégrés pour toutes les solutions Detection and Response. Il n'est donc plus nécessaire d'installer Kaspersky Endpoint Agent pour l'intégrer à ces solutions.

2. Le mode de compatibilité Azure WVD est désormais pris en charge. Cette fonctionnalité garantit l'affichage correct de l'état de la machine virtuelle Azure dans la console de Kaspersky Anti Targeted Attack Platform. Le mode de compatibilité Azure WVD permet d'attribuer un identifiant de capteur unique permanent à ces machines virtuelles.

3. Maintenant, vous pouvez configurer l'accès des utilisateurs aux appareils mobiles dans iTunes ou des applications similaires. Autrement dit, vous pouvez, par exemple, autoriser l'utilisation de l'appareil mobile uniquement dans iTunes et bloquer l'utilisation de l'appareil mobile comme disque amovible. L'application prend également en charge ces règles pour l'application Android Debug Bridge (ADB).

4. La version 11 de Kaspersky Security Center n'est plus prise en charge. Mettez à jour Kaspersky Security Center vers la dernière version.

Problèmes résolus

Le tableau ci-dessous répertorie tous les problèmes découverts dans les versions précédentes de Kaspersky Endpoint Security et corrigés dans la version actuelle.

Liste des problèmes corrigés dans la version 14.2

Identifiant	Description
10110351	Le module Contrôle des appareils autorise l'accès à un appareil MTD (carte SD) lorsque l'action **Interdire** est sélectionnée pour le type d'appareil **Disques amovibles**.
10068496	Sur un appareil protégé, le mode de protection contre le MAC spoofing peut être modifié lorsque les paramètres de la Protection contre les menaces réseau sont verrouillés dans la stratégie parente.
10095087	Lorsque l'analyse des connexions chiffrées est activée, l'accès à un site via un pare-feu de nouvelle génération (NGFW) dont le certificat a été révoqué déclenche une notification indiquant une redirection vers un domaine dont le certificat n'est pas fiable.
10140912	Lorsque l'application est installée, l'ordinateur ne détecte pas l'appareil PDA BHT1100B fonctionnant sous Windows Mobile.
10141009	Si le module Chiffrement des fichiers est installé, l'application Anthropic Claude peut ne pas démarrer.
10610853	Après la mise à jour vers la nouvelle version, la stratégie ne peut pas être ouverte, car les paramètres du Contrôle des appareils de cette version incluent des appareils qui ne sont pas pris en charge dans la version précédente.

Identifiant	Description
10720516	Les pièces jointes contenues dans des fichiers aux formats Office peuvent ne pas s'ouvrir lorsque l'application est installée.
10421967	La connexion à une boîte aux lettres partagée échoue si celle-ci a été ajoutée en tant que compte distinct.

Liste des problèmes corrigés dans le plug-in Internet 14.2.0.8289

Identifiant	Description
9946286	Lors de l'ajout d'une adresse de site à une règle du Contrôle Internet, il est impossible d'utiliser un masque qui ne comporte pas de point entre le domaine et la zone de domaine.
10054657 10507166	Après la migration vers la nouvelle version, certains modules (tels que Contrôle des appareils et Contrôle des applications) ne peuvent pas être gérés à l'aide d'une stratégie.
10084390	Dans les paramètres du module Contrôle des appareils, le type d'appareil **Disque dur** apparaît en double, ce qui entraîne le blocage des disques durs des utilisateurs.
10113718	Dans certains cas, les règles personnalisées du Pare-feu ne s'affichent pas.
10311613	Dans les paramètres du module Prévention des intrusions, il est impossible d'ajouter une ressource protégée au moyen d'un masque utilisant le caractère `*`.
10391923	Dans le Contrôle des applications, lors de la création d'une catégorie d'applications basée sur le hachage MD5 d'un fichier, aucun avertissement n'indique que cette catégorie n'est pas valide et ne fonctionnera pas.
10571790	Pour le module Contrôle des applications, le titre de la liste des règles de blocage en mode **Autoriser tout ce qui ne figure pas dans la liste des règles** a été corrigé.
10592891 10689065	Dans la zone de confiance, le champ **Commentaires** ne s'affiche pas pour les exclusions de la section **Exclusions de l'analyse des logiciels malveillants**.
10613015 10689049 10592534	Dans le module Contrôle des appareils, le champ **Commentaires** ne s'affiche pas pour les appareils de confiance.
10645068 10689057	La tâche *Supprimer la clé* ne s'exécute pas si un fichier de clé de licence au format KEY est sélectionné.
10685370 10685422	Dans le module Contrôle des appareils, il est impossible d'ajouter un nouvel appareil à la liste des appareils de confiance si un appareil portant le même nom y figure déjà.
10721136	Les tâches de groupe ne peuvent pas être enregistrées si aucune date de fin n'est indiquée dans les paramètres de planification.
10753509	La modification de la liste des utilisateurs et des groupes associés aux appareils de confiance dans le module Contrôle des appareils peut modifier les types d'enregistrements, de sorte que les paramètres ne s'appliquent plus à l'appareil.
10773402	Dans certains cas, les modifications apportées aux paramètres de la stratégie peuvent ne pas être enregistrées en raison de profils corrompus.
10822620	Les paramètres du module Protection contre le chiffrement ne s'affichent pas dans la stratégie, et les modifications apportées aux paramètres de notification ne sont pas enregistrées.
10817035	Dans une stratégie enfant, il est possible d'ajouter un appareil de confiance même si ce paramètre est désactivé dans la stratégie parente (« cadenas » fermé). Cependant, l'appareil ajouté n'est pas enregistré.
10678009	Dans le plug-in Internet de Kaspersky Endpoint Security, l'ajout d'une nouvelle règle du Pare-feu à une stratégie échoue si une règle a déjà été créée à l'aide d'une plage d'adresses IP.

Liste des problèmes corrigés dans la version 14.1

Identifiant	Description
10140523	L'activation du NVMe natif dans Windows 11 peut entraîner un comportement instable de l'application.
9340076	Sur un appareil sur lequel l'application est installée et le module Chiffrement des fichiers est activé, l'Explorateur Windows n'actualise pas automatiquement le contenu d'un dossier réseau après sa modification depuis un autre appareil.

Identifiant	Description
9722863	Le rapport du Contrôle des appareils n'inclut pas l'événement de déconnexion du jeton USB.
10006481	Après l'application d'une règle qui refuse le trafic entrant, les connexions TCP actives aux services externes peuvent être interrompues prématurément en raison d'un calcul incorrect du délai d'expiration.
10140912	L'application ne détecte pas l'appareil PDA BHT1100B.
10157563	Folder Redirection peut ne pas fonctionner après un redémarrage sur les postes de travail VDI.
10158494	Le Contrôle des appareils enregistre plusieurs événements de connexion et de déconnexion d'un appareil amovible sans reconnexion physique de celui-ci.

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 ?

DÉPLOIEMENT

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 réalise la mise à jour ?

SÉCURITÉ

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 analyse des logiciels malveillants 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 ?

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

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 ?

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.

L'application n'est pas conçue pour être utilisée dans des processus technologiques impliquant des systèmes de contrôle automatisés. Pour protéger les appareils dans de tels systèmes, il est recommandé d'utiliser l'application Kaspersky Industrial CyberSecurity for Nodes.

Technologies de détection des menaces

Machine learning

Kaspersky Endpoint Security utilise un modèle basé sur l'apprentissage machine. Ce modèle a été développé par les experts de Kaspersky. Ensuite, le modèle est continuellement alimenté en données sur les menaces provenant du réseau KSN (entraînement du modèle).

Analyse 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 d'experts

Kaspersky Endpoint Security utilise des données sur les menaces ajoutées par les analystes de virus de Kaspersky. Les analystes de virus évaluent 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 du système d'analyse automatique des objets. Le système traite tous les objets qui sont envoyés à Kaspersky. Le système détermine ensuite la réputation des objets et ajoute les données aux bases antivirus. Si le système ne parvient pas à déterminer la réputation d'un objet, il envoie des demandes aux analystes de virus de Kaspersky.

Sandbox

Kaspersky Endpoint Security traite l'objet dans une machine virtuelle. Kaspersky Sandbox analyse le comportement de l'objet et prend une décision concernant sa réputation. Cette technologie est disponible uniquement si vous utilisez la solution Kaspersky Sandbox.

Cloud Sandbox

Kaspersky Endpoint Security analyse les objets dans un environnement isolé fourni par Kaspersky. La technologie Cloud Sandbox est activée en permanence et est disponible pour tous les utilisateurs de Kaspersky Security Network, quel que soit le type de licence qu'ils utilisent. Si vous avez déjà déployé la solution Endpoint Detection and Response, vous pouvez activer un compteur distinct pour les menaces détectées par Cloud Sandbox.

Modules de l'application

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.

Section	Module
Protection principale	**Protection contre les fichiers malicieux** Le module Protection contre les fichiers malicieux vous permet d'empêcher l'infection du système de fichiers de l'ordinateur. Par défaut, le module Protection contre les fichiers malicieux réside en permanence dans la mémoire vive (RAM) de l'ordinateur et analyse en temps réel tous les fichiers ouverts, enregistrés ou exécutés. Ce module analyse les fichiers sur tous les disques de l'ordinateur, y compris 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. **Protection contre les menaces Internet** Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants depuis Internet et 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. **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 protège l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et d'une analyse heuristique. La Protection contre les menaces par emails peut analyser les messages entrants et sortants. L'application prend en charge les protocoles POP3, SMTP, IMAP et NNTP dans les clients de messagerie suivants : • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Pour analyser le trafic dans les clients de messagerie Mozilla Thunderbird, MyOffice Mail et R7-Office Organizer, vous devez ajouter le certificat Kaspersky à la liste de certificats et sélectionner la propre liste de certificats. La Protection contre les menaces par emails ne prend pas en charge d'autres protocoles et clients de messagerie. La Protection contre les menaces par emails peut ne pas toujours être en mesure d'accéder aux messages *au niveau du protocole* (par exemple, lors de l'utilisation de la solution Microsoft Exchange). Pour cette raison, la Protection contre les menaces par emails inclut une extension pour Microsoft Office Outlook. L'extension permet d'analyser les messages *au niveau du client de messagerie*. L'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2010, 2013, 2016, 2019, 2021, 2024 et 365. Sur les ordinateurs équipés d'un processeur ARM, l'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2016, Outlook 2021, Outlook 2024 et Outlook 365 pour ARM64. **Protection contre les menaces réseau** Le module *Protection contre les menaces réseau* (également appelé Intrusion Detection System, IDS) surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, l'application 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 l'application. 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. **Pare-feu** Le module Pare-feu bloque les connexions non autorisées à un 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. **Protection BadUSB** Le module Protection BadUSB permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier. **Protection AMSI** Le module Protection AMSI est destiné à prendre en charge 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.

Section	Module
Protection avancée	**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. 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 à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés . **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 repose sur les modèles de comportement dangereux et garantit la protection proactive de l'ordinateur. Le module Détection comportementale surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus. **Protection contre le chiffrement** Le module Protection contre le chiffrement 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. **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. Le module Protection contre les Exploits surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus. **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. **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.
Contrôles de sécurité	**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. **Contrôle des appareils** Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à un 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. **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 dont l'accès est limité par Contrôle Internet, Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement. **Contrôle évolutif des anomalies** 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 suite 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 les bases de données de l'application. **Inspection des journaux** L'inspection des journaux surveille l'intégrité de l'environnement protégé en fonction de l'analyse du journal des événements Windows. Lorsque l'application détecte des signes de comportement atypique dans le système, elle en informe l'administrateur, car ce comportement peut indiquer une tentative de cyberattaque. **Contrôle de l'intégrité du système** Le module Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Endpoint Security génère les événements correspondants et en informe l'administrateur.

Section	Module
Tâches	**Analyse des logiciels malveillants** Kaspersky Endpoint Security analyse l'ordinateur à la recherche de virus et d'autres menaces. L'Analyse des logiciels malveillants 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. **Mise à jour des bases et des modules d'application** 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. 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. **Annulation 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. **Vérification de l'intégrité de l'application** 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.
Chiffrement des données	**Chiffrement des fichiers** Le module permet de créer des règles de chiffrement de fichiers. Vous pouvez sélectionner des dossiers standards pour le chiffrement, sélectionner un dossier manuellement ou sélectionner des fichiers individuels par extension. **Chiffrement du disque** Le module permet de chiffrer le disque dur à l'aide de Kaspersky Disk Encryption ou de Chiffrement de disque BitLocker. **Chiffrement des disques amovibles** Le module permet de protéger les données sur les disques amovibles. Vous pouvez utiliser le Chiffrement du disque (FDE) ou le Chiffrement des fichiers (FLE).

Section	Module
Detection and Response	**Endpoint Detection and Response Optimum** Agent intégré pour la solution Kaspersky Endpoint Detection and Response Optimum (ci-après également "EDR Optimum"). *Kaspersky Endpoint Detection and Response* est une solution permettant de protéger l'infrastructure informatique des entreprises contre les cybermenaces avancées. La fonctionnalité de la solution combine la détection automatique des menaces avec la capacité de réagir à ces menaces pour contrer les attaques avancées, notamment les nouveaux exploits, les ransomwares, les attaques sans fichier ainsi que les méthodes utilisant des outils système légitimes. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agent intégré pour la solution Kaspersky Endpoint Detection and Response Expert (ci-après également "EDR Expert"). EDR Expert offre davantage de fonctionnalités de surveillance et de réponse aux menaces que EDR Optimum. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** et **Network Detection and Response (KATA)** Agents intégrés pour la gestion des modules Endpoint Detection and Response et Network Detection and Response qui font partie de la solution 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 trois unités fonctionnelles : • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Vous pouvez acheter l'ensemble des unités fonctionnelles ou des unités fonctionnelles individuelles séparément. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform. **Sandbox** Agent intégré pour Sandbox. Le module *Sandbox* détecte et bloque automatiquement les menaces avancées sur les ordinateurs. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Sandbox et Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agent intégré pour prendre en charge le fonctionnement de la solution Kaspersky Managed Detection and Response. La solution *Kaspersky Managed Detection and Response (MDR)* détecte et analyse automatiquement les incidents de sécurité dans votre infrastructure. Pour ce faire, MDR utilise les données de télémétrie reçues des terminaux et Machine learning. MDR envoie les données de l'incident aux experts de Kaspersky. Les experts peuvent alors traiter l'incident et, par exemple, ajouter une nouvelle entrée dans les bases antivirus. Les experts peuvent également émettre des recommandations sur le traitement de l'incident et, par exemple, suggérer d'isoler l'ordinateur du réseau. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Managed Detection and Response.

Modes de l'application : Standard, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows fait partie de nombreuses solutions Kaspersky. En fonction de la solution, vous devez sélectionner un mode pour l'application.

Mode Standard

Il s'agit du mode principal et par défaut de l'application. Vous pouvez installer l'application dans ce mode dans le cadre des solutions Kaspersky EPP (Endpoint Protection Platform). Par exemple, Kaspersky Endpoint Security en mode Standard fait partie de Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security offre une protection complète des postes de travail et des serveurs contre diverses menaces, attaques réseau et escroqueries. En mode standard, des agents intégrés peuvent également être associés aux solutions Kaspersky Detection and Response, notamment EDR, MDR, KUMA et d'autres.

EDR Agent

Ce mode permet de déployer les solutions Kaspersky Detection and Response avec des solutions EPP tierces. Les solutions Detection and Response incluent Kaspersky Managed Detection and Response (MDR) et Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent prend également en charge la solution SIEM de Kaspersky, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Dans ce mode, les modules de protection standard comme la Protection contre les menaces sur les fichiers ou la Protection contre les menaces Internet ne sont pas disponibles. La protection standard de l'ordinateur est assurée par la solution EPP tierce. EDR Agent surveille en permanence les processus s'exécutant sur ces ordinateurs, les connexions réseau ouvertes et les fichiers en cours de modification, et il interagit avec les solutions Detection and Response.

Light Agent

Ce mode sert à protéger les environnements virtuels. Kaspersky Endpoint Security en mode Light Agent fait partie de la solution Kaspersky Hybrid Cloud Security. Le Light Agent protège les machines virtuelles avec des systèmes d'exploitation invités pour les postes de travail et les serveurs. Les mêmes modules de protection et de contrôle sont disponibles dans ce mode et dans le mode Standard. La différence est que les objets sont analysés à la recherche de virus et d'autres programmes malveillants par un module de solution spécial installé sur une machine virtuelle distincte, ou SVM (Secure Virtual Machine). Ainsi, le Light Agent utilise les ressources de la SVM pour assurer la sécurité de l'infrastructure au lieu des ressources de la machine virtuelle.

Distribution

La distribution contient les paquets de distribution suivants :

- **AES256**

  Ce paquet de distribution est conçu pour être installé sur des ordinateurs avec une architecture x86/x64. Ce paquet de distribution contient des outils cryptographiques qui mettent en œuvre l'algorithme de chiffrement AES (Advanced Encryption Standard) avec une longueur de clé effective de 256 bits.

- **AES56**

  Ce paquet de distribution est conçu pour être installé sur des ordinateurs avec une architecture x86/x64. Le paquet de distribution contient les outils de chiffrement qui exploitent l'algorithme de chiffrement AES avec une clé de 56 bits.

- **Arm64**

  Ce paquet de distribution est conçu pour être installé sur des ordinateurs basés sur l'architecture ARM. Ce paquet de distribution n'est pas conçu pour être installé sur des serveurs.

Avant l'installation, assurez-vous que le paquet de distribution correspond à l'architecture de votre processeur. Si le paquet de distribution ne correspond pas à l'architecture du processeur, le programme d'installation terminera l'installation sur une erreur.

Le paquet de distribution est une archive autoextractible au format EXE. Pour afficher le contenu du paquet de distribution, vous devez extraire l'archive dans un dossier séparé. Chaque paquet de distribution contient les fichiers suivants :

`kes_win.msi`	Fichier 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 de gestion des applications dans la Console d'administration de Kaspersky Security Center.
`bases.cab`	Les fichiers des paquets de mise à jour utilisés lors de l'installation de l'application.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Fichiers pour la suppression des applications incompatibles.
`incompatible.txt`	Fichier contenant la liste des logiciels susceptible de poser des problèmes de compatibilité avec Kaspersky Endpoint Security. Kaspersky ne garantit pas la compatibilité de Kaspersky Endpoint Security avec les logiciels de la liste.
`ksn_<language ID>.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.
`kes.cab`	Fichiers pour l'interface graphique de l'application.
`aes256.cab` / `aes56.cab`	Fichiers pour l'algorithme de chiffrement AES (non inclus dans le paquet de distribution Arm64).
`package.kcat`	Dossier contenant les signatures du kit de distribution de l'application. La signature numérique garantit l'authenticité et l'intégrité du kit de distribution de l'application.

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

Cet article répertorie les versions des logiciels sur lesquelles l'application a été testée et avec lesquelles son bon fonctionnement est garanti. L'application peut également fonctionner avec d'autres versions de logiciels, mais ces configurations n'ont pas fait l'objet d'un cycle de test complet et ne figurent pas dans la liste des versions dont la prise en charge est garantie.

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

Pour installer l'application, vous devez disposer des privilèges d'administrateur sur l'ordinateur.

Configuration minimale requise

Exigences minimales	Poste de travail (x86/x64)	Serveur (x86/x64)	Arm
Stockage	2 Go	2 Go	2 Go
Processeur	1 GHz, prise en charge des instructions SSE2	1,4 GHz, prise en charge des instructions SSE2	1 GHz, architecture Armv8.1
Mémoire vive	Poste de travail (x86) : 1 Go Poste de travail (x64) : 2 Go	2 Go Remarque : Le serveur requiert 8 Go de mémoire pour installer l'application avec l'agent intégré permettant l'intégration à Kaspersky Anti Targeted Attack Platform.	4 Go
Microsoft .NET Framework	4 ou ultérieur	4 ou ultérieur	4.8 ou ultérieur

Postes de travail

Systèmes d'exploitation compatibles pour les postes de travail :

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1
- Windows 8 Professional/Enterprise
- Windows 8.1 Professional/Enterprise
- Windows 10 Home/Pro/Pro for Workstations/Education/Enterprise/Enterprise multi-session
- Windows 11 Home/Pro/Pro for Workstations/Education/Enterprise/Enterprise multi-session
- Windows 11 for Arm64 Home/Pro/Pro for Workstations/Education/Enterprise

Les systèmes d'exploitation Windows, à partir de la version 11 24H2, prennent en charge le UDP Receive Segment Coalescing Offload (URO). La technologie est activée par défaut si la carte réseau compatible et les pilotes sont installées sur l'ordinateur. La désactivation d'URO sur l'ordinateur d'un utilisateur peut réduire considérablement les performances de l'application.

Pour assurer le bon fonctionnement de Kaspersky Endpoint Security, le service Windows Security Center (wscsvc) doit être exécuté sur l'ordinateur de l'utilisateur.

Kaspersky Endpoint Security ne peut pas être installé sur Microsoft Windows 7 sans la présence des mises à jour suivantes du système d'exploitation : KB4490628 (12 mars 2019) et KB4474419 (23 septembre 2019). Pour en savoir plus, consultez la Base des connaissances du Support Technique.

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

Les particularités de la prise en charge du système d'exploitation Microsoft Windows 11 sont reprises dans la base des connaissances du Support Technique.

Serveurs

Kaspersky Endpoint Security prend en charge des principaux modules de l'application sur les ordinateurs fonctionnant sous le système d'exploitation Windows pour les serveurs. Vous pouvez utiliser Kaspersky Endpoint Security for Windows à la place de Kaspersky Security for Windows Server sur les serveurs et clusters de votre organisation (Cluster Mode). L'application prend également en charge le Server Core Mode (voir les problèmes connus).

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 Web Server 2008 R2 Service Pack 1 ;
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2016 Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2019 Essentials/Standard/Datacenter (y compris le mode Server Core) ;

- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (y compris le mode Server Core) ;
- Serveur Windows 2025 Standard/Datacenter.

Kaspersky Endpoint Security ne peut pas être installé sur Microsoft Windows Server 2008 R2 sans la présence des mises à jour suivantes du système d'exploitation : KB4490628 (12 mars 2019) et KB4474419 (23 septembre 2019).

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 :

Les particularités de la prise en charge du système d'exploitation Microsoft Windows Server 2022 sont reprises dans la base des connaissances du Support Technique.

Systèmes d'exploitation non compatibles pour les serveurs :

- Windows Server 2003 Standard/Enterprise/Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation/Standard/Enterprise/Datacenter Service Pack 2 et suivants ;
- Windows Server 2008 Standard/Enterprise/Datacenter Service Pack 2
- Windows Server 2008 Core Standard/Enterprise/Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard/Premium Service Pack 2

Plateformes virtuelles

Plateformes virtuelles prises en charge pour une utilisation des applications en mode standard :

- VMware Workstation Pro 15.5.2 ;
- Version corrective de VMware ESXi 7.0 ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009 ;
- Citrix Provisioning 2009 ;
- Citrix Hypervisor 8.2 LTSR

L'application prend en charge les machines virtuelles créées à l'aide d'Hyper-V sous Windows 11 Pro Arm64.

Machines virtuelles pour l'installation de Light Agent

L'installation de Kaspersky Endpoint Security en mode Light Agent sur des machines virtuelles basées sur l'architecture ARM n'est pas prise en charge.

Le BIOS sur les machines virtuelles doit prendre en charge la spécification SMBIOS version 2.1 ou toute version ultérieure.

Les paquets et utilitaires suivants doivent être installés sur des machines virtuelles :

- Lors de l'utilisation de Microsoft Hyper-V – paquet Integration Services.
- Lors de l'utilisation de VMware vSphere – paquet VMware Tools.
- Lors de l'utilisation de XenServer – paquet XenTools.
- Lors de l'utilisation de HUAWEI FusionSphere – paquet HUAWEI Tools.
- Lors de l'utilisation d'hyperviseurs basés sur KVM – QEMU Guest Agent.

Consultez l'aide de Kaspersky Security for Virtualization Light Agent afin de connaître la configuration requise de l'infrastructure virtuelle pour l'exécution de l'application en mode Light Agent.

Pour le bon fonctionnement de l'application, il faut utiliser une interface réseau virtualisée dont la bande passante est d'au moins 100 Mbit/s.

Serveurs de terminaux

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
- Microsoft Remote Desktop Services basé sur Windows Server 2022
- Microsoft Remote Desktop Services basé sur Windows Server 2025
- Citrix RDSH inclus dans Citrix Virtual Apps and Desktops 7 2507 LTSR

Prise en charge de Kaspersky Security Center

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

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

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).

À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez configurer différents ensembles de modules pour différents types de système d'exploitation dans le paquet d'installation. Autrement dit, vous pouvez déployer l'application sur les postes de travail et les serveurs à l'aide du même paquet d'installation.

L'installation de Kaspersky Endpoint Security en mode Light Agent sur des machines virtuelles basées sur l'architecture ARM n'est pas prise en charge.

Fonction	Poste de travail	Poste de travail basé sur l'architecture ARM	Serveur	Mode Server Core
Protection avancée				
Kaspersky Security Network	✓	✓	✓	✓
Détection comportementale	✓	✓	✓	✓
Protection contre le chiffrement	✓	✓	✓	✓
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	✓	✓	✓	–
Pare-feu	✓	✓	✓	✓
Protection contre les menaces réseau	✓	✓	✓	✓
Protection BadUSB	✓	✓	✓	–
Protection AMSI	✓	✓	✓	✓
Contrôles de sécurité				
Inspection des journaux	–	–	✓	–
Contrôle des applications	✓	✓	✓	✓
Contrôle des appareils	✓	✓	✓	✓
Contrôle Internet	✓	✓	✓	–
Contrôle évolutif des anomalies	✓	✓	–	–
Contrôle de l'intégrité du système	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Chiffrement des données				
Kaspersky Disk Encryption	✓	–	–	–
Chiffrement de disque BitLocker	✓	✓	✓	✓
Chiffrement des fichiers	✓	–	–	–
Chiffrement des disques amovibles	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Intégration KUMA	✓	✓	✓	✓

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 suivantes :

- Console d'administration. Module logiciel enfichable pour la Microsoft Management Console (MMC) installée sur le poste de travail de l'administrateur.
- Web Console. Module de Kaspersky Security Center installé sur le Serveur d'administration. Vous pouvez travailler dans Web Console à l'aide d'un navigateur sur n'importe quel ordinateur.

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.

Kaspersky Endpoint Security fait partie de la solution Kaspersky Next Pro View. Pour en savoir plus sur les fonctionnalités de l'application lorsqu'elle fonctionne dans le cadre de cette solution, consultez l'aide de Kaspersky Next.

Comparaison des fonctions de Kaspersky Endpoint Security

Fonction	Kaspersky Security Center		Kaspersky Security Center
	Console d'administration	Web Console	Cloud Console
Protection avancée			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Détection comportementale	✓	✓	✓
Protection contre le chiffrement			
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	✓	✓	✓
Pare-feu	✓	✓	✓
Protection contre les menaces réseau	✓	✓	✓
Protection BadUSB	✓	✓	✓
Protection AMSI	✓	✓	✓

Fonction	Kaspersky Security Center		Kaspersky Security Center
	Console d'administration	Web Console	Cloud Console
Contrôles de sécurité			
Inspection des journaux	✓	✓	✓
Contrôle des applications	✓	✓	✓
Contrôle des appareils	✓	✓	✓
Contrôle Internet	✓	✓	✓
Contrôle évolutif des anomalies	✓	✓	✓
Contrôle de l'intégrité du système	✓	✓	✓
Cloud Discovery	–	–	✓
Chiffrement des données			
Kaspersky Disk Encryption	✓	✓	–
Chiffrement de disque BitLocker	✓	✓	✓
Chiffrement des fichiers	✓	✓	–
Chiffrement des disques amovibles	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Intégration KUMA	✓	✓	✓
Tâches			
Ajout d'une clé	✓	✓	✓
Modification de la sélection des modules de l'application	✓	✓	✓
Inventaire	✓	✓	✓
Mise à jour	✓	✓	✓
Annulation de la mise à jour	✓	✓	✓
Analyse des logiciels malveillants	✓	✓	✓
Vérification de l'intégrité de l'application	✓	✓	–
Suppression des données	✓	✓	✓
Administrer les comptes de l'Agent d'authentification (Kaspersky Disk Encryption)	✓	✓	–
Analyse IOC (EDR)	–	✓	✓
Déplacement du fichier en quarantaine (EDR)	–	✓	✓
Obtention du fichier (EDR)	–	✓	✓
Supprimer le fichier (EDR)	–	✓	✓
Démarrage du processus (EDR)	–	✓	✓
Fin du processus (EDR)	–	✓	✓

Compatibilité avec d'autres applications

Kaspersky Endpoint Security est incompatible avec certaines applications de Kaspersky ainsi qu'avec certaines applications tierces. Par conséquent, avant d'installer, de mettre à jour la version de l'application et de modifier les modules de l'application, Kaspersky Endpoint Security analyse l'ordinateur pour vérifier si de telles applications sont présentes.

Compatibilité avec les applications tierces

Kaspersky Endpoint Security est incompatible avec les applications qui font partie de systèmes tiers de protection des terminaux (Endpoint Protection Platform, PPE). Kaspersky Endpoint Security peut également rencontrer des problèmes de compatibilité avec d'autres applications. Pour déterminer la compatibilité, Kaspersky Endpoint Security se base sur une liste de logiciels établie par Kaspersky. Cette liste est contenue dans le fichier incompatible.txt. Ce fichier est inclus dans le kit de distribution.

Kaspersky ne garantit pas la compatibilité de Kaspersky Endpoint Security avec les logiciels de la liste. Si une application de la liste est découverte, le programme d'installation arrête le déploiement de Kaspersky Endpoint Security. Il se peut que le programme d'installation supprime automatiquement certaines applications de la liste. Si vous êtes prêt à ignorer les risques et que vous souhaitez installer Kaspersky Endpoint Security ainsi qu'un logiciel de la liste sur le même ordinateur, vous pouvez ignorer la vérification de l'ordinateur (voir les instructions ci-dessous).

TÉLÉCHARGER LE FICHIER INCOMPATIBLE.TXT

Compatibilité avec les applications de Kaspersky

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

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.

- Endpoint Sensor dans le cadre de Kaspersky Anti Targeted Attack Platform et des solutions Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent dans le cadre des solutions Detection and Response de Kaspersky.

  Kaspersky modifie le processus pour que toutes les solutions Detection and Response fonctionnent avec l'agent intégré de Kaspersky Endpoint Security à la place de Kaspersky Endpoint Agent. À partir de la version 12.1, l'application prend en charge toutes les solutions Detection and Response.

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

  À partir de Kaspersky Endpoint Security 12.0, vous pouvez migrer de Kaspersky Security for Windows Server vers Kaspersky Endpoint Security for Windows et utiliser la même solution pour protéger les postes de travail et les serveurs.

- 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.

Ignorer la vérification de la présence de logiciels susceptibles de poser des problèmes de compatibilité

Si Kaspersky Endpoint Security détecte un logiciel dans la liste incompatible.txt, l'installation de l'application sera interrompue. Pour poursuivre l'installation, il faut supprimer cette application. Toutefois, si le fournisseur du logiciel tiers a indiqué dans sa documentation que son logiciel est compatible avec Endpoint Protection Platform (PPE), vous pouvez installer Kaspersky Endpoint Security sur un ordinateur où est installée une application de ce fournisseur. Par exemple, le fournisseur de la solution Endpoint Detection and Response (EDR) peut indiquer que celle-ci est compatible avec des systèmes PPE tiers. Si c'est le cas, vous devez lancer l'installation de Kaspersky Endpoint Security sans exécuter de vérification d'installation du logiciel. Pour ce faire, transmettez les paramètres suivants au programme d'installation :

- `SKIPPRODUCTCHECK=1` Désactivez la recherche d'un logiciel installé. La liste des logiciels susceptibles de poser des problèmes de compatibilité figure dans le fichier incompatible.txt du kit de distribution. Si aucune valeur n'est définie pour ce paramètre et qu'aucun logiciel de la liste n'est détecté, l'installation de Kaspersky Endpoint Security sera interrompue.
- `SKIPPRODUCTUNINSTALL=1` Désactivez la suppression automatique des logiciels détectés de la liste incompatible.txt. Si le paramètre n'est pas spécifié, Kaspersky Endpoint Security tente de supprimer le logiciel susceptible de poser des problèmes de compatibilité.
- `CLEANERSIGNCHECK=0` Désactivez la vérification de la signature numérique des applications trouvées par le contrôle. Si ce paramètre n'est pas défini, la vérification des signatures numériques est désactivée lors du déploiement de l'application via Kaspersky Security Center. Lorsque l'application est installée localement, la vérification de la signature numérique est activée par défaut.

Vous pouvez transmettre des paramètres dans la ligne de commande lors de l'installation locale de l'application.

Si, au cours du processus d'installation, vous avez ignoré la recherche de logiciels susceptibles de provoquer des problèmes de compatibilité, Kaspersky Endpoint Security peut exécuter à nouveau cette vérification lorsque les modules de l'application changent. Pour ignorer la recherche des logiciels installés, vous devez configurer la tâche *Modification de la sélection des modules de l'application*.

Exemple :

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Pour installer Kaspersky Endpoint Security à distance, vous devez ajouter les paramètres appropriés au fichier de génération du paquet d'installation nommé `kes_win.kud` dans `[Setup]` (voir ci-dessous). Le fichier `kes_win.kud` est inclus dans le kit de distribution.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

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.
- 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 .
4. Les paramètres reçus du fichier de configuration (install.cfg).

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.

Lors de l'installation de Kaspersky Endpoint Security, le système d'exploitation peut afficher ses propres messages. Les connexions réseau et Internet peuvent également être interrompues pendant l'installation de l'application.

Lors de l'installation, de la mise à jour ou de la désinstallation de Kaspersky Endpoint Security, des erreurs peuvent survenir. Pour en savoir plus sur la résolution de ces erreurs, consultez la Base de connaissances du support technique.

Déploiement via Kaspersky Security Center

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. Avant d'installer l'application, vous devez vous assurer que l'Agent d'administration de Kaspersky Security Center est installé sur l'ordinateur. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client.

Kaspersky Security Center 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 fichier d'installation ;
  2. création de la tâche d'installation à distance.

Kaspersky Security Center 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.

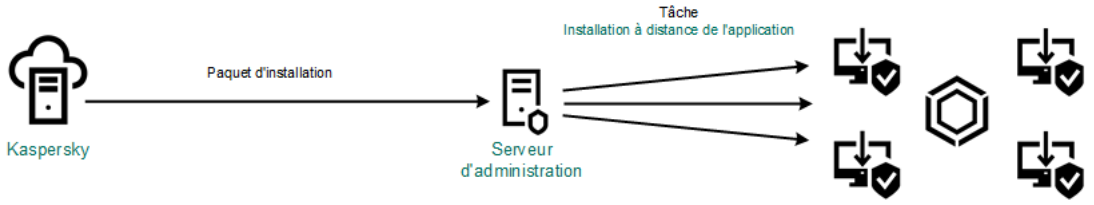
Installation standard de l'application

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 fichier d'installation de Kaspersky Endpoint Security.

   Le *fichier 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 fichier 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 fichier d'installation est créé sur la base des fichiers portant l'extension kpd et kud qui figurent dans la distribution de l'application. Le fichier 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 *Installation à distance d'une application* du Serveur d'administration de Kaspersky Security Center.



Déploiement de Kaspersky Endpoint Security

Procédure de lancement de l'Assistant de déploiement de sécurité dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Avancé** → **Installation à distance**.
3. 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 fichier d'installation

Sélectionnez le fichier de Kaspersky Endpoint Security dans la liste des fichiers d'installation. Si le fichier 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 fichiers 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.

Sélectionnez la source **Déployer le paquet Kaspersky Security Center**.

Étape 3. 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 4. Définition des paramètres de la tâche d'installation à distance

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le téléchargement du paquet d'installation**. Sélectionnez le mode d'installation de l'application :
  - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Endpoint Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.
  - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier 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.
  - **En utilisant les ressources du système d'exploitation via le 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 pour les appareils administrés via d'autres Serveurs d'administration**. 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 réinstaller l'application si elle est déjà installée**. Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.
- **Fixer l'installation de l'Agent d'administration dans les stratégies de groupe d'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 5. Sélection de la clé de licence

Ajoutez la clé au fichier 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 *Ajout d'une clé*.

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. 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 9. Lancement de l'installation

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. 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, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **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 fichier d'installation

Sélectionnez le fichier de Kaspersky Endpoint Security dans la liste des fichiers d'installation. Si le fichier d'installation de Kaspersky Endpoint Security ne figure pas dans la liste, vous pouvez le créer dans l'Assistant. Pour créer le fichier 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 fichier d'installation est automatique. Kaspersky met à jour la liste après l'émission des nouvelles versions des applications.

Vous pouvez configurer les paramètres des fichiers 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 fichier 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 *Ajout d'une 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 téléchargement du paquet d'installation**. Sélectionnez le mode d'installation de l'application :
  - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Endpoint Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.
  - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier 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.
  - **En utilisant les ressources du système d'exploitation via le 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 réinstaller l'application si elle est déjà installée**. Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.
- **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'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 définis**.

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. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Création du fichier d'installation

Le *fichier 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 fichier 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 fichier d'installation est créé sur la base des fichiers portant l'extension kpd et kud qui figurent dans la distribution de l'application. Le fichier 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 fichier 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 **Créer un paquet d'installation**.

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

Étape 1. Sélection du type de fichier d'installation

Choisissez l'option **Créer un paquet d'installation pour une application Kaspersky**.

Étape 2. Sélection du nom du fichier d'installation

Saisissez le nom du paquet d'installation, par exemple, *Kaspersky Endpoint Security for Windows 14.2*.

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 kit de distribution.

Si nécessaire, mettez à jour les bases antivirus dans le paquet d'installation à l'aide de la case **Copier les mises à jour depuis le 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 fichier d'installation est créé et ajouté dans Kaspersky Security Center. Le fichier 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.

Dans les paramètres du paquet d'installation, vous pouvez sélectionner des modules d'application pour différents types de système d'exploitation. Autrement dit, le paquet d'installation inclut deux ensembles de modules, pour les postes de travail et pour les serveurs. Avant de déployer le paquet d'installation, le programme d'installation détecte le type du système d'exploitation et installe uniquement les modules d'application que vous avez sélectionnés pour ce type de système d'exploitation. De cette façon, vous pouvez utiliser le même paquet d'installation pour les postes de travail et les serveurs.

Le fichier d'installation contient les bases antivirus du stockage du Serveur d'administration. Vous pouvez mettre à jour les bases dans le fichier d'installation pour réduire la consommation de trafic lors de la mise à jour des bases après l'installation de Kaspersky Endpoint Security.

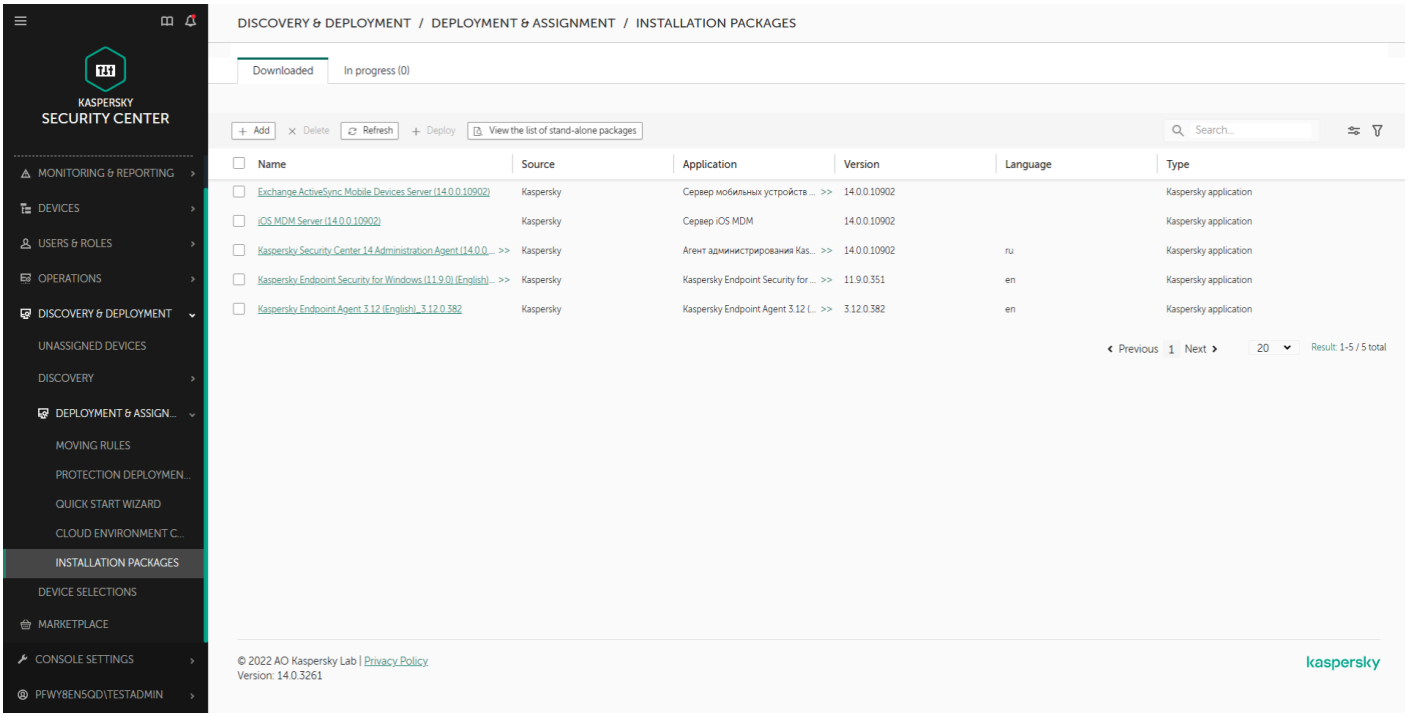
Comment créer un paquet d'installation dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

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

2. Cliquez sur **Ajouter**.

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



Liste des paquets d'installation

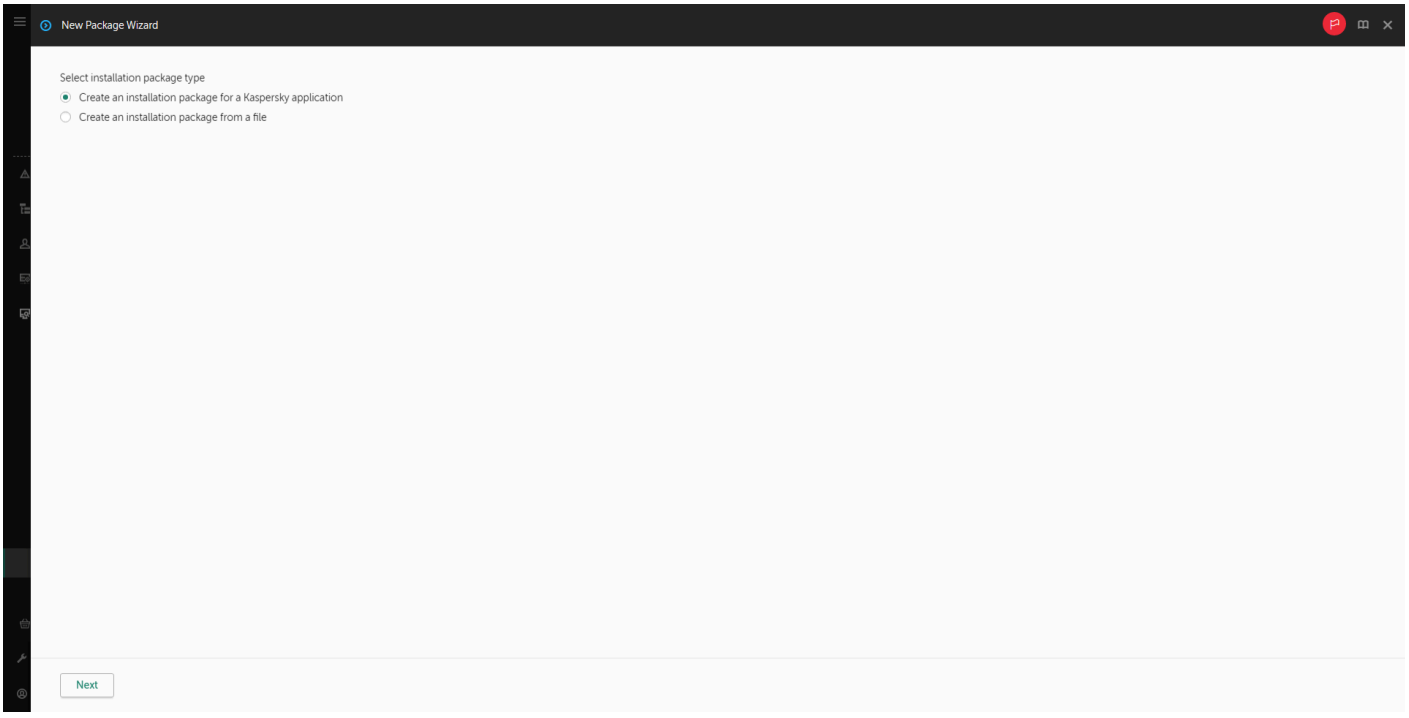
Étape 1. Sélection du type de fichier d'installation

Choisissez l'option **Générer un paquet d'installation pour une application Kaspersky**.

L'Assistant créera un fichier 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 fichier d'installation à partir d'un fichier.

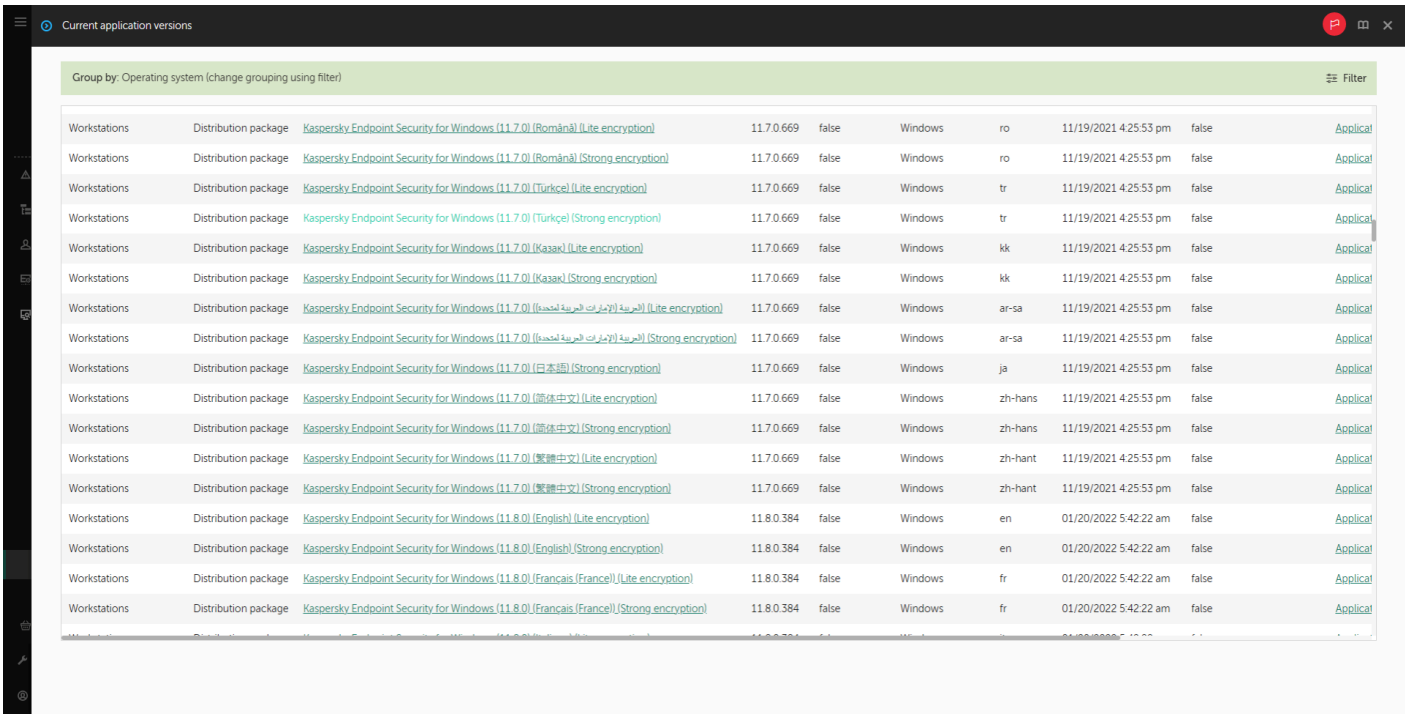
La création du paquet d'installation de Kaspersky Endpoint Security à partir d'un fichier est accessible uniquement dans Kaspersky Security Center Web Console.



Types de paquets d'installation

Étape 2. Paquets d'installation

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



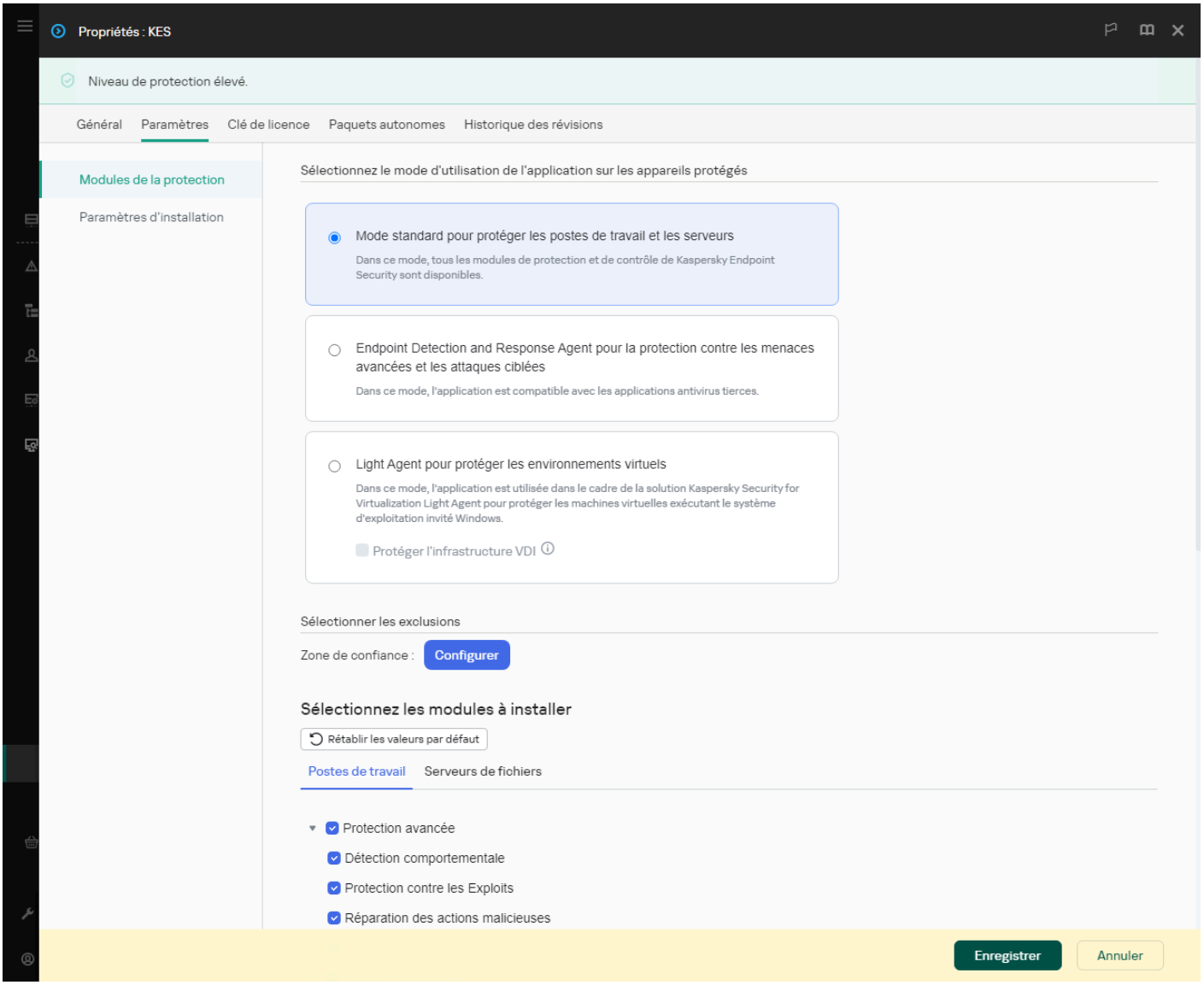
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Lite encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Strong encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Lite encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Strong encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Lite encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Strong encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Lite encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Strong encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (日本語) (Strong encryption)	11.7.0.669	false	Windows	ja	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Strong encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Lite encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Strong encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat

Liste des paquets d'installation sur les serveurs Kaspersky

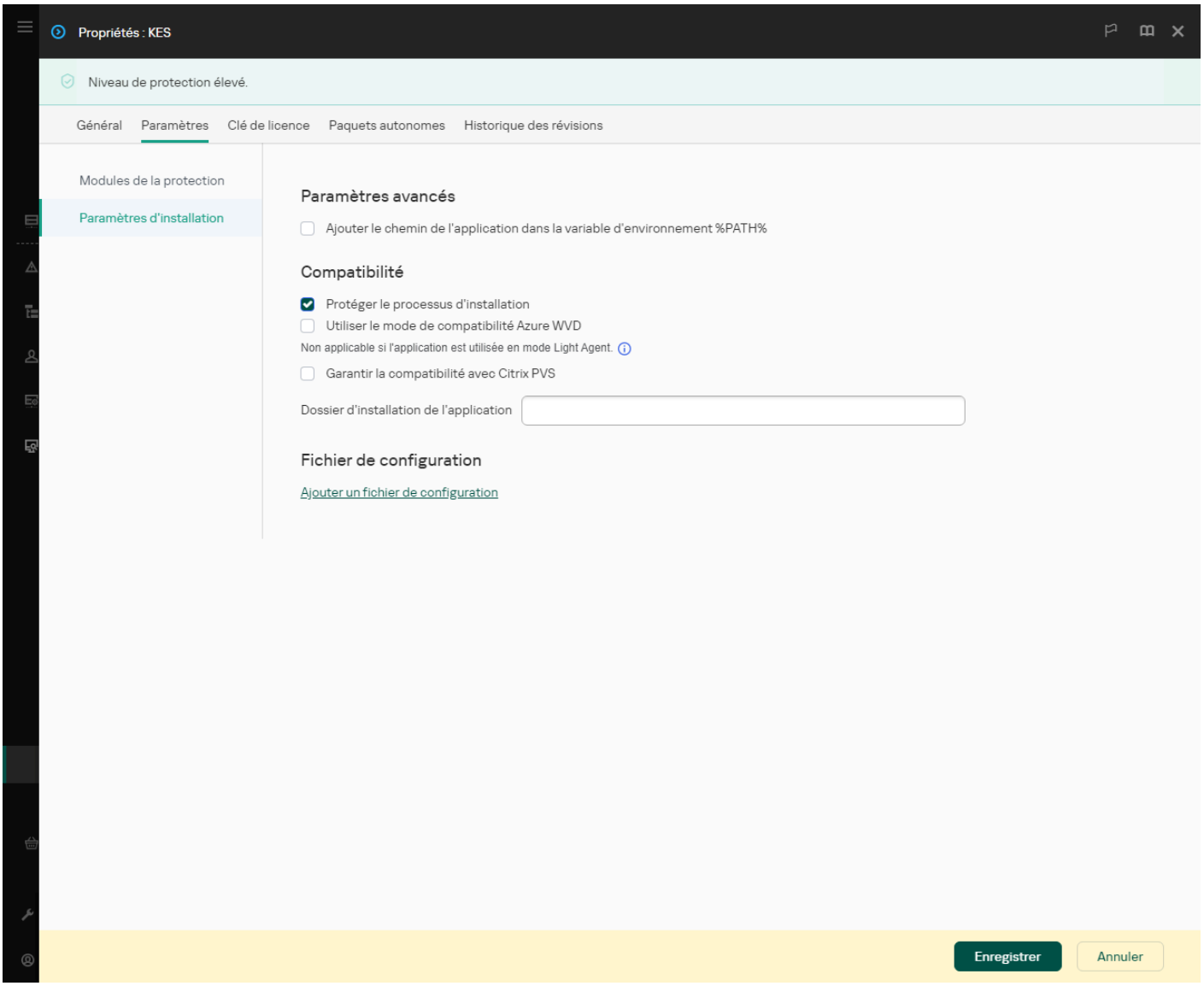
Le fichier d'installation est créé et ajouté dans Kaspersky Security Center. Le fichier d'installation permet d'installer Kaspersky Endpoint Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application.

Dans les paramètres du paquet d'installation, vous pouvez sélectionner des modules d'application pour différents types de système d'exploitation. Autrement dit, le paquet d'installation inclut deux ensembles de modules, pour les postes de travail et pour les serveurs. Avant de déployer le paquet d'installation, le programme d'installation détecte le type du système d'exploitation et installe uniquement les modules d'application que vous avez sélectionnés pour ce type de système d'exploitation. De cette façon, vous pouvez utiliser le même paquet d'installation pour les postes de travail et les serveurs.

Le fichier d'installation contient les bases antivirus du stockage du Serveur d'administration. Vous pouvez mettre à jour les bases dans le fichier d'installation pour réduire la consommation de trafic lors de la mise à jour des bases après l'installation de Kaspersky Endpoint Security.



Modules inclus dans le paquet d'installation



Paramètres d'installation du paquet d'installation

Paramètres du fichier d'installation

Section	Description
Modules de la protection	**Mode standard**. La configuration par défaut. Cette configuration vous permet d'utiliser tous les modules de l'application, y compris les modules qui prennent en charge les solutions Detection and Response. Cette configuration est utilisée pour assurer une protection complète de l'ordinateur contre diverses menaces, attaques réseau et fraudes. **Endpoint Detection and Response Agent**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces. **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Section	Description
Exclusions	À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware. Vous pouvez également configurer la zone de confiance plus tard dans les propriétés de la stratégie : exclusions d'analyse et applications de confiance.
Sélectionnez les modules à installer	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*. Vous pouvez créer des ensembles de modules distincts pour les postes de travail et les serveurs. Avant de déployer le paquet d'installation, le programme d'installation détecte le type du système d'exploitation et installe uniquement les modules d'application que vous avez sélectionnés pour ce type de système d'exploitation. De cette façon, vous pouvez utiliser le même paquet d'installation pour les postes de travail et les serveurs. L'ensemble des modules disponibles dépend de la configuration de l'application : **Mode standard** Kaspersky Data Encryption, le Chiffrement des fichiers et tous les agents intégrés, à l'exception d'EDR Optimum, ne sont pas installés par défaut. Ces modules peuvent être ajoutés dans les paramètres du fichier d'installation. **Endpoint Detection and Response Agent** Dans cette configuration, seuls les agents intégrés pour les solutions Kaspersky Detection and Response sont disponibles. **Light Agent pour protéger les environnements virtuels** Dans cette configuration, vous pouvez utiliser presque tous les modules d'application disponibles dans la configuration **Mode standard**, à l'exception des modules de chiffrement des données et du Contrôle évolutif des anomalies.
Clé de licence	Dans cette section, vous pouvez activer l'application. Pour activer l'application, vous devez sélectionner une clé de licence. Avant cela, vous devez ajouter la clé au Serveur d'administration. 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.
Applications incompatibles	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.
Paramètres d'installation	**Ajouter le chemin d'accès au fichier avp.com à la variable système %PATH%**. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% pour le confort de l'utilisation de l'interface de la ligne de commande. **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). **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. **Utiliser le mode de compatibilité Azure WVD**. Cette fonctionnalité garantit l'affichage correct de l'état de la machine virtuelle Azure dans la console de Kaspersky Anti Targeted Attack Platform. Pour surveiller les performances de l'ordinateur, Kaspersky Endpoint Security envoie la télémétrie aux serveurs KATA. La télémétrie comprend un identifiant de l'ordinateur (Sensor ID). Le mode de compatibilité Azure WVD permet d'attribuer un Sensor ID unique permanent à ces machines virtuelles. Si le mode de compatibilité est désactivé, l'Sensor ID peut changer après le redémarrage de l'ordinateur en raison du fonctionnement des machines virtuelles Azure. Cela peut entraîner l'apparition de doublons de machines virtuelles sur la console. **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(x86)%\Kaspersky Lab\KES.14.2`. **Fichier de configuration**. Installation de l'application avec les paramètres prédéfinis. Pour ce faire, vous devez charger un 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. L'Assistant de création de paquet ne prend pas en charge les fichiers de configuration chiffrés. Lors de l'exportation du fichier de configuration, ignorez l'étape de chiffrement du fichier.

Mise à jour des bases dans le fichier d'installation

Le fichier d'installation contient les bases antivirus extraites du stockage du Serveur d'administration et qui étaient à jour au moment de la création du fichier d'installation. Une fois le fichier 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 *Téléchargement des mises à jour sur 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 fichier d'installation uniquement dans la Console d'administration de Kaspersky Security Center et dans Kaspersky Security Center Web Console. Il n'est pas possible de mettre à jour les bases dans le fichier d'installation dans l'application Kaspersky Security Center Cloud Console.

Procédure de mise à jour des bases antivirus dans le fichier d'installation via la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.

   La liste des paquets d'installation téléchargés depuis Kaspersky Security Center s'affiche.
3. Ouvrez les propriétés du fichier d'installation.
4. Dans la section **Général**, cliquez sur **Mettre à jour les bases**.

Les bases antivirus du fichier d'installation sont alors mises à jour à partir du stockage du Serveur d'administration. Le fichier `bases.cab` qui figure dans la fichier 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 fichier d'installation via Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

   La liste des paquets d'installation téléchargés depuis Web Console s'affiche.
2. Cliquez sur le nom du fichier d'installation de Kaspersky Endpoint Security dans lequel vous souhaitez mettre à jour les bases antivirus.

   La fenêtre des propriétés du fichier d'installation s'ouvre.
3. Sous l'onglet **Informations générales**, cliquez sur le lien **Mettre à jour les bases**.

Les bases antivirus du fichier d'installation sont alors mises à jour à partir du stockage du Serveur d'administration. Le fichier `bases.cab` qui figure dans la fichier 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 à distance d'une application* prévue. La tâche *Installation à distance d'une application* permet de déployer le paquet d'installation de l'application sur tous les ordinateurs de l'organisation. Avant de déployer le fichier 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. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.
3. Cliquez sur **Nouvelle tâche**.

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

Étape 1. Sélection du type de tâche

Choisissez **Serveur d'administration de Kaspersky Security Center** → **Installation à distance d'une application**.

Étape 2. Sélection du fichier d'installation

Sélectionnez le fichier de Kaspersky Endpoint Security dans la liste des fichiers d'installation. Si le fichier 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 fichiers 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 fichier 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 téléchargement du paquet d'installation**. Sélectionnez le mode d'installation de l'application :

  - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Endpoint Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.

  - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier 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.

  - **En utilisant les ressources du système d'exploitation via le 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 pour les appareils administrés via d'autres Serveurs d'administration**. 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 réinstaller 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 14.2*.

Étape 10. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. 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, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Installation à distance d'une 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 sera affectée**, sélectionnez 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 fichier d'installation

Cette étape permet de configurer le fichier d'installation :

1. Choisissez le fichier d'installation de Kaspersky Endpoint Security for Windows (14.2).

2. Choisissez le fichier 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**, sélectionnez le mode d'installation de l'application :

   - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Endpoint Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Ensuite, Kaspersky Endpoint Security est installé à l'aide de l'Agent d'administration.

   - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier 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.

   - **En utilisant les ressources du système d'exploitation via le 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 maximal de téléchargements simultanés**, définissez la limite du nombre de requêtes adressées au Serveur d'administration pour le téléchargement du fichier d'installation. La restriction des demandes permet d'éviter la surcharge du réseau.

5. Dans le champ **Nombre maximal de tentatives d'installation**, définissez 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 réinstaller 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 le type de système d'exploitation avant le téléchargement**. 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 **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'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 **Demander aux utilisateurs de fermer 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 pour les appareils administrés via d'autres Serveurs d'administration**, 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. Assurez-vous que le compte utilisateur à partir duquel vous exécutez l'Assistant d'installation fait partie du groupe administrateurs.

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_kes.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 :

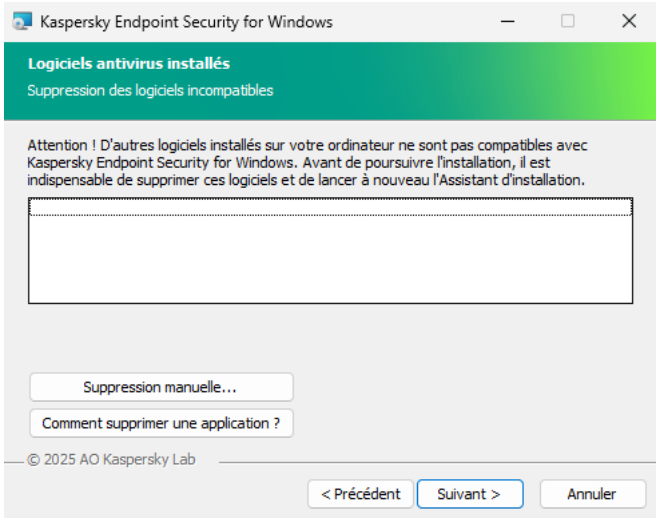
- Vérifiez s'il existe des logiciels installés susceptibles de présenter des problèmes de compatibilité avec Kaspersky Endpoint Security (la liste de ces logiciels est disponible dans le fichier incompatible.txt inclus dans le kit de distribution).

- Respect des configurations logicielle et matérielle ;

- La présence de Microsoft .NET Framework.

- Présences des privilèges pour l'installation du logiciel.

Si une des conditions énumérées n'est pas remplie, un message apparaît. Par exemple, une notification concernant un logiciel incompatible (voir la figure ci-dessous).



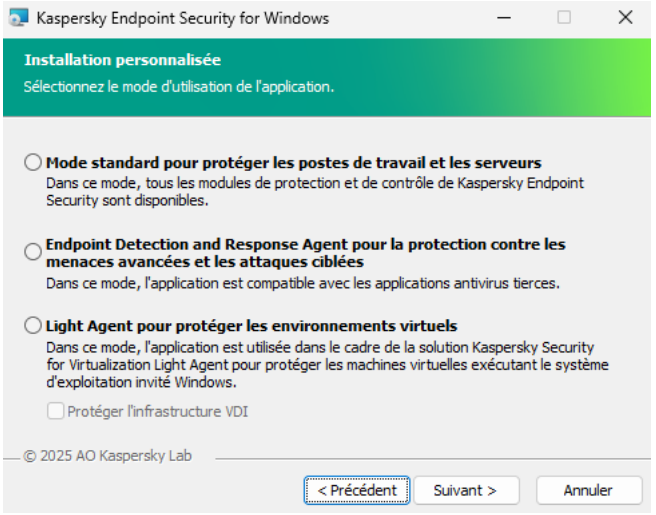
Suppression des logiciels incompatibles

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 14.2 for Windows, et la version précédente de l'application est supprimée automatiquement. Cela se concerne les versions suivantes de l'application :

- Kaspersky Endpoint Security 12.3 for Windows (version 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (version 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (version 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (version 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (version 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (version 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (version 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (version 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (version 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (version 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (version 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (version 14.1.0.423)

Configuration de Kaspersky Endpoint Security



Choix de la configuration de l'application

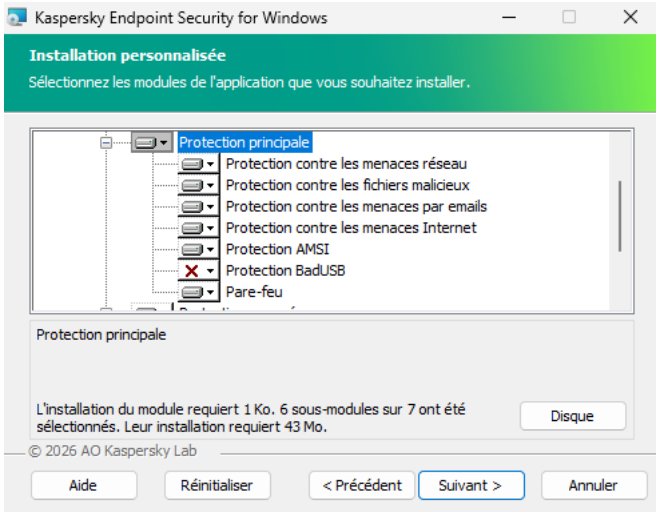
Mode standard. La configuration par défaut. Cette configuration vous permet d'utiliser tous les modules de l'application, y compris les modules qui prennent en charge les solutions Detection and Response. Cette configuration est utilisée pour assurer une protection complète de l'ordinateur contre diverses menaces, attaques réseau et fraudes.

Endpoint Detection and Response Agent. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

Light Agent pour protéger les environnements virtuels. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Modules de Kaspersky Endpoint Security

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



Sélection des modules de l'application à installer

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

- Kaspersky Disk Encryption
- Chiffrement des fichiers
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Intégration avec KUMA

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.

Si vous devez installer des modules Detection and Response, Kaspersky Endpoint Security prend en charge les configurations suivantes :

- Endpoint Detection and Response Optimum seulement
- Endpoint Detection and Response Expert (cloud) seulement
- Endpoint Detection and Response Expert (on-premises) seulement
- Network Detection and Response (KATA) seulement

- Sandbox seulement
- Endpoint Detection and Response Optimum et Sandbox
- Endpoint Detection and Response Expert (cloud) et Sandbox
- Endpoint Detection and Response Expert (on-premises) et Sandbox
- Network Detection and Response (KATA) et Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) et Managed Detection and Response

Kaspersky Endpoint Security vérifie la sélection des modules avant d'installer l'application. Si la configuration sélectionnée des modules Detection and Response n'est pas prise en charge, Kaspersky Endpoint Security ne peut pas être installé.

Sélection du 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(x86)%\Kaspersky Lab\KES.14.2`.

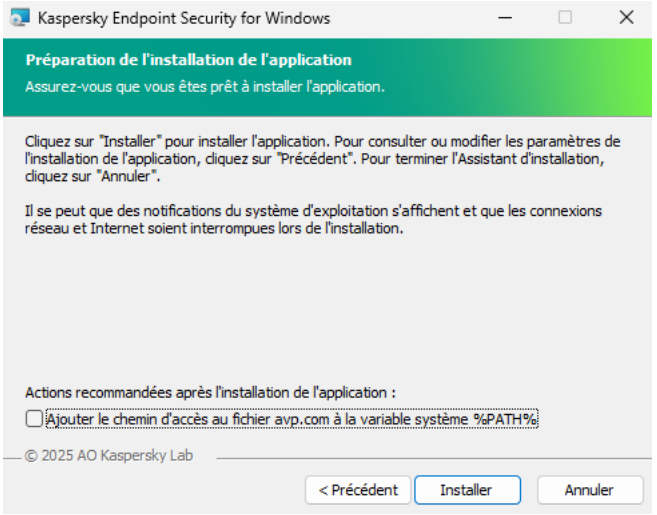
Configuration de la zone de confiance

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware.

Vous pouvez également configurer la zone de confiance plus tard dans les propriétés de la stratégie : exclusions d'analyse et applications de confiance.

Paramètres avancés



Paramètres d'installation avancés de l'application

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 d'accès au fichier avp.com à la variable système %PATH%. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% pour le confort de l'utilisation de l'interface de la ligne de commande.

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 **Gestion des applications** choisissez la section **Paquets**.

3. Dans la partie supérieure de la console, dans le panne d'administration, cliquez sur le bouton **Création du 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 fichier d'installation.
      - Dans le champ **Dossier source**, 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 **Programme standard**.

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

      - Saisissez dans le champ **Nom** le nom unique du fichier 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 **Exécuter avec les droits d'administration** dans la liste **Mode d'exécution**.

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

      - Cochez la case **Exécuter un autre programme en premier** 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 **Ce programme ne peut s'exécuter que sur des plateformes spécifiées** dans le groupe **Exigences de plateformes** 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 fichier d'installation créé apparaîtra dans la section **Paquets** dans la liste des paquets d'installation disponibles.

5. Dans le menu contextuel du fichier 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 fichier d'installation ou choisissez le fichier 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.

Utilisez le fichier setup.ini uniquement lorsque vous installez l'application en mode silencieux.

Vous ne pouvez pas ajouter de chemin au fichier de configuration install.cfg dans le fichier setup.ini. L'application ignore également le fichier de configuration install.cfg s'il se trouve dans le même dossier que le kit de distribution de Kaspersky Endpoint Security. Pour appliquer les paramètres du fichier de configuration install.cfg, vous devez indiquer le chemin d'accès au fichier dans la commande suivante d'installation de l'application : `CONFIGPATH=<path to the configuration file>`.

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 en mode standard. 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.
- `[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.

Les valeurs `yes`, `on`, `enable`, `enabled` et `true` peuvent être utilisées à la place de la valeur `1`. Les valeurs `no`, `off`, `disable`, `disabled` et `false` peuvent être utilisées à la place de la valeur `0`.

Paramètres du fichier setup.ini

Section	Paramètre	Description
`[Setup]`	`InstallDir`	Chemin d'accès au dossier d'installation de l'application.
	`ActivationCode`	Code d'activation de Kaspersky Endpoint Security.
	`Eula`	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`	Acceptation de la Politique de confidentialité. Le texte de la Politique de confidentialité fait partie du kit de distribution de Kaspersky Endpoint Security. L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.
	`KSN`	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 : • `1` : acceptation de la participation à KSN. • `0` : refus de la participation à KSN (valeur par défaut). 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.
	`CLEANERSIGNCHECK`	Vérification des signatures numériques des fichiers de logiciels détectés dans la liste incompatible.txt. Pour supprimer le logiciel, Kaspersky Endpoint Security exécute le fichier d'installation du logiciel. Si le fichier d'installation ne possède pas de signature numérique, Kaspersky Endpoint Security considère que le fichier n'est pas fiable et interrompt la suppression du logiciel pour éviter l'exécution d'un code potentiellement malveillant. Si l'application ne peut pas vérifier la signature numérique du fichier logiciel détecté, l'installation de Kaspersky Endpoint Security est arrêtée avec une erreur. La valeur par défaut est différente selon la méthode d'installation du logiciel : • `0` signifie que la vérification de la signature numérique est désactivée (valeur par défaut en cas de déploiement via Kaspersky Security Center). • `1` signifie que la vérification de la signature numérique est activée (valeur par défaut si l'application est installée localement).
	`Login`	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.

Section	Paramètre	Description
	`Password`	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`). 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.
	`PasswordArea`	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 `Login` et `Password`). Pour indiquer plusieurs valeurs, utilisez le caractère `;`. Valeurs possibles : • `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. • `EXPORT` – exportation des paramètres de l'application Par exemple, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Activation ou désactivation du mécanisme de protection de l'installation de l'application. Valeurs possibles : • `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. 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).
	`PROTECTOSSERVICES`	Protection des fonctionnalités des services du système d'exploitation. La protection des services du système d'exploitation empêche les applications tierces d'interférer avec le fonctionnement des services du système d'exploitation. Ces services incluent par exemple le service de lancement automatique de l'application. • `1` signifie que la protection des services du système d'exploitation est activée (valeur par défaut). • `0` signifie que la protection des services du système d'exploitation est désactivée.
	`EnableAzureSupport`	Activation ou désactivation du mode de compatibilité Azure WVD. Valeurs possibles : • `1` – Le mode de compatibilité Azure WVD est activé. • `0` – Le mode de compatibilité Azure WVD est désactivé (valeur par défaut). Cette fonctionnalité garantit l'affichage correct de l'état de la machine virtuelle Azure dans la console de Kaspersky Anti Targeted Attack Platform. Pour surveiller les performances de l'ordinateur, Kaspersky Endpoint Security envoie la télémétrie aux serveurs KATA. La télémétrie comprend un identifiant de l'ordinateur (Sensor ID). Le mode de compatibilité Azure WVD permet d'attribuer un Sensor ID unique permanent à ces machines virtuelles. Si le mode de compatibilité est désactivé, l'Sensor ID peut changer après le redémarrage de l'ordinateur en raison du fonctionnement des machines virtuelles Azure. Cela peut entraîner l'apparition de doublons de machines virtuelles sur la console.
	`Reboot`	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. 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.
	`AddEnvironment`	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 : • `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%.

Section	Paramètre	Description
	AMPPL	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. La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019. Valeurs possibles : • 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.
	UPGRADEMODE	Mode de mise à jour de l'application : • Seamless signifie mettre à jour l'application avec un redémarrage de l'ordinateur (valeur par défaut). • Force signifie mettre à jour l'application sans redémarrage. Vous pouvez mettre à jour l'application sans redémarrage à partir de la version 11.10.0. Pour mettre à jour une version antérieure de l'application, vous devez redémarrer l'ordinateur. Vous pouvez aussi installer les correctifs sans redémarrage à partir de la version 11.11.0. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Ainsi, le mode de mise à jour de l'application sera précisé dans les paramètres de l'application. Vous pouvez modifier ce paramètre dans les paramètres de l'application ou dans la stratégie. Lors de la mise à jour d'une application déjà installée, la priorité du paramètre précisé dans le fichier setup.ini est supérieure à celle du paramètre précisé dans les paramètres de l'application ou dans la ligne de commande. Par exemple, si le mode de mise à jour Force est spécifié dans le fichier setup.ini et que le mode Seamless est précisé dans les paramètres de l'application, la mise à jour sera installée sans redémarrage (Force). Si vous utilisez le fichier setup.ini, où le paramètre UPGRADEMODE n'est pas précisé, le programme d'installation utilisera une valeur par défaut (Seamless) et installera la mise à jour avec un redémarrage de l'ordinateur.
	SetupReg	Activation de l'enregistrement des clés du registre du fichier setup.reg dans le registre. La valeur du paramètre SetupReg: setup.reg.
	EnableTraces	Activation ou désactivation du traçage de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier %ProgramData%\Kaspersky Lab\KES.14.2\Traces après le lancement. Valeurs possibles : • 1 : le traçage est activé. • 0 : le traçage est désactivé (valeur par défaut).
	TracesLevel	Niveau de détail du traçage Valeurs possibles : • 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	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). Valeurs possibles : • 1 : l'administration via l'API REST est autorisée. • 0 : l'administration via l'API REST est interdite (valeur par défaut). 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 administrer l'application via l'API REST, il est impossible de l'administrer via les systèmes d'administration de Kaspersky.
	RESTAPI_User	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. L'ajout d'un nom d'utilisateur est une condition indispensable à l'administration de l'application via l'API REST.
	RESTAPI_Port	Port destiné à l'administration de l'application via l'API REST. Le port 6782 est utilisé par défaut. Assurez-vous que le port est disponible.

Section	Paramètre	Description
	`RESTAPI_Certificate`	Certificat pour l'identification des demandes (par exemple, `RESTAPI_Certificate=C:\cert.pem`). L'interaction sécurisée de Kaspersky Endpoint Security avec le client REST nécessite la configuration de l'identification des requêtes. Pour ce faire, vous devez installer un certificat et signer ensuite la charge utile de chaque demande.
	`StandaloneMode`	Installation de l'application en mode Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* est une application installée sur des postes de travail et des serveurs individuels dans l'infrastructure informatique de l'organisation pour prendre en charge les solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform. EDR Agent est compatible avec les applications PPE tierces. Vous pouvez ainsi utiliser des outils de sécurité d'infrastructure tiers ainsi que la solution Detection and Response de Kaspersky. Pour installer EDR Agent, dans la section `[Components]`, sélectionnez les modules `StandaloneKATA`, `StandaloneNDR` ou `StandaloneMDR`. EDR Agent ne prend pas en charge les autres modules d'application. Valeurs possibles : • `1` pour installer l'application en mode EDR Agent. • `0` pour installer l'application en mode Standard (par défaut).
	`KSVLAMode`	Installation de l'application en mode Light Agent. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Valeurs possibles : • `1` pour installer l'application en mode Light Agent. • `0` pour installer l'application en mode Standard (par défaut).
	`InstallOnVDI`	Activation du mode de protection VDI lors de l'installation de l'application en mode Light Agent (`KSVLAMode=1`). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées. Valeurs possibles : • `1` pour activer le mode de protection VDI. • `0` pour désactiver le mode de protection VDI (par défaut).
	`KESExclusions`	Ajout d'exclusions d'analyse et d'applications de confiance prédéfinies lors de l'installation de l'application sur le serveur. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Par exemple, les exclusions de l'analyse prédéfinies pour les serveurs SQL incluent les fichiers de bases de données MDF et LDF. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. Valeurs possibles : • `1` active les exclusions de l'analyse et d'applications de confiance prédéfinies. • `0` désactive les exclusions de l'analyse et d'applications de confiance prédéfinies (par défaut).
	`LAExclusions`	Ajout d'exclusions d'analyse et d'applications de confiance prédéfinies lors de l'installation de l'application sur une machine virtuelle (mode Light Agent). Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware. Valeurs possibles : • `1` active les exclusions de l'analyse et d'applications de confiance prédéfinies. • `0` désactive les exclusions de l'analyse et d'applications de confiance prédéfinies (par défaut).

Section	Paramètre	Description
	`EnableUniqueSensorID`	Création d'un identifiant unique d'ordinateur (Sensor ID) lors de l'installation ou de la mise à jour de l'application. Le Sensor ID est utilisé dans la solution Kaspersky Anti Targeted Attack Platform pour identifier les ordinateurs qui envoient des données télémétriques au serveur. Lors de la création du Sensor ID, l'application utilise un algorithme qui prend en compte la configuration de l'ordinateur, comme le numéro de série de la carte mère. Dans certains cas, par exemple lors de l'utilisation de l'application dans un environnement virtuel, le Sensor ID peut être dupliqué. Par conséquent, Kaspersky Anti Targeted Attack Platform ne peut pas identifier l'ordinateur à partir duquel les données télémétriques sont envoyées. Pour créer un Sensor ID unique, vous devez définir le paramètre `EnableUniqueSensorID=1`. Par conséquent, l'application créera le Sensor ID à l'aide d'un algorithme différent, qui prend en compte les autres données relatives à l'ordinateur. Cela permet d'obtenir un Sensor ID unique. Par défaut, le paramètre n'est pas défini. L'application hérite du Sensor ID dans les cas suivants : • mise à jour de la version de l'application ; • migration de la configuration [KES+KEA] vers la configuration [KES+agent intégré]. Dans le cadre de la réparation de l'application, le programme d'installation tente d'hériter Sensor ID. Si le Sensor ID ne peut pas être restauré, l'application crée un nouveau Sensor ID.
	`CitrixCompatibility`	Activation de la prise en charge de Citrix Provisioning Services pour l'installation de Kaspersky Endpoint Security sur une machine virtuelle.
`[Components]`	`ALL`	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. En raison du mode de prise en charge des solutions Detection and Response, les modules Endpoint Detection and Response Optimum et Sandbox sont installés sur l'ordinateur. Le module Endpoint Detection and Response Expert (cloud) n'est pas compatible avec cette configuration.
	`MailThreatProtection`	Protection contre les menaces par emails.
	`WebThreatProtection`	Protection contre les menaces Internet.
	`AMSI`	Protection AMSI.
	`HostIntrusionPrevention`	Prévention des intrusions.
	`BehaviorDetection`	Détection comportementale.
	`ExploitPrevention`	Protection contre les Exploits.
	`RemediationEngine`	Réparation des actions malicieuses.
	`Firewall`	Pare-feu.
	`NetworkThreatProtection`	Protection contre les menaces réseau.
	`WebControl`	Contrôle Internet.
	`DeviceControl`	Contrôle des appareils.
	`ApplicationControl`	Contrôle des applications.
	`AdaptiveAnomaliesControl`	Contrôle évolutif des anomalies.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Inspection des journaux
	`AntiCryptor`	Protection contre le chiffrement
	`FileThreatProtection`	Protection contre les fichiers malicieux.
	`SystemIntegrityMonitor`	Contrôle de l'intégrité du système.
	`FileEncryption`	Bibliothèques pour le chiffrement des fichiers.
	`DiskEncryption`	Bibliothèques pour le chiffrement du disque.
	`MSBitLocker`	Bibliothèques d'administration du chiffrement BitLocker.
	`BadUSBAttackPrevention`	Protection BadUSB.

Section	Paramètre	Description
	`EDR`	Endpoint Detection and Response Optimum Le module n'est pas compatible avec les modules Endpoint Detection and Response Expert (cloud) (`EDRCloud`) et Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Le module n'est pas compatible avec les modules Endpoint Detection and Response Optimum (`EDR`) et Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Le module n'est pas compatible avec les modules Endpoint Detection and Response Expert (cloud) (`EDRCloud`) et Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox ou KATA Sandbox. *Kaspersky Sandbox* est une solution autonome de détection et de réponse de Kaspersky. *KATA Sandbox* est un module de la solution Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Le module n'est pas compatible avec les modules Endpoint Detection and Response Expert (cloud) (`EDRCloud`) et Endpoint Detection and Response Optimum (`EDR`).
	`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 : • `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.
	`KUMAIntegration`	Intégration avec KUMA.
	`StandaloneKATA`	Installation de l'application en mode Endpoint Detection and Response Agent (EDR Agent) pour l'intégration avec Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Installation de l'application en mode Endpoint Detection and Response Agent (EDR Agent) pour l'intégration avec Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Installation de l'application en mode Endpoint Detection and Response Agent (EDR Agent) pour l'intégration avec Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Installation de l'application en mode Endpoint Detection and Response Agent (EDR Agent) pour l'intégration avec KUMA.
`[Tasks]`	`ScanMyComputer`	Tâche d'analyse complète. Valeurs possibles : • `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 : • `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 : • `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.

Processus de Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows lance les processus décrits dans le tableau ci-dessous.

Processus de Kaspersky Endpoint Security for Windows

Nom du fichier	Fonction
avp.exe	Processus de travail de Kaspersky Endpoint Security for Windows.
avpsus.exe	Ce processus permet d'installer et annuler les mises à jour critiques et approuvées des modules d'application.

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.

  > Ce mode n'est pas disponible si l'installation a été effectuée via Kaspersky Security Center. Vous pouvez modifier la sélection de modules d'application dans le Panneau de configuration uniquement après l'installation de l'application en local.

- 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.

- Si l'application est installée en mode Light Agent dans une infrastructure VDI, la modification des modules définis n'est pas prise en charge.

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

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.
2. Cliquez sur **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 (14.2)** → **Sélectionnez les modules à installer**.

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

Sélectionnez la configuration de l'application

- **Mode standard pour protéger les hôtes**. La configuration par défaut. Cette configuration vous permet d'utiliser tous les modules de l'application, y compris les modules qui prennent en charge les solutions Detection and Response. Cette configuration est utilisée pour assurer une protection complète de l'ordinateur contre diverses menaces, attaques réseau et fraudes.
- **Endpoint Detection and Response Agent pour la protection contre les menaces avancées et les attaques ciblées**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

  Lorsque vous modifiez la configuration de l'application pour qu'EDR Agent fonctionne avec MDR, assurez-vous que les modules chargés de recevoir la télémétrie sont activés.

- **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

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

Étape 3. Paramètres avancés

Configurez les paramètres avancés de la tâche (cf. tableau ci-après).

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. 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 6. Définition du nom de la tâche

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

Étape 7. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Dans la liste déroulante **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 **Appareils auxquels la tâche sera affectée**, sélectionnez 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 les détails de la tâche à la fin de la création** et quittez l'Assistant.

Dans les propriétés des tâches, sélectionnez l'onglet **Paramètres de l'application**. Sélectionnez ensuite la configuration de l'application :

- **Mode standard pour protéger les postes de travail et les serveurs**. La configuration par défaut. Cette configuration vous permet d'utiliser tous les modules de l'application, y compris les modules qui prennent en charge les solutions Detection and Response. Cette configuration est utilisée pour assurer une protection complète de l'ordinateur contre diverses menaces, attaques réseau et fraudes.

- **Endpoint Detection and Response Agent pour la protection contre les menaces avancées et les attaques ciblées**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

  Lorsque vous modifiez la configuration de l'application pour qu'EDR Agent fonctionne avec MDR, assurez-vous que les modules chargés de recevoir la télémétrie sont activés.

- **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Choisissez les modules de l'application qui seront accessibles sur l'ordinateur. Configurez les paramètres avancés de la tâche (cf. tableau ci-après).

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.

Lors de l'installation, de la mise à jour ou de la désinstallation de Kaspersky Endpoint Security, des erreurs peuvent survenir. Pour en savoir plus sur la résolution de ces erreurs, consultez la Base de connaissances du support technique.

Paramètre	Description
Paramètres de la tâche	**Vérifier la présence d'applications incompatibles d'éditeurs tiers**. Par défaut, Kaspersky Endpoint Security vérifie la compatibilité des applications installées. La liste des logiciels susceptibles de poser des problèmes de compatibilité figure dans le fichier incompatible.txt. Le fichier est inclus dans le kit de distribution. Si l'analyse des applications installées est activée, lorsqu'une application de la liste est détectée, Kaspersky Endpoint Security arrête la tâche. Vous pouvez désactiver l'analyse des logiciels installés si la documentation du fournisseur du logiciel tiers revendique la compatibilité avec Endpoint Protection Platform (PPE). **Supprimer les applications incompatibles d'éditeurs tiers**. Suppression automatique des applications mentionnées dans le fichier incompatible.txt avant la modification l'ensemble des modules. Si cette fonctionnalité est activée, Kaspersky Endpoint Security tente de supprimer les applications qui peuvent entraîner des problèmes de compatibilité afin de poursuivre la tâche. **Utiliser le mode de compatibilité Azure WVD**. Cette fonctionnalité garantit l'affichage correct de l'état de la machine virtuelle Azure dans la console de Kaspersky Anti Targeted Attack Platform. Pour surveiller les performances de l'ordinateur, Kaspersky Endpoint Security envoie la télémétrie aux serveurs KATA. La télémétrie comprend un identifiant de l'ordinateur (Sensor ID). Le mode de compatibilité Azure WVD permet d'attribuer un Sensor ID unique permanent à ces machines virtuelles. Si le mode de compatibilité est désactivé, l'Sensor ID peut changer après le redémarrage de l'ordinateur en raison du fonctionnement des machines virtuelles Azure. Cela peut entraîner l'apparition de doublons de machines virtuelles sur la console.
Exclusions	À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware. Vous pouvez également configurer la zone de confiance plus tard dans les propriétés de la stratégie : exclusions d'analyse et applications de confiance.
Mode séparé/Mode combiné	Vous pouvez créer des ensembles de modules distincts pour les postes de travail et les serveurs : **Mode séparé**. Avant de déployer le paquet d'installation, le programme d'installation détecte le type du système d'exploitation et installe uniquement les modules d'application que vous avez sélectionnés pour ce type de système d'exploitation. De cette façon, vous pouvez utiliser le même paquet d'installation pour les postes de travail et les serveurs. **Mode combiné** propose une liste commune de modules pour les postes de travail et les serveurs. La disponibilité de chaque module dépend du type de système d'exploitation. Dans ce mode, il est conseillé de créer un paquet d'installation distinct pour les postes de travail et un paquet d'installation distinct pour les serveurs. Vous pouvez configurer la liste commune des modules dans le paquet d'installation uniquement en mode standard.
Utiliser le mot de passe pour modifier la sélection de modules de l'application	Les administrateurs activent généralement la protection par mot de passe pour restreindre l'accès à Kaspersky Endpoint Security. Autrement dit, pour modifier la sélection des modules de l'application, vous devez entrer les identifiants d'un utilisateur disposant de l'autorisation **Supprimer/Modifier/Réparer l'application**. Par exemple, vous pouvez utiliser le compte KLAdmin.
Utiliser le mot de passe pour désinstaller Kaspersky Endpoint Agent et Kaspersky Security for Windows Server	Les administrateurs activent généralement la protection par mot de passe dans les paramètres de ces tâches pour restreindre l'accès à Kaspersky Endpoint Agent (KEA) et Kaspersky Security for Windows Server (KSWS). Autrement dit, si vous migrez de la configuration [KES+KEA] vers [KES+agent intégré], ou si vous migrez de KSWS vers KES, vous devez saisir un mot de passe pour supprimer ces applications.

Mise à jour à partir de la version précédente de l'application

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

- Avant de commencer la mise à jour de l'application, il est conseillé de fermer toutes les applications en cours d'exécution.
- Avant la mise à jour, 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.
- Pour modifier la langue de l'application, dans la tâche *Installation à distance d'une application*, sélectionnez le paquet d'installation correspondant à la localisation souhaitée et mettez à jour l'application. La possibilité de modifier la langue de l'application est disponible depuis Kaspersky Endpoint Security for Windows 14.2.

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

- Kaspersky Endpoint Security 12.3 for Windows (version 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (version 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (version 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (version 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (version 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (version 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (version 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (version 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (version 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (version 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (version 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (version 14.1.0.423)

Lors de l'installation, de la mise à jour ou de la désinstallation de Kaspersky Endpoint Security, des erreurs peuvent survenir. Pour en savoir plus sur la résolution de ces erreurs, consultez la Base de connaissances du support technique.

Méthodes de mise à jour des applications

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

- À l'aide du service de mise à jour de Kaspersky (Seamless Update – SMU).
- localement à l'aide de l'Assistant d'installation de l'application.
- localement via la ligne de commande.
- À distance via 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).
- à distance à l'aide de System Center Configuration Manager.

Si l'application déployée sur le réseau de l'organisation comporte un ensemble de modules différent de l'ensemble par défaut, sa mise à jour via la Console d'administration (MMC) diffère de sa mise à jour via Web Console. La mise à jour de Kaspersky Endpoint Security possède les particularités suivantes :

- Kaspersky Security Center Web Console.

  Si vous avez créé un fichier 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 fichier 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 fichier d'installation. Autrement dit, si la nouvelle version de l'application utilise l'ensemble de modules par défaut, l'agent MDR intégré, par exemple, 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 fichier d'installation.

Mise à jour de l'application sans redémarrage

La mise à jour de l'application sans redémarrage assure un fonctionnement ininterrompu du serveur lorsque la version de l'application est mise à jour.

La mise à jour de l'application sans redémarrage présente les limitations suivantes :

- Vous pouvez mettre à jour l'application sans redémarrage à partir de la version 11.10.0. Pour mettre à jour une version antérieure de l'application, vous devez redémarrer l'ordinateur.
- Vous pouvez installer les correctifs sans redémarrage à partir de la version 11.11.0. Pour installer des correctifs pour les versions antérieures de l'application, un redémarrage de l'ordinateur peut être nécessaire.

- La mise à jour de l'application sans redémarrage n'est pas disponible sur les ordinateurs dont le chiffrement des données est activé (chiffrement Kaspersky (FDE), BitLocker, Chiffrement des fichiers (FLE)). Pour mettre à jour l'application sur les ordinateurs dont le chiffrement des données est activé, l'ordinateur doit être redémarré.

- L'application ne peut pas être mise à jour sur la machine virtuelle sans redémarrage. Pour mettre à jour l'application sur une machine virtuelle, vous devez redémarrer la machine virtuelle.

Après la mise à jour de l'application, l'installation d'un correctif, la modification de l'ensemble des modules de l'application ou la restauration, Kaspersky Endpoint Security redémarre et commence à utiliser la nouvelle version. Le redémarrage de Kaspersky Endpoint Security peut durer jusqu'à une minute. Pendant cette période, le niveau de la protection de l'ordinateur est réduit. Après le redémarrage de l'application, le niveau de protection de l'ordinateur sera rétabli.

Comment sélectionner le mode de mise à jour des applications dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.

5. Dans le groupe **Paramètres avancés**, cochez ou décochez la case **Installer les mises à jour de l'application sans redémarrer l'ordinateur** pour configurer le mode de mise à jour des applications.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner le mode de mise à jour des applications dans Web Console ?

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.

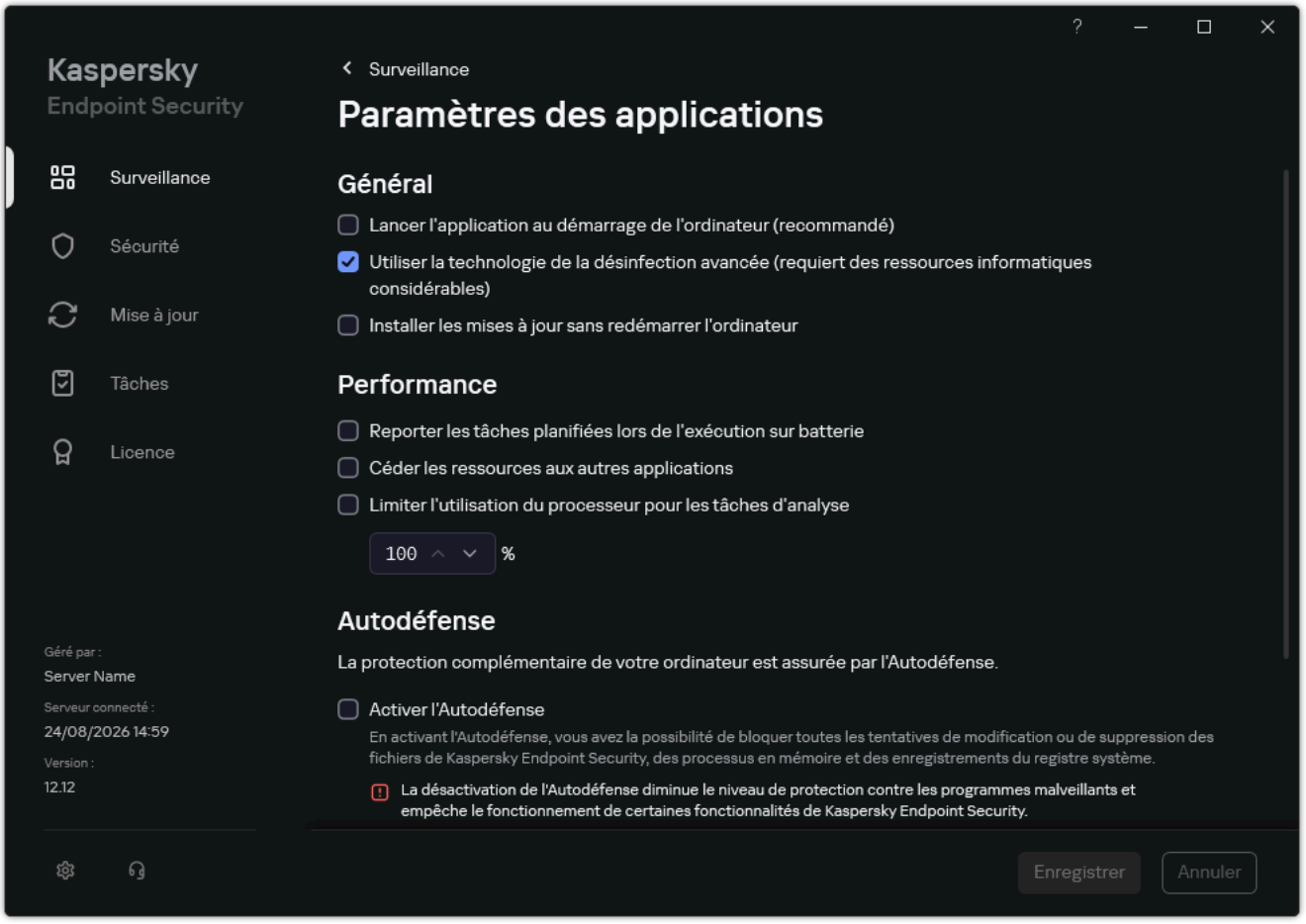
5. Dans le groupe **Paramètres de mise à jour de l'application**, cochez ou décochez la case **Installer les mises à jour de l'application sans redémarrer l'ordinateur** pour configurer le mode de mise à jour des applications.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner le mode de mise à jour des applications 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. Dans le groupe **Général**, cochez ou décochez la case **Installer les mises à jour sans redémarrer l'ordinateur** pour configurer le mode de mise à jour des applications.

4. Enregistrez vos modifications.

Vous pouvez également sélectionner le mode de mise à jour de l'application lorsque vous installez l'application depuis la ligne de commande (à l'aide de l'option `UPGRADEMODE`).

Une fois que la procédure de mise à jour de l'application sans redémarrage est terminée, la nouvelle version de Kaspersky Endpoint Security est installée sur l'ordinateur. La version précédente de l'application est supprimée automatiquement.

Vous ne pouvez pas lancer la mise à jour de l'application avant la fin de la mise à jour précédente.

Vous pouvez vérifier l'état de la mise à jour de Kaspersky Endpoint Security à l'aide du rapport sur la version de l'application Kaspersky dans la console Kaspersky Security Center.

Mise à jour SMU de l'application

Pour mettre à jour l'application à l'aide du service de mise à jour de Kaspersky (Seamless Update ; SMU), il n'est pas nécessaire de lancer le programme d'installation, contrairement aux autres méthodes de mise à jour. Kaspersky Endpoint Security obtient la nouvelle version de l'application avec les bases antivirus provenant de la même source.

Une mise à jour SMU permet de mettre à jour l'application sur tous les ordinateurs de votre organisation vers la version la plus récente. Avant d'appliquer une mise à jour SMU, nous recommandons de tester la nouvelle version de l'application sur quelques ordinateurs. Pour ce faire, il faut mettre à jour manuellement l'application sur ces ordinateurs (par exemple, localement à l'aide de l'Assistant d'installation). Vous ne pouvez pas sélectionner des ordinateurs individuellement lorsque vous effectuez une mise à jour SMU.

La planification des mises à jour de l'application est déterminée par l'équipe de Kaspersky. Pour s'assurer du bon fonctionnement de la nouvelle version de l'application, Kaspersky diffuse des mises à jour disponibles étape par étape. Cela signifie que votre mise à jour SMU pourrait être disponible jusqu'à deux mois après la publication d'une nouvelle version.

Vous pouvez gérer la mise à jour SMU de l'application à l'aide de la tâche *Mise à jour des bases et des modules d'application*. Pour que la nouvelle version de l'application soit incluse dans le même paquet que les bases antivirus, vous devez autoriser la mise à jour des *modules d'application* dans les paramètres de la tâche *Mise à jour des bases et des modules d'application*. La tâche *Mise à jour des bases et des modules d'application* vous permet également d'autoriser la mise à jour de l'application sans redémarrage.

Étapes d'une mise à jour SMU de l'application

1. **Après la publication d'une nouvelle version de l'application, Kaspersky diffuse la mise à jour.**

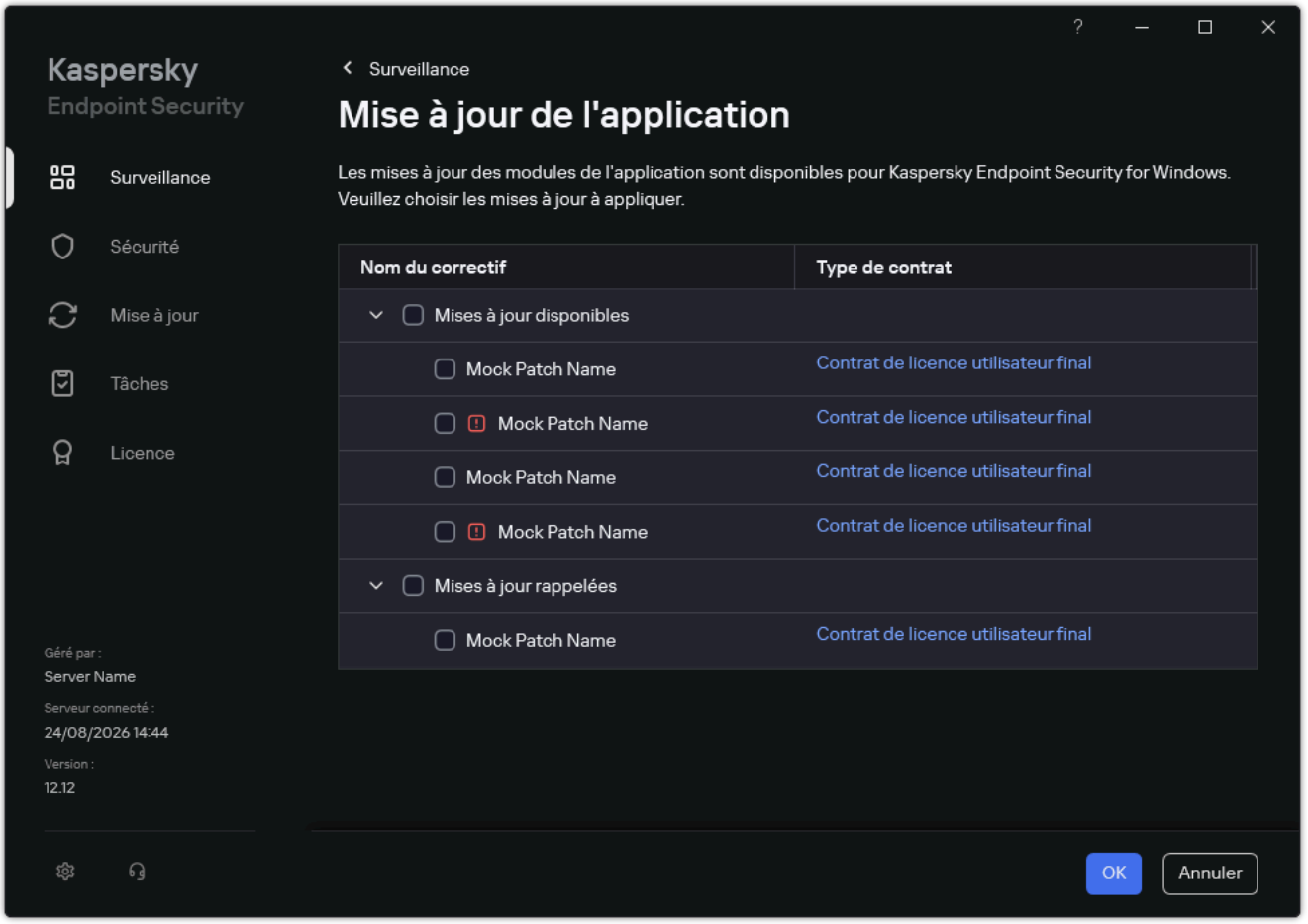
2. **L'utilisateur approuve la mise à jour de l'application.**

   Si l'ordinateur est connecté à Kaspersky Security Center, la mise à jour est mise à disposition dans Kaspersky Security Center, dans la section **Mise à jour des bases de données et des modules d'application de Kaspersky**. Pour plus de détails sur l'approbation des mises à jour, consultez l'aide de Kaspersky Security Center.

   Si l'ordinateur n'est pas connecté à Kaspersky Security Center, la mise à jour est mise à disposition dans la section des notifications de l'interface de l'application : . Pour approuver la mise à jour, sélectionnez une version de l'application et acceptez les conditions générales des accords (cf. ill. ci-dessous).

3. **Kaspersky Endpoint Security exécute la tâche *Mise à jour des bases et des modules d'application* selon la planification configurée.**

Kaspersky Endpoint Security met alors l'application à jour en mode « silencieux ».



Mises à jour des applications disponibles

Suppression de l'application

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

Lors de l'installation, de la mise à jour ou de la désinstallation de Kaspersky Endpoint Security, des erreurs peuvent survenir. Pour en savoir plus sur la résolution de ces erreurs, consultez la Base de connaissances du support technique.

Suppression de l'application à distance à l'aide de Kaspersky Security Center

Vous pouvez supprimer une application à distance à l'aide de la tâche *Désinstallation à distance d'une 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. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.
3. Cliquez sur **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** → **Désinstallation à distance d'une application**.

Étape 2. Sélection de l'application à supprimer

Choisissez le **Supprimer une application compatible avec Kaspersky Security Center**.

Étape 3. Paramètres de suppression de l'application

Choisissez **Kaspersky Endpoint Security for Windows (14.2)**.

Étape 4. Paramètres de l'utilitaire de désinstallation

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le téléchargement de l'utilitaire de désinstallation**. Sélectionnez les modes de livraison des utilitaires :
  - **En &utilisant 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.
  - **En utilisant les ressources du système d'exploitation via le 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.
  - **En utilisant les ressources du système d'exploitation via les 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 le type de système d'exploitation avant le téléchargement**. 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 un mot de passe de désinstallation**.
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 14.2*.

Étape 10. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

L'application est supprimée en mode silencieux.

Procédure de suppression de l'application via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Désinstallation à distance d'une 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 **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Désinstaller une application administrée**.

2. Sélectionnez **Kaspersky Endpoint Security for Windows**.

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

   - **En utilisant 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.

   - **En utilisant les ressources du système d'exploitation via le 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.

   - **En utilisant les ressources du système d'exploitation via les 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 maximal 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. Dans le champ **Nombre maximal de tentatives de désinstallation**, définissez 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 le type de système d'exploitation avant le téléchargement**. 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 *Désinstallation à distance d'une application*. Sans mot de passe, la tâche ne pourra pas être exécutée.

Pour utiliser le mot de passe du compte KLAdmin dans la tâche Désinstallation à distance d'une application, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Désinstallation à distance d'une application** pour Kaspersky Security Center.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Cochez la case **Utiliser un mot de passe de désinstallation**.

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

6. Enregistrez vos modifications.

Redémarrez l'ordinateur pour terminer la désinstallation. Pour ce faire, l'Agent d'administration affiche une fenêtre contextuelle.

Suppression de l'application à distance à l'aide d'Active Directory

Vous pouvez désinstaller l'application à distance à l'aide d'une stratégie de groupe Microsoft Windows. Pour désinstaller l'application, vous devez ouvrir la Console d'administration de la stratégie de groupe (gpmc.msc) et utiliser l'éditeur de stratégie de groupe pour créer une tâche de suppression de l'application (pour en savoir plus, veuillez consulter le site du Support Technique de Microsoft).

Si l'opération de suppression de l'application est protégée par un mot de passe, vous devez procéder comme suit :

1. Créez un fichier BAT avec le contenu suivant:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   où `<GUID>` représente l'identifiant unique de l'application. Vous pouvez trouver le GUID de l'application dans la base de connaissances du support technique ou en utilisant la commande suivante :

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

   Exemple

   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Créez une nouvelle stratégie Microsoft Windows pour les ordinateurs dans la Console d'administration de la stratégie du groupe (gpmc.msc).

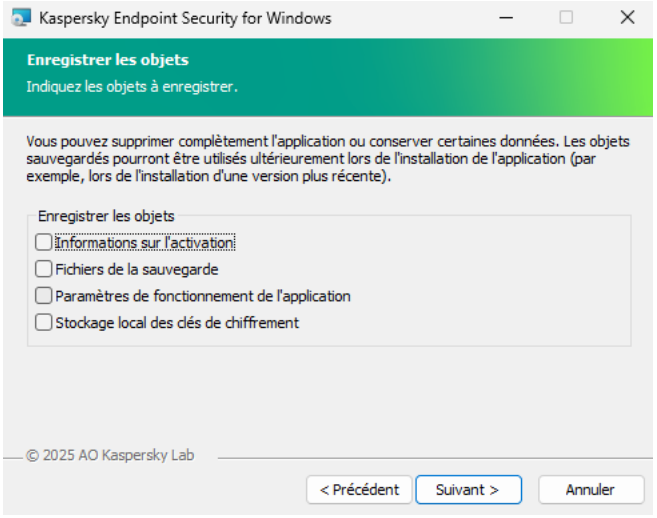
3. Utilisez la nouvelle stratégie pour exécuter le fichier BAT créé sur les ordinateurs.

Suppression de l'application en local

Vous pouvez supprimer l'application localement, à l'aide de l'Assistant d'installation. 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.

Sélection de l'opération de suppression de l'application

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 ne spécifiez aucune donnée, l'application sera complètement supprimée (voir la figure ci-dessous).



Enregistrement des données après suppression

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.

Kaspersky Endpoint Security enregistre les données dans le dossier `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Vous pouvez également supprimer l'application localement à l'aide de la ligne de commande.

Licence de l'application

Cette section présente les notions principales relatives à la licence de Kaspersky Endpoint Security.

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 connaissances 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\KES\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 permet d'utiliser l'application conformément aux conditions du Contrat de licence utilisateur final ainsi que de profiter du support technique. La liste des fonctionnalités disponibles 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. L'application ne peut pas être activée avec une licence d'évaluation après avoir été activée avec une licence commerciale.

- *Commerciale* : licence payante octroyée à l'achat de Kaspersky Endpoint Security.

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 :

- l'identifiant 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 Endpoint 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. Vous ne pouvez pas activer l'application sous l'abonnement à l'aide d'un fichier clé. Le fournisseur de services ne peut fournir qu'un code d'activation. 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.
- Obtenir un fichier clé depuis un autre Serveur d'administration.

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.

Comparaison des fonctionnalités des applications en fonction du type de licence pour les postes de travail

L'ensemble des fonctionnalités de Kaspersky Endpoint Security disponibles sur les postes de travail dépend du type de licence (voir le tableau ci-dessous).

Consulter aussi la comparaison des fonctionnalités des applications pour les serveurs

Comparaison des fonctionnalités de l'application en fonction du type de licence de Kaspersky Next, voir l'aide de Kaspersky Next.

Comparaison des fonctions de Kaspersky Endpoint Security

Fonction	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protection avancée								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Détection comportementale	✓	✓	✓	✓	✓	✓	✓	✓
Protection contre le chiffrement	✓	✓	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓
Pare-feu	✓	✓	✓	✓	✓	✓	✓	✓
Protection contre les menaces réseau	✓	✓	✓	✓	✓	✓	✓	✓
Protection BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protection AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Contrôles de sécurité								
Inspection des journaux	–	–	–	–	–	–	–	–
Contrôle des applications	✓	✓	✓	✓	✓	✓	✓	✓
Contrôle des appareils	✓	✓	✓	✓	✓	✓	✓	✓
Contrôle Internet	✓	✓	✓	✓	✓	✓	✓	✓
Contrôle évolutif des anomalies	–	✓	✓	✓	✓	✓	–	✓
Contrôle de l'intégrité du système	–	–	–	–	–	–	–	–
Chiffrement des données								

Fonction	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
Chiffrement de disque BitLocker	–	✓	✓	✓	✓	✓	–	✓
Chiffrement des fichiers	–	✓	✓	✓	✓	✓	–	✓
Chiffrement des disques amovibles	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licence de Kaspersky Sandbox doit être achetée séparément)*	✓	✓	✓	✓	✓	✓	✓	✓
Intégration avec KUMA *(la licence pour l'intégration KUMA doit être achetée séparément)*	✓	✓	✓	✓	✓	✓	✓	✓
Mode Light Agent *(pour activer l'application, vous devez ajouter une clé de licence à la SVM à laquelle le Light Agent est connecté)*	–	–	–	–	–	–	✓	✓

Comparaison des fonctionnalités des applications en fonction du type de licence pour les serveurs

L'ensemble des fonctionnalités de Kaspersky Endpoint Security disponibles sur les serveurs dépend du type de licence (voir le tableau ci-dessous).

Consulter aussi la comparaison des fonctionnalités des applications pour les postes de travail

Comparaison des fonctionnalités de l'application en fonction du type de licence de Kaspersky Next, voir l'aide de Kaspersky Next.

Fonction	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protection avancée								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Détection comportementale	✓	✓	✓	✓	✓	✓	✓	✓
Protection contre le chiffrement	✓	✓	✓	✓	✓	✓	✓	✓
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	–	✓	✓	✓	✓	✓	✓	✓
Pare-feu	✓	✓	✓	✓	✓	✓	✓	✓
Protection contre les menaces réseau	✓	✓	✓	✓	✓	✓	✓	✓
Protection BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protection AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Contrôles de sécurité								
Inspection des journaux	–	–	–	–	–	–	–	✓
Contrôle des applications	–	✓	✓	✓	✓	✓	–	✓
Contrôle des appareils	–	✓	✓	✓	✓	✓	✓	✓
Contrôle Internet	–	✓	✓	✓	✓	✓	✓	✓
Contrôle évolutif des anomalies	–	–	–	–	–	–	–	–
Contrôle de l'intégrité du système	–	–	–	–	–	–	–	✓
Chiffrement des données								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
Chiffrement de disque BitLocker	–	✓	✓	✓	✓	✓	–	✓
Chiffrement des fichiers	–	–	–	–	–	–	–	–
Chiffrement des disques amovibles	–	–	–	–	–	–	–	–

Fonction	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licence de Kaspersky Sandbox doit être achetée séparément)*	✓	✓	✓	✓	✓	✓	✓	✓
Intégration avec KUMA *(la licence pour l'intégration KUMA doit être achetée séparément)*	✓	✓	✓	✓	✓	✓	✓	✓
Mode Light Agent *(pour activer l'application, vous devez ajouter une clé de licence à la SVM à laquelle le Light Agent est connecté)*	–	–	–	–	–	–	✓	✓

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. De cette façon, vous pouvez ajouter la clé active et la clé de licence de réserve.
- À distance à l'aide de la suite logicielle Kaspersky Security Center.
  - Avec l'aide de la tâche *Ajout d'une clé*.

    Ce mode permet d'ajouter une clé sur un ordinateur concret ou sur des ordinateurs appartenant à un groupe d'administration. De cette façon, vous pouvez ajouter la clé active et la clé de licence de réserve.
  - 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.

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

- En ajoutant la clé au paquet d'installation de Kaspersky Endpoint Security.

  Cette méthode vous permet d'ajouter la clé dans les propriétés du paquet d'installation pendant le déploiement de Kaspersky Endpoint Security. L'application est automatiquement activée après l'installation.

- 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.

Si Kaspersky Endpoint Security est utilisé dans le mode Light Agent pour protéger les environnements virtuels, il n'est pas nécessaire d'activer l'application séparément.

Activation de l'application

Procédure d'activation de l'application dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Ajouter 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, veuillez consulter 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 Kaspersky Endpoint Security for Windows*.

Étape 6. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Kaspersky Endpoint Security for Windows 14.2**.

2. Dans la liste déroulante **Type de tâche**, choisissez **Ajouter 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 **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche. Passez à l'étape suivante.

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. Passez à l'étape suivante.

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

Étape 4. Fin de la création de la tâche

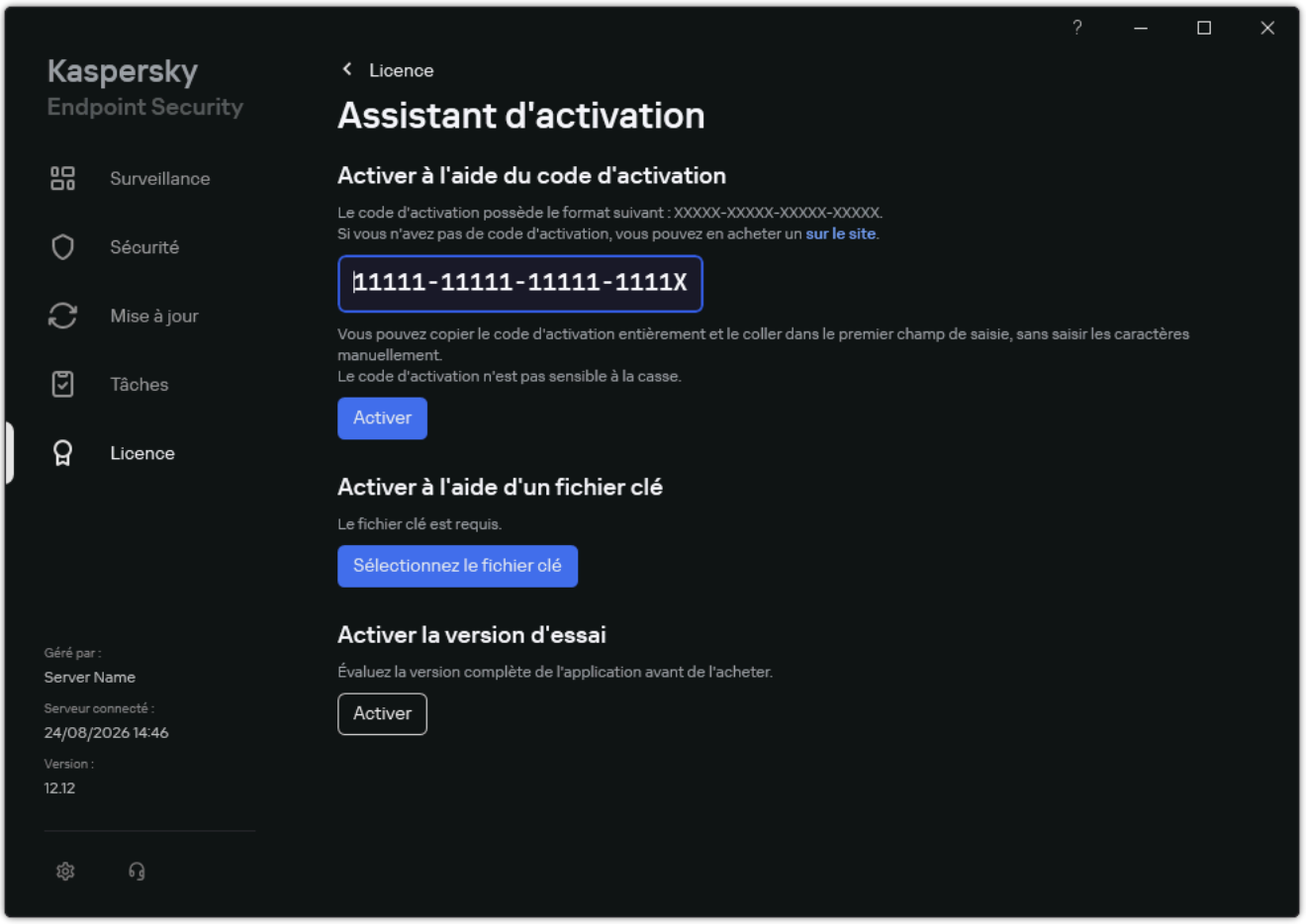
Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. Cette action entraîne l'activation de l'application Kaspersky Endpoint Security sur les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

Comment activer l'application dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Licence**.

2. Cliquez sur **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

Il est possible d'ajouter une clé de licence de réserve sur l'ordinateur via les propriétés de la tâche *Ajout d'une clé*. Une *clé de réserve* devient active à l'expiration de la clé active. 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 **Licences pour les logiciels 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 **Distribuer automatiquement la clé de licence sur les appareils administrés**.

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, sélectionnez **Opérations** → **Licence** → **Licences**.

   Une liste de clés de licence s'ouvre.

2. Ouvrez les propriétés de la clé de licence.

3. Sous l'onglet **Général**, activez le commutateur **Distribuer automatiquement la clé de licence sur les appareils administrés**.

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**.

Si vous activez l'application à l'aide d'un *code d'activation*, vous devez disposer d'un accès à Internet afin de pouvoir contacter les serveurs d'activation de Kaspersky. Si vous activez l'application à l'aide d'un *fichier clé*, vous ne devez pas disposer d'un accès à Internet. Si les ordinateurs se trouvent dans un segment isolé du réseau sans accès à Internet, pour activer l'application à l'aide d'un code, vous devez autoriser l'utilisation du Serveur d'administration de Kaspersky Security Center comme serveur proxy. Autrement dit, l'application peut accéder aux serveurs d'activation via le Serveur d'administration connecté à Internet.

Comment autoriser l'utilisation du Serveur d'administration comme serveur proxy pour l'activation de l'application dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.

4. Cochez la case **Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation**.

5. Enregistrez vos modifications.

Comment autoriser l'utilisation du Serveur d'administration comme serveur proxy pour l'activation de l'application dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Intégration KSC**.

5. Cochez la case **Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation**.

6. Enregistrez vos modifications.

Si vous ne pouvez pas activer l'application à l'aide d'un *code d'activation*, vous pouvez essayer d'obtenir un *fichier clé* en utilisant la solution Kaspersky, puis tenter à nouveau d'activer l'application via une méthode différente.

Surveillance de l'utilisation des licences

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

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

Détails de l'activation de l'application dans le cadre de Kaspersky Security Center Cloud Console

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 en savoir plus sur les licences de Kaspersky Security Center, veuillez consulter 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.

Suppression d'une clé de licence

Pour supprimer une clé de licence, vous devez exécuter une tâche spéciale sur vos ordinateurs. Vous pouvez par exemple supprimer une clé de licence pour réorganiser les unités de licence. De plus, lorsque la licence expire, Kaspersky Endpoint Security vous avertit. Si vous avez ajouté une clé de licence à court terme pour essayer l'application (par exemple, le module complémentaire EDR Optimum), vous pouvez supprimer cette clé de licence pour vous débarrasser des notifications et corriger l'état de votre ordinateur.

La tâche *Suppression de la clé* permet de supprimer toutes les clés de licence de l'ordinateur. Vous pouvez supprimer des clés de licence actives, ainsi que des clés de licence de réserve. En plus de la clé de licence d'activation de Kaspersky Endpoint Security, vous pouvez supprimer les clés de licence individuelles des solutions Kaspersky Detection and Response (par exemple, le module complémentaire EDR Optimum).

Comment supprimer une clé de licence dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.
   La liste des tâches s'ouvre.
2. Cliquez sur **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 (14.2)** → **Suppression de la clé**.

Étape 2. Sélection de la licence

Sélectionnez la clé de licence que vous souhaitez supprimer. Vous pouvez sélectionner une clé de licence dans la bibliothèque de clés de Kaspersky Security Center ou sélectionner un fichier clé.

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 de tâche, par exemple, *Supprimer la clé de la version bêta*.

Étape 6. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment supprimer une clé de licence dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Kaspersky Endpoint Security for Windows 14.2**.

2. Dans la liste déroulante **Type de tâche**, choisissez **Supprimer la clé**.

3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Supprimer la clé de la version bêta*.

4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche. Passez à l'étape suivante.

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

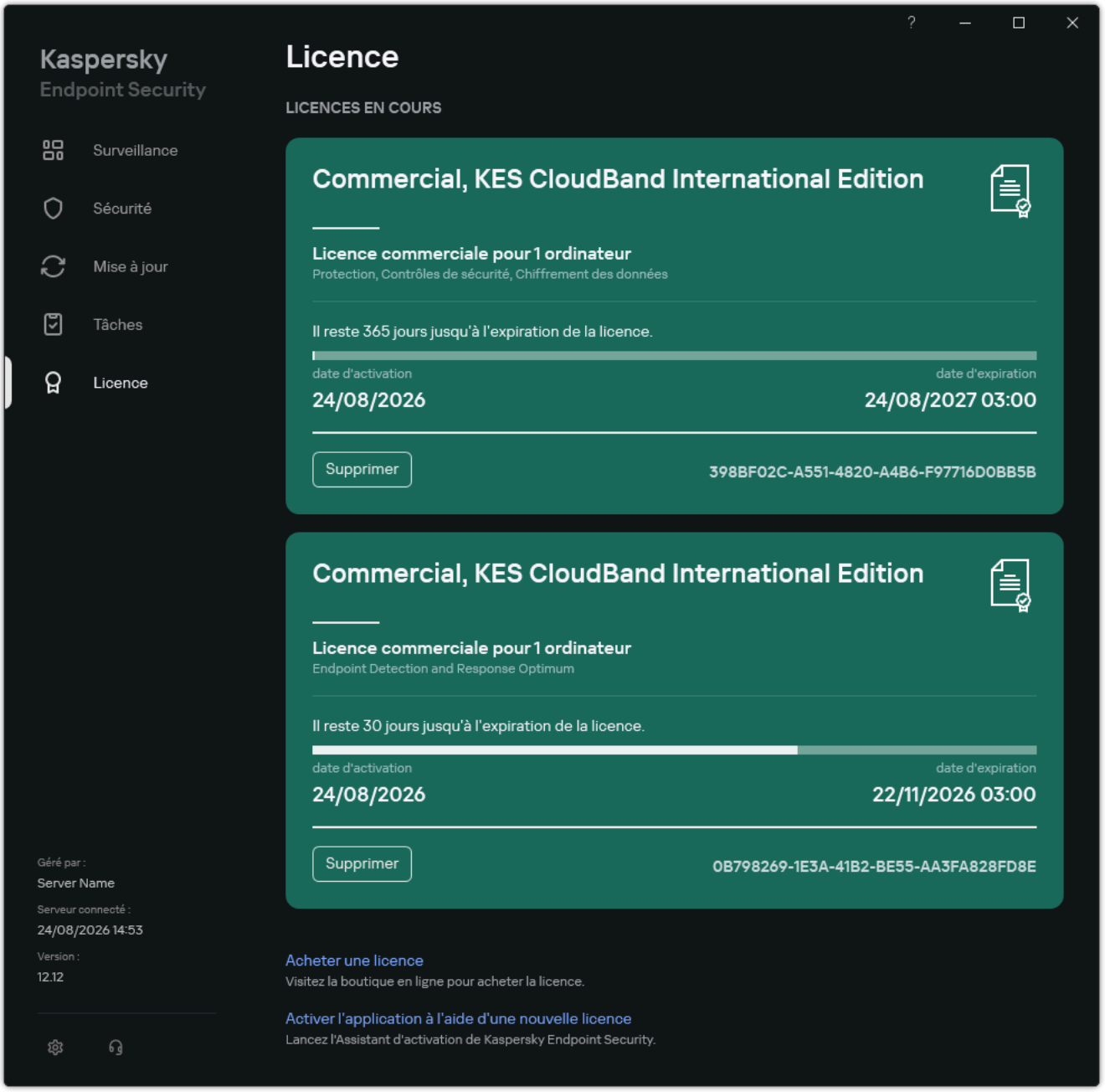
Sélectionnez la clé de licence que vous souhaitez supprimer. Vous pouvez sélectionner une clé de licence dans la bibliothèque de clés de Kaspersky Security Center ou sélectionner un fichier clé. Passez à l'étape suivante.

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**.

Comment supprimer une clé de licence dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Licence**.
2. Sélectionnez une clé que vous souhaitez supprimer et cliquez sur **Supprimer**.



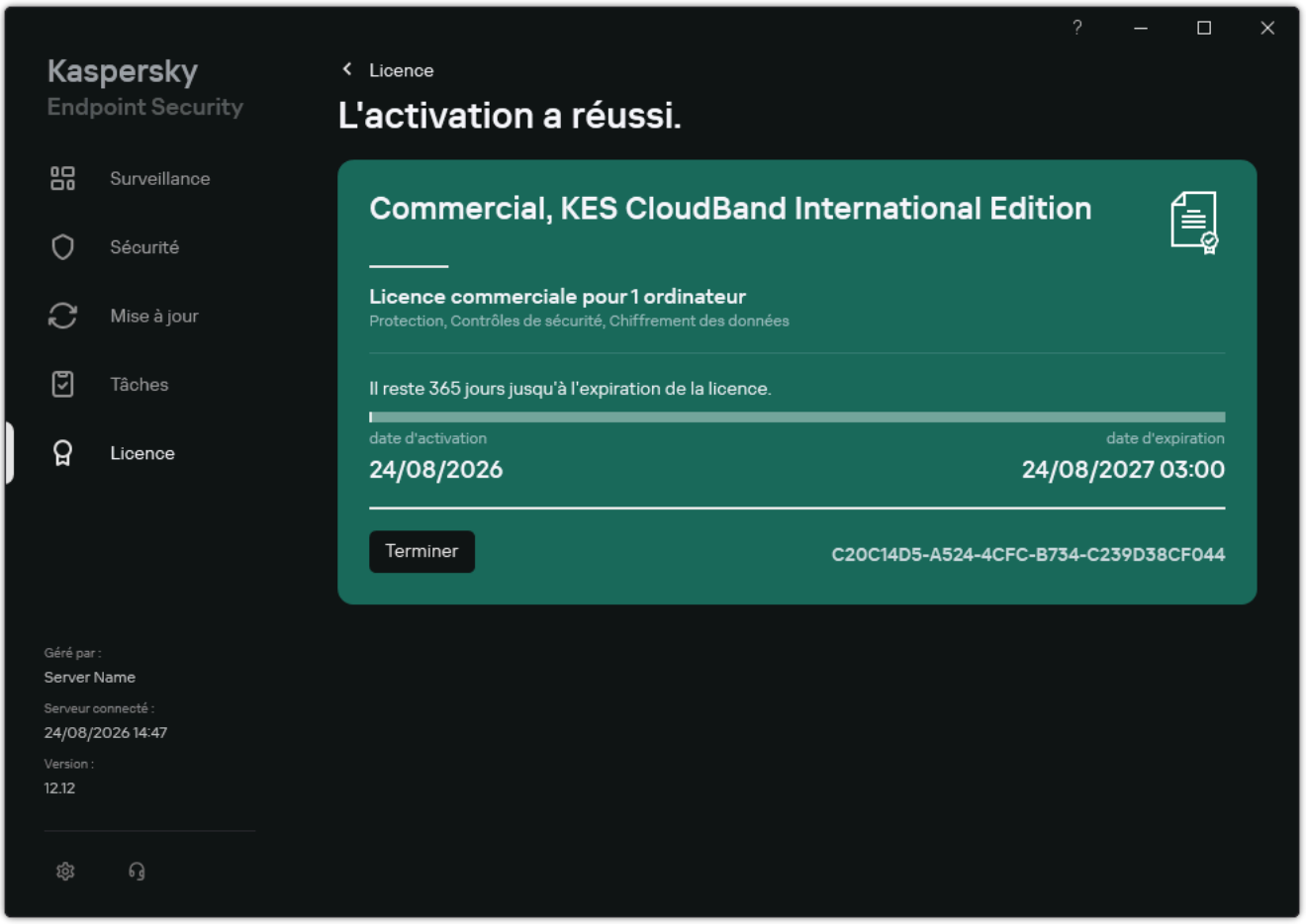
Fenêtre Licence

Vous pouvez également supprimer une clé de licence sur la ligne de commande.

Consultation des informations relatives à la licence

Pour consulter les informations sur la licence,

Dans la fenêtre principale de l'application, accédez à la section **Licence** (cf. ill. ci-dessous).



Fenêtre Licence

La section affiche 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. Une clé de licence de réserve peut devenir active uniquement après l'expiration de la clé active ou après avoir supprimé la clé active en cliquant sur **Supprimer**.
- *Nom de l'application*. Le nom complet de l'application de Kaspersky achetée.
- *Type de licence*. Les types de licence suivants sont prévus : évaluation et commercial.
- *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*. Date de début et date de fin de la durée de validité de la licence (uniquement pour la clé active), durée restante de la durée de validité de la licence.

  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.

- *Clé*. La clé est une succession unique de caractères alphanumériques, formée au départ du code d'activation ou du fichier clé.

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 à l'aide d'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, accédez à la section **Licence**.

2. Exécutez une des actions 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.

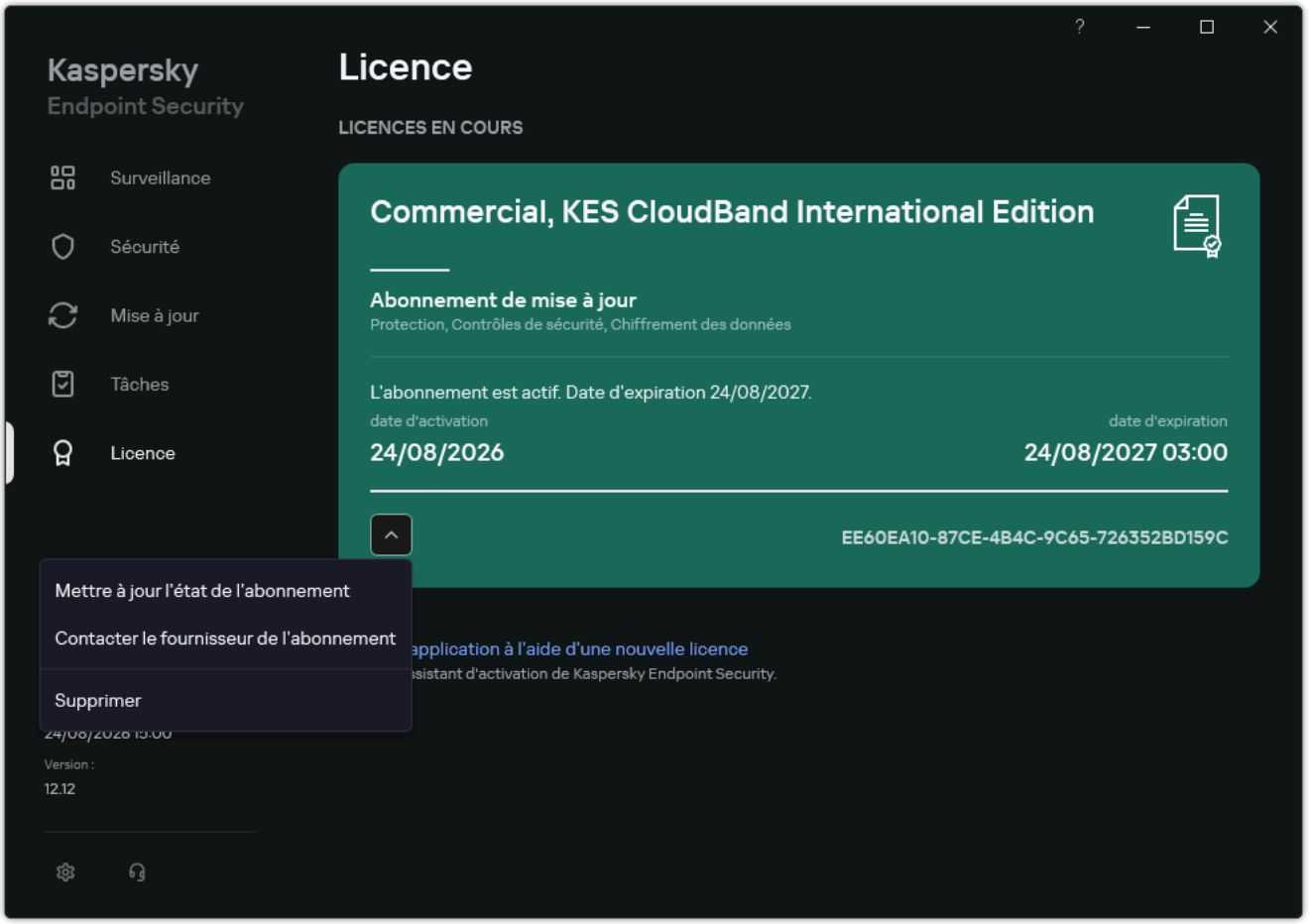
Vous pouvez renouveler l'abonnement sur le site Internet du prestataire de services.

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, accédez à la section **Licence**.

2. Cliquez sur **Contacter le fournisseur de l'abonnement**.

   Vous pouvez mettre à jour l'état de l'abonnement manuellement. 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.



Renouvellement de l'abonnement

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 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 Web Console et Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (ci-après également dénommée *Web Console*). Il s'agit d'une interface Web permettant d'administrer un système de protection basé sur les applications Kaspersky. Vous pouvez travailler dans Kaspersky Security Center Web Console à l'aide d'un navigateur sur n'importe quel appareil. Pour obtenir de plus amples informations sur Kaspersky Security Center 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 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 Web Console. Le plug-in Internet doit être installé sur un ordinateur sur lequel Kaspersky Security Center Web Console est installé. 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 Web**).

Si vous utilisez Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Endpoint Detection and Response Optimum, vous devez installer le plug-in d'administration de Kaspersky Endpoint Detection and Response . Vous avez besoin du plug-in d'administration pour afficher les détails de l'alerte. Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Par conséquent, pour créer des tâches de réponse aux menaces, vous avez besoin du plug-in d'administration de Kaspersky Endpoint Security et pour consulter les détails des alertes, vous avez besoin du plug-in d'administration EDR.

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 l'application de Kaspersky Security Center Web Console.

  Web Console propose automatiquement de lancer l'Assistant de configuration initiale de l'application lors de la première connexion de Web Console au Serveur d'administration. Vous pouvez également exécuter l'Assistant de configuration initiale de l'application dans l'interface de Web Console (**Découverte et déploiement** → **Déploiement et attribution** → **Assistant de démarrage rapide de l'application**). L'Assistant de configuration initiale de l'application 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 l'application de Kaspersky Security Center 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 Web**). 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 Web**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site de Kaspersky.

À compter de Kaspersky Endpoint Security 12.11 for Windows, la procédure d'installation du plug-in Internet a changé. Le paquet de distribution inclut désormais deux plug-ins Internet : *Kaspersky Endpoint Security for Windows 14.2.0* et *Unified Protection and Management Plug-in*. Cela est dû au passage à un plug-in Web unique et unifié pour l'administration des applications Kaspersky. Le plug-in Web unifié permet de créer une stratégie unique pour administrer plusieurs applications Kaspersky (par exemple, Kaspersky Endpoint Security for Windows, macOS et Linux). La transition vers le plug-in Web unifié peut nécessiter plusieurs versions. Une fois la transition terminée, le paquet de distribution inclura uniquement *Unified Protection and Management Plug-in*.

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 Web**). 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**). 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 Web**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site 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.

Si le plug-in d'administration de Kaspersky Endpoint Security est installé dans la Console d'administration, l'installation de la nouvelle version du plug-in d'administration pour possède les particularités suivantes :

- La version précédente du plug-in d'administration de Kaspersky Endpoint Security est supprimée.
- Le plug-in d'administration de Kaspersky Endpoint Security d'une nouvelle version prend en charge l'administration de l'application Kaspersky Endpoint Security 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 débuter 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.

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 et des modules d'application ;
- Activation de l'application à l'aide d'un code d'activation (activation 2.0) ;
- Utilisation de Kaspersky Security Network.

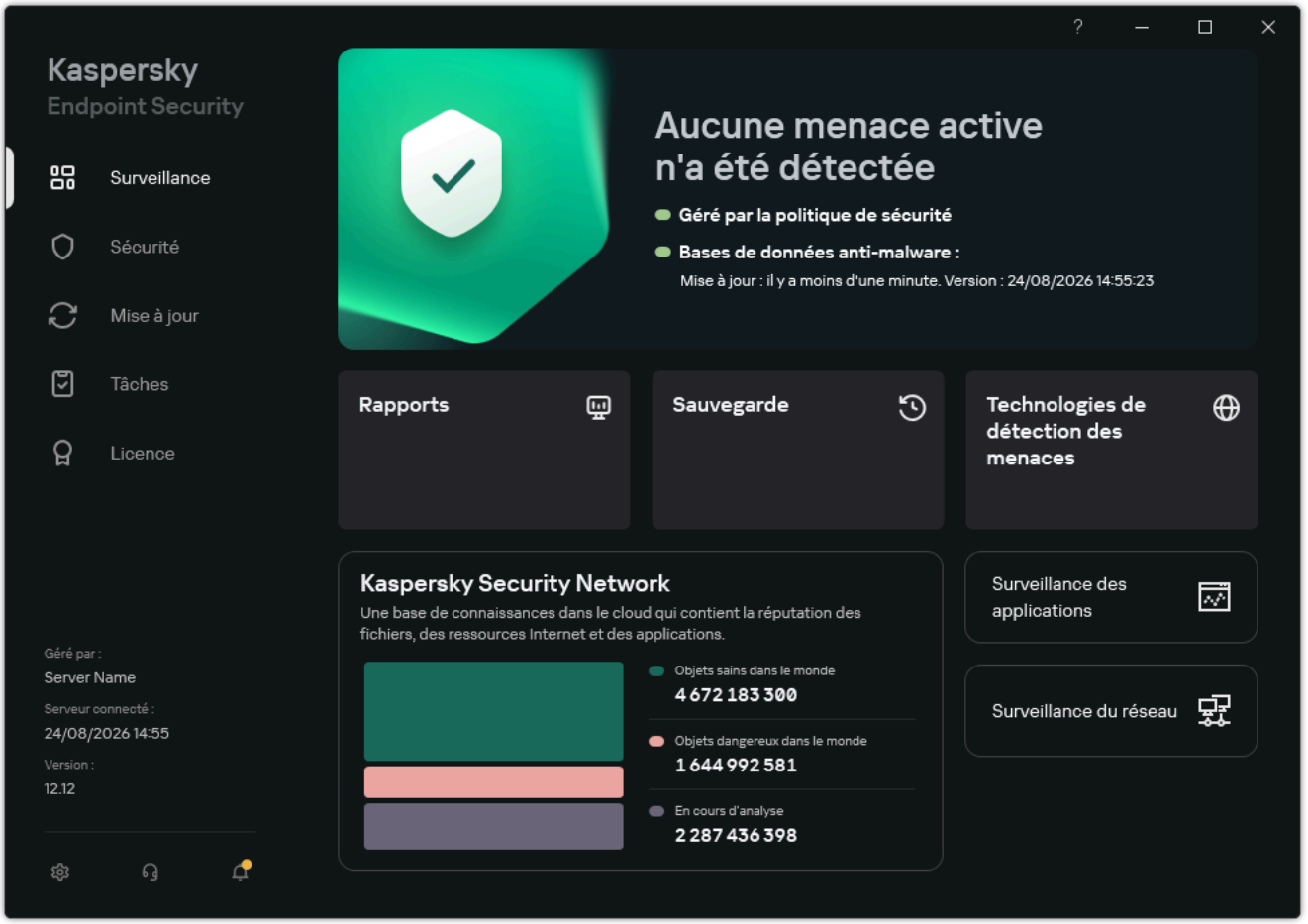
L'utilisation du protocole TLS sécurise l'application et offre les fonctionnalités suivantes :

- 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 Public Key Infrastructure (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 Self-Signed Certificate. 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

Surveillance	• **Rapports**. Consultez les événements qui se sont produits pendant le fonctionnement de l'application, les modules individuels et les tâches. • **Sauvegarde**. 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. *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 à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés. • **Surveillance des applications**. Consultez les informations relatives au fonctionnement des applications installées. La Surveillance des applications 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.
Sécurité	État de fonctionnement des modules installés. Vous pouvez également passer à la configuration des modules ou à la visualisation des rapports.
Mise à jour	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 la section à l'utilisateur ou restreindre la gestion des tâches.
Tâches	Gérez les tâches d'analyse de Kaspersky Endpoint Security. Vous pouvez effectuer une analyse des logiciels malveillants et un contrôle d'intégrité de l'application. Un administrateur peut masquer des tâches à un utilisateur ou restreindre la gestion des tâches.

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.
	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.

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.

Si l'icône de l'application dans la zone de notification de la barre des tâches est masquée, cela signifie que l'administrateur a désactivé l'affichage de l'interface de l'application dans la stratégie.

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, cliquez sur **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 de recherche de logiciels malveillants. L'application continue également à utiliser Kaspersky Security Network.

- **Désactiver la stratégie/Activer la stratégie**. Désactivation de 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 **Activer 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**. Désactivation de 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 **Activer la stratégie** dans le menu contextuel de l'application.

- **Tâches**. Liste déroulante contenant les éléments suivants :

  - **Vérification de l'intégrité de l'application**.

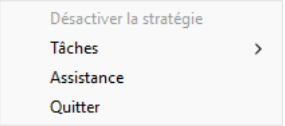
  - **Restauration des bases de données à leur version précédente**.

  - **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 :

- **Simplifié**. 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 uniquement les notifications nécessitant une action de l'utilisateur au-dessus de l'icône de l'application.
- **Complet**. 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.
- **Ne pas afficher l'interface utilisateur**. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.

4. Dans le groupe **Interaction avec l'utilisateur**, configurez l'affichage de l'interface de l'application :

   - **Afficher l'interface utilisateur**. 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. Si nécessaire, vous pouvez activer la fonctionnalité **Masquer la section Surveillance des applications** permettant de masquer les données relatives à l'activité des applications sur l'ordinateur, limitant ainsi l'accès des utilisateurs à l'outil Surveillance des applications.

   - **Afficher l'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 uniquement les notifications nécessitant une action de l'utilisateur au-dessus de l'icône de l'application.

   - **Ne pas afficher l'interface utilisateur**. 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.

5. Enregistrez vos modifications.

Configuration du mode d'affichage de l'interface de l'application dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.

5. Dans le groupe **Visibilité pour les utilisateurs**, configurez l'affichage de l'interface de l'application :

   - **Afficher l'interface utilisateur**. Si cette fonctionnalité est désactivée, aucun signe du fonctionnement de Kaspersky Endpoint Security ne s'affiche sur l'ordinateur client. De même, l'icône dans la zone de notification Windows et les notifications ne sont pas disponibles.

   - **Simplifié**. 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 uniquement les notifications nécessitant une action de l'utilisateur au-dessus de l'icône de l'application.

   - **Complet**. 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.

   - **Masquer la section Surveillance des applications**. Si vous souhaitez masquer les informations relatives à l'activité des applications sur l'ordinateur de l'utilisateur, vous pouvez restreindre l'accès des utilisateurs à l'outil Surveillance des applications.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Préparation de l'application pour utilisation

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 l'application de Kaspersky Security Center crée automatiquement une stratégie pour Kaspersky Endpoint Security.

- Créez les tâches *Mise à jour des bases et des modules d'application* et *Analyse des logiciels malveillants*.

  La tâche *Mise à jour des bases et des modules d'application* 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 des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

  La tâche *Analyse des logiciels malveillants* est requise afin de détecter en temps utiles les virus et autres programmes dangereux. Il faut créer la tâche *Analyse des logiciels malveillants* manuellement.

  Création d'une tâche Analyse des logiciels malveillants dans la Console d'administration (MMC)

  1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

     La liste des tâches s'ouvre.

  2. Cliquez sur **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 (14.2)** → **Analyse des logiciels malveillants**.

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, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

- **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 échoue, 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 avancée 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.

- **Exécuter uniquement lorsque l'ordinateur est inactif**. Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.

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 *Analyse des logiciels malveillants*. 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. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. L'analyse des logiciels malveillants est alors exécutée sur les ordinateurs de l'utilisateur conformément à la planification définie.

Comment créer une tâche Analyse des logiciels malveillants dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Analyse des logiciels malveillants**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Analyse hebdomadaire*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Pour configurer la planification de l'exécution de la tâche, accédez aux propriétés de la tâche.

   Il est recommandé de planifier l'exécution de cette tâche au moins une fois par semaine.

8. Cochez la case en regard de la tâche.

9. Cliquez sur **Démarrer**.

   Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

L'analyse des logiciels malveillants est alors exécutée sur les ordinateurs de l'utilisateur conformément à la planification définie.

- Optimiser les performances de Kaspersky Endpoint Security.

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.

Chaque paramètre de stratégie comporte l'attribut (« cadenas »). L'état de cet attribut détermine si le paramètre sera transmis aux appareils gérés du groupe d'administration :

- Si le « cadenas » est ouvert (), la valeur de ce paramètre n'est pas transmise aux appareils administrés. Le paramètre peut être modifié dans l'interface locale de l'application. On parle alors de paramètres *déverrouillés*.

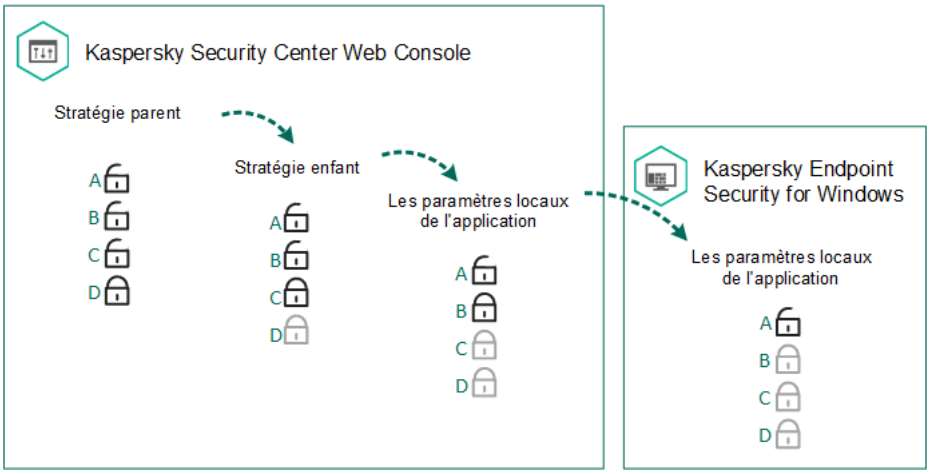
- Si le « cadenas » est fermé (), la valeur de ce paramètre est transmise aux appareils administrés. On parle alors de paramètres *verrouillés*. Les paramètres bloqués ne peuvent pas être modifiés dans l'interface locale de l'application.

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.

Héritage des paramètres

Les stratégies, à l'instar des groupes d'administration, ont une hiérarchie. 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.

Par défaut, une stratégie enfant hérite des paramètres de la stratégie parent. Si le paramètre de la stratégie parent comporte l'attribut (« cadenas » fermé), alors, dans les stratégies enfants et les paramètres d'application locaux, la valeur de ce paramètre sera remplacée conformément à la stratégie parent, et le paramètre sera verrouillé. Si nécessaire, vous pouvez désactiver l'héritage des paramètres de la stratégie parent. 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 droits 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 (par défaut, cette section est masquée dans l'interface de la console).

Révisions des stratégies

Kaspersky Security Center suit les modifications apportées aux stratégies et crée les révisions. Une *révision* est un ensemble de paramètres modifiés enregistrés par l'utilisateur. Les révisions vous permettent de comparer et d'annuler les modifications apportées aux paramètres de la stratégie. Outre l'ensemble des paramètres modifiés, la révision comprend des informations sur l'utilisateur à l'origine des modifications, ainsi que l'heure, l'adresse IP, le commentaire de l'utilisateur et d'autres données pertinentes.

Pour consulter le journal des révisions, ouvrez les propriétés de la stratégie et accédez à la section **Historique des révisions**. Pour obtenir plus de détails sur l'utilisation des révisions, consultez l'aide de Kaspersky Security Center.

Création d'une stratégie

Lors de la création d'une stratégie, l'Assistant propose des paramètres pertinents pour le mode sélectionné. Par exemple, pour le mode Light Agent, vous devez ajouter un Serveur de protection (SVM). Lorsque vous utilisez l'application pour protéger un serveur SQL, vous devez ajouter des exclusions d'analyse prédéfinies pour vous assurer que le fonctionnement du serveur n'est pas perturbé. Une fois le mode sélectionné, l'Assistant propose des paramètres de stratégie pertinents. Vous pouvez ensuite modifier ces paramètres dans les propriétés de la 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 l'espace de travail, sélectionnez l'onglet **Stratégies**.
4. Cliquez sur **Nouvelle stratégie**.

   L'Assistant de création de la stratégie démarre.
5. Suivez les instructions de l'Assistant de création de stratégie.

Étape 1.

Sélectionnez l'application **Kaspersky Endpoint Security for Windows (14.2)**.

Étape 2.

Saisissez le nom de la stratégie de groupe, par exemple *Stratégie pour le bureau*.

Vous pouvez également créer des stratégies sur la base de stratégies existantes à l'aide de l'Assistant Nouvelle stratégie. Pour ce faire, lors de la définition du nom de la stratégie de groupe, cochez la case **&Utiliser les paramètres de stratégie d'une version antérieure de l'application**. L'Assistant permet également de créer une stratégie Kaspersky Endpoint Security (KES) basée sur une stratégie d'une autre solution, par exemple Kaspersky Security for Windows Server (KSWS) ou Kaspersky Security for Virtualization Light Agent for Windows.

Étape 3. Participation au Kaspersky Security Network

Lisez la Déclaration de Kaspersky Security Network (KSN) et acceptez-la.

Étape 4.

En fonction de l'utilisation prévue de Kaspersky Endpoint Security, vous pouvez configurer une stratégie pour les modes d'application suivants :

- Mode standard pour protéger les hôtes

Ce mode permet de choisir la manière dont vous souhaitez configurer la stratégie :

- **Créer une stratégie avec les paramètres par défaut**. Les paramètres par défaut sont considérés comme optimaux. Ces paramètres sont recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources.

- **Modifier les paramètres de la stratégie dans l'Assistant**. Cette méthode permet de gérer les paramètres d'une stratégie pas à pas à l'aide d'un Assistant. Vous pouvez également gérer les paramètres d'une stratégie à l'aide d'un fichier de configuration de l'application (voir l'étape suivante).

- Endpoint Detection and Response Agent pour la protection contre les menaces avancées et les attaques ciblées.

  Endpoint Detection and Response Agent est une application installée sur les postes de travail et les serveurs individuels de l'infrastructure informatique de l'organisation pour prendre en charge les solutions Detection and Response par Kaspersky. À l'étape suivante, vous devez sélectionner une solution pour l'intégration d'EDR Agent.

- Light Agent pour protéger les environnements virtuels.

  Pour utiliser l'application en mode Light Agent, vous devez configurer une connexion avec une machine virtuelle SVM. Ces paramètres sont nécessaires au fonctionnement de l'application en mode Light Agent.

Kaspersky Endpoint Security fournit une stratégie commune pour tous les modes d'application et types de systèmes d'exploitation. Cela signifie que la stratégie couvre l'ensemble des paramètres. Cependant, il se peut que l'application ignore certains paramètres de la stratégie, car Kaspersky Endpoint Security est déployé dans un mode dans lequel certaines fonctionnalités ne sont pas disponibles. Par exemple, lors de l'utilisation de l'application en mode Endpoint Detection and Response Agent, seuls les paramètres pertinents pour l'intégration aux solutions Kaspersky Detection and Response et pour l'intégration à KUMA sont disponibles.

Nous recommandons d'utiliser des stratégies différentes selon les modes et les types de systèmes d'exploitation.

Étape 5. Paramètres d'importation

Cette étape est disponible si vous avez sélectionné la configuration manuelle de la stratégie à l'étape 4.

Vous pouvez créer une stratégie à partir des paramètres de Kaspersky Endpoint Security contenus dans un fichier de configuration CFG. L'Assistant de création d'une stratégie ne prend pas en charge les fichiers de configuration chiffrés. Lors de l'exportation du fichier de configuration, ignorez l'étape de chiffrement du fichier.

Lors de l'importation d'un fichier de configuration CFG de l'application, tous les paramètres de stratégie ne sont pas accessibles à l'Assistant. Par exemple, les profils de stratégie ne figurent pas dans les paramètres de l'application. Si vous souhaitez transférer tous les paramètres et profils vers la stratégie, vous pouvez importer une autre stratégie à partir d'un fichier KLP.

Lors de l'importation d'un fichier de configuration, Kaspersky Endpoint Security ne transfère pas les mots de passe des conteneurs crypto. Si vous utilisez l'authentification bidirectionnelle lors de la connexion aux serveurs, vous devez spécifier les mots de passe des conteneurs crypto depuis le début.

Étape 6–10. Configuration des paramètres de stratégie

Cette étape est disponible si vous avez sélectionné la configuration manuelle de la stratégie à l'étape 4.

Suivez les étapes pour gérer les paramètres de stratégie.

Étape 11. Configuration de la zone de confiance

Configurez la zone de confiance. Vous pouvez ajouter des exclusions d'analyse et des applications de confiance prédéfinies. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent également vous aider à configurer rapidement Kaspersky Endpoint Security en mode Light Agent dans les environnements virtuels Citrix et VMware.

Étape 12. Selection de l'état de la stratégie

- **Actif**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.

  Les paramètres de la stratégie active sont conservés sur les ordinateurs clients lors de la synchronisation. Il est impossible d'application simultanément plusieurs stratégies à un ordinateur et pour cette raison, il ne peut y avoir qu'une stratégie active par groupe.

- **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.

  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.

- **Pour les utilisateurs itinérants**. La stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.

Quittez l'Assistant.

Création d'une stratégie dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur **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. Sélectionnez le mode de l'application :

- Mode standard pour protéger les postes de travail et les serveurs

- Endpoint Detection and Response Agent pour la protection contre les menaces avancées et les attaques ciblées.

  Si vous sélectionnez ce mode, vous pouvez créer une stratégie pour intégrer l'ordinateur aux solutions Kaspersky Detection and Response. L'Assistant vous propose de configurer l'intégration pour Kaspersky Managed Detection and Response, puis pour Kaspersky Anti Targeted Attack Platform (EDR).

- Light Agent pour protéger les environnements virtuels.

  Si vous sélectionnez ce mode, à l'étape suivante, vous devez configurer la connexion au Serveur de protection (SVM). Ces paramètres sont nécessaires au fonctionnement de l'application en mode Light Agent.

Kaspersky Endpoint Security fournit une stratégie commune pour tous les modes d'application et types de systèmes d'exploitation. Cela signifie que la stratégie couvre l'ensemble des paramètres. Cependant, il se peut que l'application ignore certains paramètres de la stratégie, car Kaspersky Endpoint Security est déployé dans un mode dans lequel certaines fonctionnalités ne sont pas disponibles. Par exemple, lors de l'utilisation de l'application en mode Endpoint Detection and Response Agent, seuls les paramètres pertinents pour l'intégration aux solutions Kaspersky Detection and Response et pour l'intégration à KUMA sont disponibles.

> Nous recommandons d'utiliser des stratégies différentes selon les modes et les types de systèmes d'exploitation.

6. Configurez la zone de confiance. Vous pouvez ajouter des exclusions d'analyse et des applications de confiance prédéfinies. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent également vous aider à configurer rapidement Kaspersky Endpoint Security en mode Light Agent dans les environnements virtuels Citrix et VMware.

7. Sous l'onglet **Général**, exécutez les actions suivantes :

- modifier le nom de la stratégie ;

- Sélectionner l'état d'une stratégie :

  - **Actif**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.

    Les paramètres de la stratégie active sont conservés sur les ordinateurs clients lors de la synchronisation. Il est impossible d'application simultanément plusieurs stratégies à un ordinateur et pour cette raison, il ne peut y avoir qu'une stratégie active par groupe.

- **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.

  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.

- **Pour les utilisateurs itinérants**. 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.

  - **Imposer l'héritage des paramètres aux 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 la 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.

8. L'onglet **Paramètres de l'application** permet de configurer les paramètres de la stratégie de Kaspersky Endpoint Security.

9. Quittez l'Assistant.

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 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.

Exportation et importation d'une stratégie

Kaspersky Endpoint Security permet d'exporter une stratégie avec ses paramètres et ses profils dans un fichier KLP. Vous pouvez ensuite utiliser la fonctionnalité d'exportation/d'importation des stratégies pour sauvegarder des stratégies, les transférer vers un autre serveur ou, par exemple, les transférer de Kaspersky Security Center Windows vers Kaspersky Security Center Linux. Pour en savoir plus sur la gestion des stratégies, consultez l'aide de Kaspersky Security Center.

Comment exporter et importer 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 requis.

3. Dans l'espace de travail, sélectionnez l'onglet **Stratégies**.

4. Pour exporter une stratégie, procédez comme suit :

   a. Cliquez sur la stratégie que vous souhaitez exporter.

   b. Cliquez sur le lien **Exporter la stratégie dans le fichier** situé dans la partie droite de la fenêtre.

   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format KLP dans lequel vous voulez exporter la stratégie et choisissez le dossier dans lequel vous souhaitez enregistrer le fichier.

   d. Enregistrez le fichier.

5. Pour importer une stratégie, procédez comme suit :

   a. Cliquez sur **Importer une stratégie à partir d'un fichier**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de stratégie KLP que vous souhaitez importer.

   c. Ouvrez le fichier.

   Cette action ajoute une nouvelle stratégie avec l'état *Stratégie inactive*.

Comment exporter et importer la stratégie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Pour exporter une stratégie, procédez comme suit :

   a. Cochez la case en regard de la stratégie que vous souhaitez exporter.

   b. Appuyez sur le bouton **Exporter**.

   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format KLP dans lequel vous voulez exporter la stratégie et choisissez le dossier dans lequel vous souhaitez enregistrer le fichier.

   d. Enregistrez le fichier.

3. Pour importer une stratégie, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Sélectionnez le fichier de stratégie KLP que vous souhaitez importer.

   c. Une fois que la stratégie a été traitée, sélectionnez le groupe d'administration auquel vous souhaitez l'appliquer.

   d. Cliquez sur le bouton **Terminée** pour terminer l'importation de la stratégie.

   Cette action ajoute une nouvelle stratégie avec l'état *Inactive*.

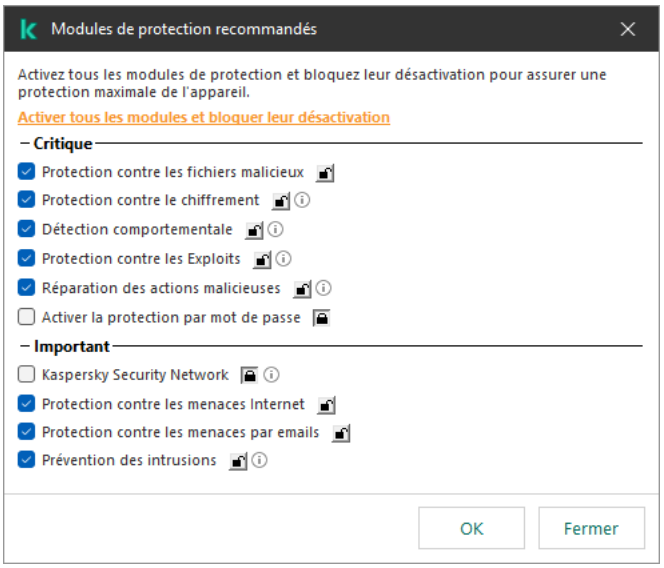
Indicateur du niveau de protection

L'indicateur de niveau de sécurité s'affiche en haut de la fenêtre des propriétés 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.
    - Protection des services d'application contre l'administration externe.
  - **Important**. Cette catégorie contient les modules suivants :
    - Kaspersky Security Network.
    - Protection contre les menaces Internet.
    - Protection contre les menaces par emails.
    - Prévention des intrusions.
    - Protection par mot de passe.
- **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 protection recommandés** apparaît à droite. Cette fenêtre permet d'activer n'importe quel module de la protection recommandé.

Après la mise à jour de l'application, l'indicateur de niveau de protection peut indiquer un niveau de protection inférieur à celui d'avant la mise à jour. Cette situation se produit parce que la nouvelle version de l'application introduit de nouveaux modules ou fonctionnalités importants pour la sécurité de l'ordinateur. Après avoir mis à jour l'application, vous devrez gérer les nouveaux paramètres afin de garantir le maintien d'un niveau de protection élevé.



Indicateur du niveau de sécurité de la stratégie

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 :

- **Analyse des logiciels malveillants**. 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 *Analyse des logiciels malveillants* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale de l'application. Il est recommandé de planifier l'exécution de cette 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 de la sélection des modules 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 des bases et des modules d'application**. Kaspersky Endpoint Security met à jour les bases et les modules de l'application. La tâche *Mise à jour des bases et des modules d'application* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale de l'application. 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.

- **Annulation 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 de l'application**. 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.

- **Administrer les 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.

Si l'application fonctionne dans le cadre de la solution Endpoint Detection and Response de Kaspersky, vous pouvez exécuter des tâches supplémentaires en tant qu'actions de réponse à la détection (responses). Par exemple, vous pouvez mettre fin aux processus à distance à l'aide de la tâche *Fin du processus*.

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 d'administration.

3. Cliquez sur **Nouvelle tâche**.

   L'Assistant de création de tâche démarre.

4. Suivez les instructions de l'Assistant de création de tâche.

Comment créer une tâche dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   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 la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

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** → **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.

Gestion 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Tâches locales** → **Administration des tâches**.

4. Configurez le mode d'utilisation des tâches (cf. tableau ci-dessous).

5. 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, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.

5. Sous **Actions autorisées**, configurez le mode d'utilisation des tâches (cf. tableau ci-dessous).

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Paramètres de gestion des tâches

Paramètre	Description
Accéder aux tâches locales	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, 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. Si cette case est décochée, les tâches locales sont masquées dans l'interface de l'application. 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. L'utilisateur peut toujours lancer la recherche 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.
Afficher les tâches de groupe	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. Si cette case n'est pas cochée, Kaspersky Endpoint Security affiche une liste de tâches vide.
Gérer les tâches de groupe	Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans la console de 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. Si cette case n'est pas cochée, Kaspersky Endpoint Security lance automatiquement les tâches selon la planification ou l'administrateur les lance manuellement dans la console de Kaspersky Security Center.

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 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 (14.2)**, puis ouvrez les propriétés de l'application d'un double-clic.

7. Dans la section **Paramètres généraux**, configurez Kaspersky Endpoint Security ainsi que les rapports et le stockage.

   Les autres sections de la fenêtre des propriétés de l'application sont constituées par défaut pour 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**.

8. Enregistrez vos modifications.

Configuration des paramètres locaux de l'application dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

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. Sélectionnez l'onglet **Applications**.

4. Cliquez sur **Kaspersky Endpoint Security for Windows 14.2**.

   La fenêtre des paramètres locaux de l'application s'ouvre.

5. Sélectionnez l'onglet **Paramètres de l'application**.

6. Configurez les paramètres locaux de l'application.

7. Enregistrez vos modifications.

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)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. La case **Lancer l'application au démarrage de l'ordinateur (recommandé)** permet de configurer le lancement de l'application.
5. Enregistrez vos modifications.

Configuration du lancement de Kaspersky Endpoint Security dans Web Console

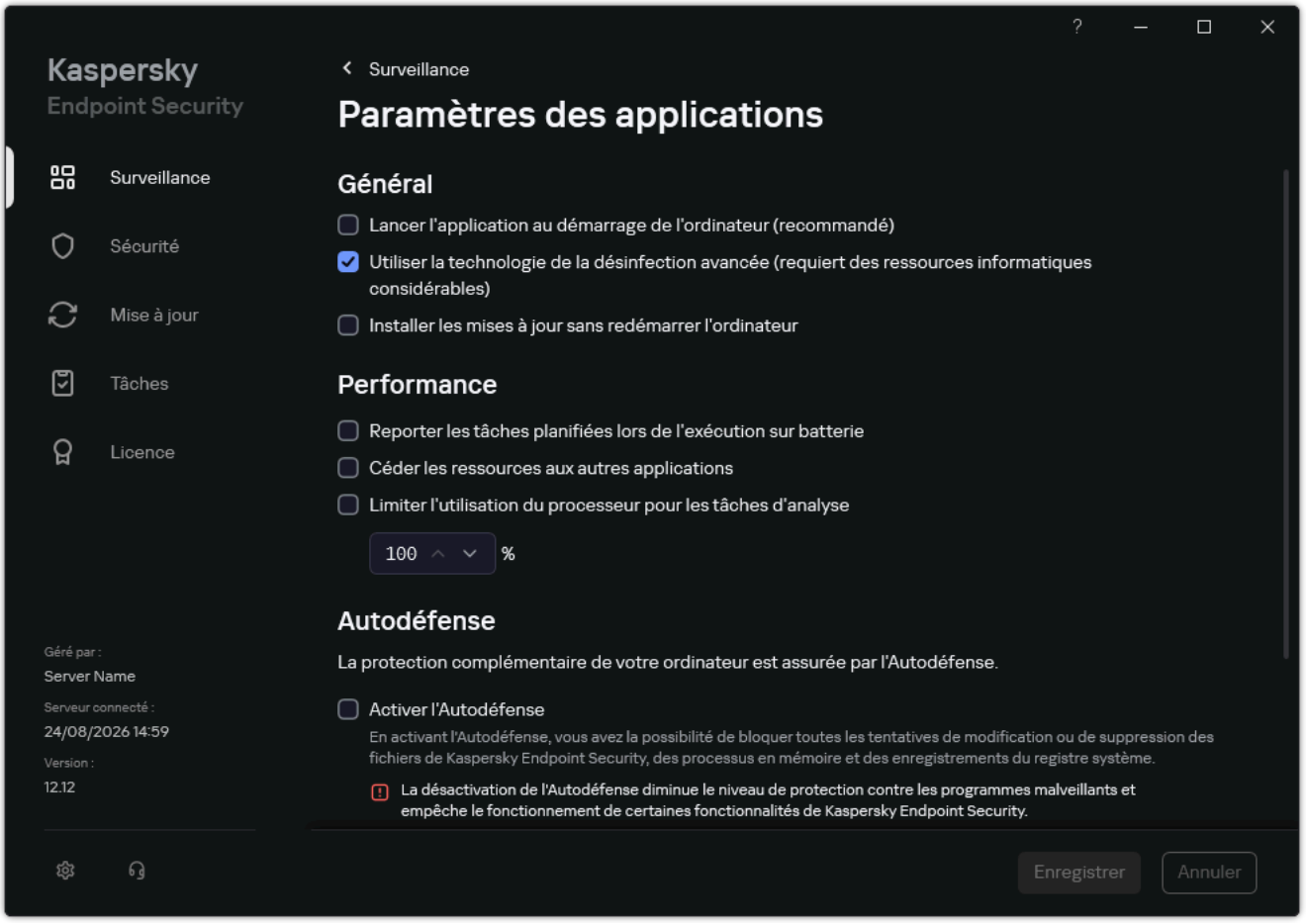
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.
5. La case **Lancer Kaspersky Endpoint Security au démarrage de l'ordinateur (recommandé)** permet de configurer le lancement de l'application.
6. Enregistrez vos modifications.

Configuration du lancement de Kaspersky Endpoint Security dans l'interface d'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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. La case **Lancer l'application au démarrage de l'ordinateur (recommandé)** permet de configurer le lancement de l'application.

4. Enregistrez vos modifications.

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 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 (14.2)**, puis ouvrez les propriétés de l'application d'un double-clic.

7. Exécutez une des actions suivantes :

   - Si vous souhaitez lancez 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, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

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. Sélectionnez 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

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 klpsm.exe.

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`.

Pour quitter l'application via la ligne de commande, il faut activer la gestion externe des services système.

Lancement et arrêt de l'application depuis la ligne de commande

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.
   - **Suspendre** : la protection et le contrôle de l'ordinateur sont activés quand vous décidez de les rétablir.
4. Cliquez sur **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.

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.

- 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 l'application vers la stratégie.

- Transférer les paramètres de fonctionnement de Kaspersky Endpoint Security d'un ordinateur à l'autre (cf. instructions ci-après).

Exportation d'un fichier de configuration

À partir de la version 14.2 de Kaspersky Endpoint Security, le fichier de configuration exporté peut être chiffré. Le fichier de configuration pouvant contenir des identifiants, nous vous recommandons de le chiffrer. Vous ne pouvez pas modifier un fichier chiffré. Toute tentative de modification du fichier de configuration endommagera celui-ci.

Le chiffrement du fichier de configuration présente les caractéristiques suivantes :

- Kaspersky Endpoint Security permet d'importer des fichiers chiffrés uniquement dans l'interface utilisateur de l'application ou via la ligne de commande. Vous ne pouvez pas utiliser un tel fichier dans une console de Kaspersky Security Center pour configurer une stratégie ou installer l'application à distance. Si vous prévoyez d'ajouter le fichier à une stratégie ou à un paquet d'installation, ignorez l'étape de chiffrement du fichier.

- Il est impossible de récupérer le mot de passe d'un fichier chiffré.

- Les versions de Kaspersky Endpoint Security antérieures à la version 14.1 ne prennent pas en charge l'importation de fichiers de configuration chiffrés. Si vous prévoyez d'importer le fichier dans une version antérieure de l'application, ignorez l'étape de chiffrement du fichier.

Pour créer un fichier de configuration, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Gestion des paramètres**.
3. Cliquez sur **Exporter**.
4. Pour enregistrer le fichier de configuration, la protection par mot de passe doit être activée. L'utilisateur doit avoir l'autorisation **Exporter les paramètres**.
5. 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.

6. Si nécessaire, activez le commutateur **Chiffrer le fichier exporté** et saisissez le mot de passe de chiffrement du fichier de configuration.

   Enregistrez le mot de passe dans un espace de stockage sécurisé. Il est impossible de récupérer ce mot de passe.

7. Enregistrez le fichier.

L'application crée alors un fichier de configuration.

Importation d'un fichier de configuration

Lors de l'importation d'un fichier de configuration, Kaspersky Endpoint Security ne transfère pas les mots de passe des conteneurs crypto. Si vous utilisez l'authentification bidirectionnelle lors de la connexion aux serveurs, vous devez spécifier les mots de passe des conteneurs crypto depuis le début.

Pour importer les paramètres de fonctionnement de Kaspersky Endpoint Security depuis le fichier de configuration, procédez comme suit :

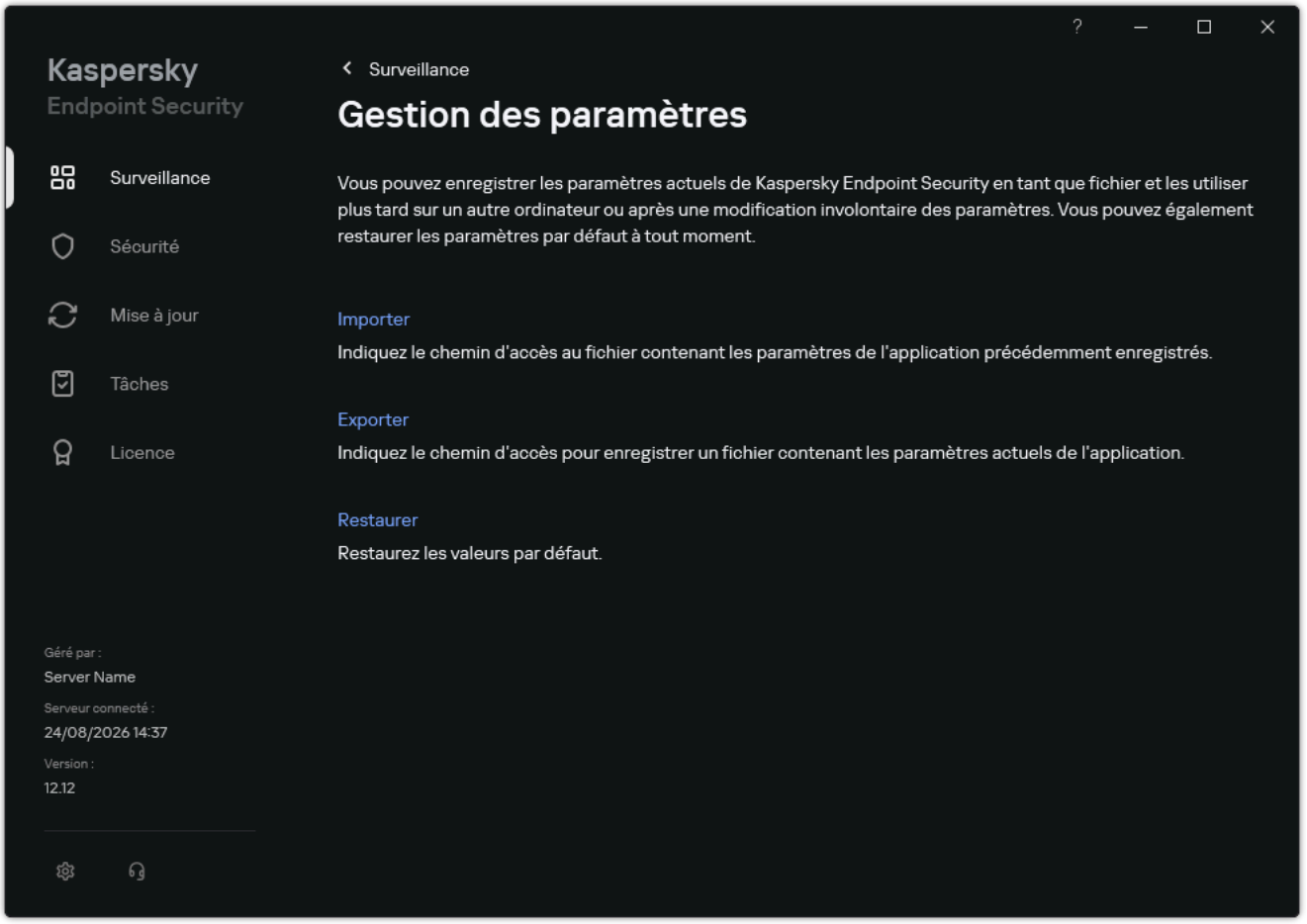
1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Gestion des paramètres**.
3. Cliquez sur **Importer**.
4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au fichier de configuration.

5. Si le fichier de configuration est chiffré, saisissez le mot de passe que vous avez indiqué lors de l'exportation.

> Si vous avez oublié le mot de passe de chiffrement du fichier de configuration, vous ne pouvez pas le récupérer. Dans ce cas, vous devez répéter les étapes d'exportation du fichier de configuration.

6. Ouvrez le fichier.

Tous les paramètres de Kaspersky Endpoint Security prendront les valeurs définies dans le fichier de configuration choisi.



Gestion des paramètres de l'application

Restauration des paramètres par défaut de l'application

Vous pouvez à tout moment restaurer les paramètres de fonctionnement de l'application recommandés par Kaspersky. Lorsque les paramètres sont restaurés, le niveau de protection **Recommandé** sera sélectionné pour tous les modules de la protection.

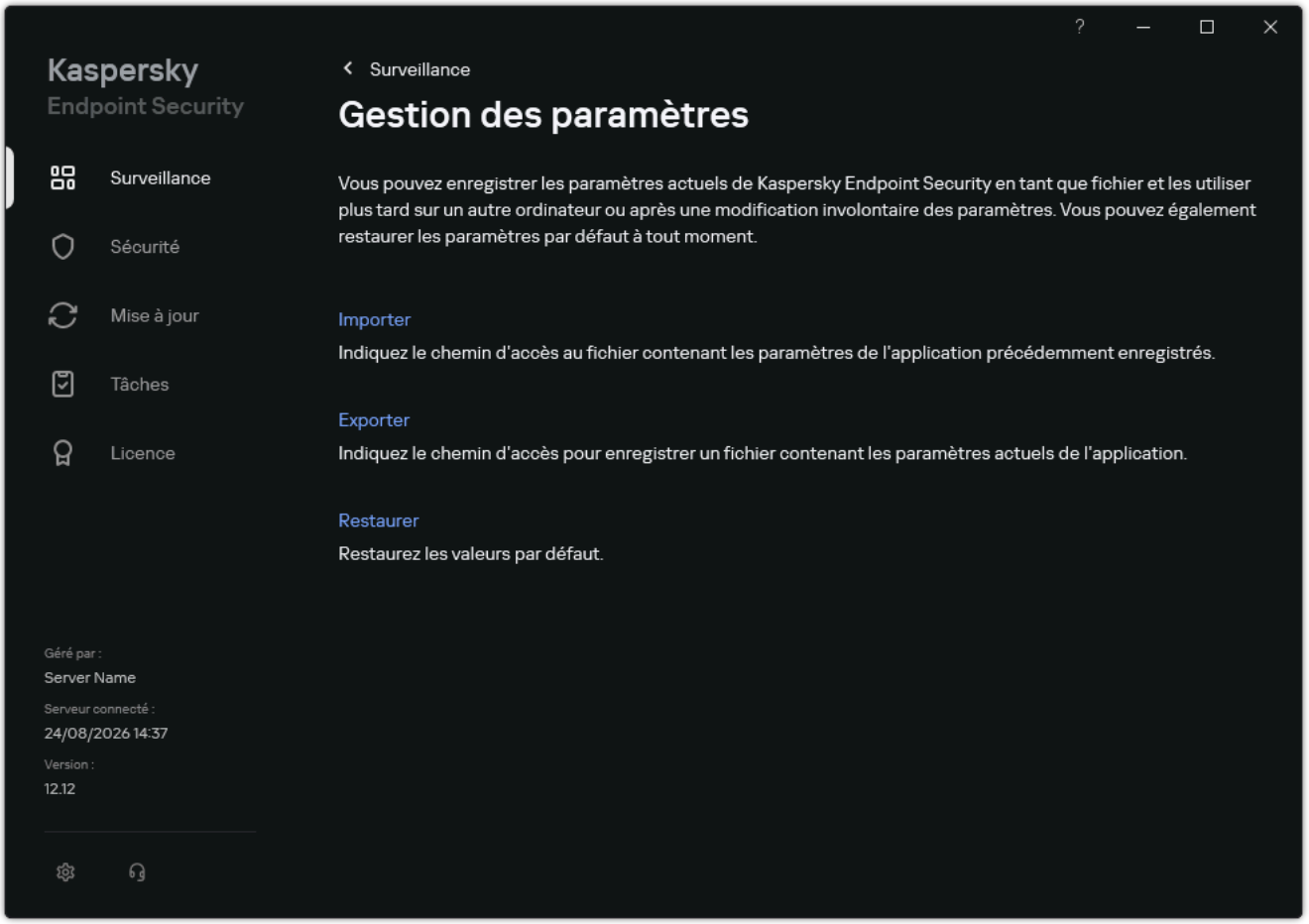
Pour restaurer les paramètres par défaut de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Gestion des paramètres**.

3. Cliquez sur **Restaurer**.

4. Enregistrez vos modifications.



Gestion des paramètres de l'application

Performances de Kaspersky Endpoint Security et compatibilité avec d'autres applications

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 d'analyse complète ;
- Tâche Analyse des zones critiques ;
- Tâche d'analyse personnalisée ;
- Tâche de vérification 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

La consommation des ressources de l'ordinateur lors de l'analyse de l'ordinateur peut augmenter la charge des sous-systèmes du processeur et du disque dur. 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 céder les ressources à d'autres applications.

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 la désinfection avancée 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 *Analyse des logiciels malveillants* à l'heure qui convient le mieux aux utilisateurs.

Activation et désactivation du mode d'économie d'énergie

Le *mode économie d'énergie* est une fonctionnalité qui réduit la charge pesant sur les ressources de l'ordinateur portable et prolonge l'autonomie de la batterie sans compromettre considérablement le niveau de sécurité. En mode d'économie d'énergie, l'application limite le lancement des tâches planifiées. Le mode d'économie d'énergie permet ainsi de trouver un juste équilibre entre le niveau de sécurité et l'autonomie de la batterie de l'ordinateur portable.

Quand le mode d'économie d'énergie est activé, les tâches suivantes ne sont pas exécutées quand un ordinateur est alimenté par la batterie, mais si elles sont programmées :

- *Analyse complète*.
- *Analyse des zones critiques*.
- *Analyse personnalisée*.
- *Vérification de l'intégrité de l'application*.
- *Analyse IOC*.
- *Mise à jour des bases et des modules d'application* (correctifs uniquement)

L'application ne suspend les mises à jour programmées de la base de données que lorsque l'ordinateur portable fonctionne sur batterie et que le niveau de charge de celle-ci est inférieur à 30 % (valeur par défaut). Vous pouvez modifier le niveau de charge minimal de la batterie en dessous duquel l'application suspend les mises à jour programmées des bases antivirus en modifiant le Registre (voir les instructions ci-dessous). Dans tous les autres cas, Kaspersky Endpoint Security met à jour ses bases de données selon la planification, que l'ordinateur portable soit branché sur secteur ou fonctionne sur batterie, ou que l'application soit en mode économie d'énergie.

Comment activer ou désactiver le mode d'économie d'énergie dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.

5. Dans le groupe **Performance**, utilisez la case **Reporter les tâches planifiées en cas d'alimentation par batterie** pour activer ou désactiver le mode d'économie d'énergie.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le mode d'économie d'énergie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Performances**.

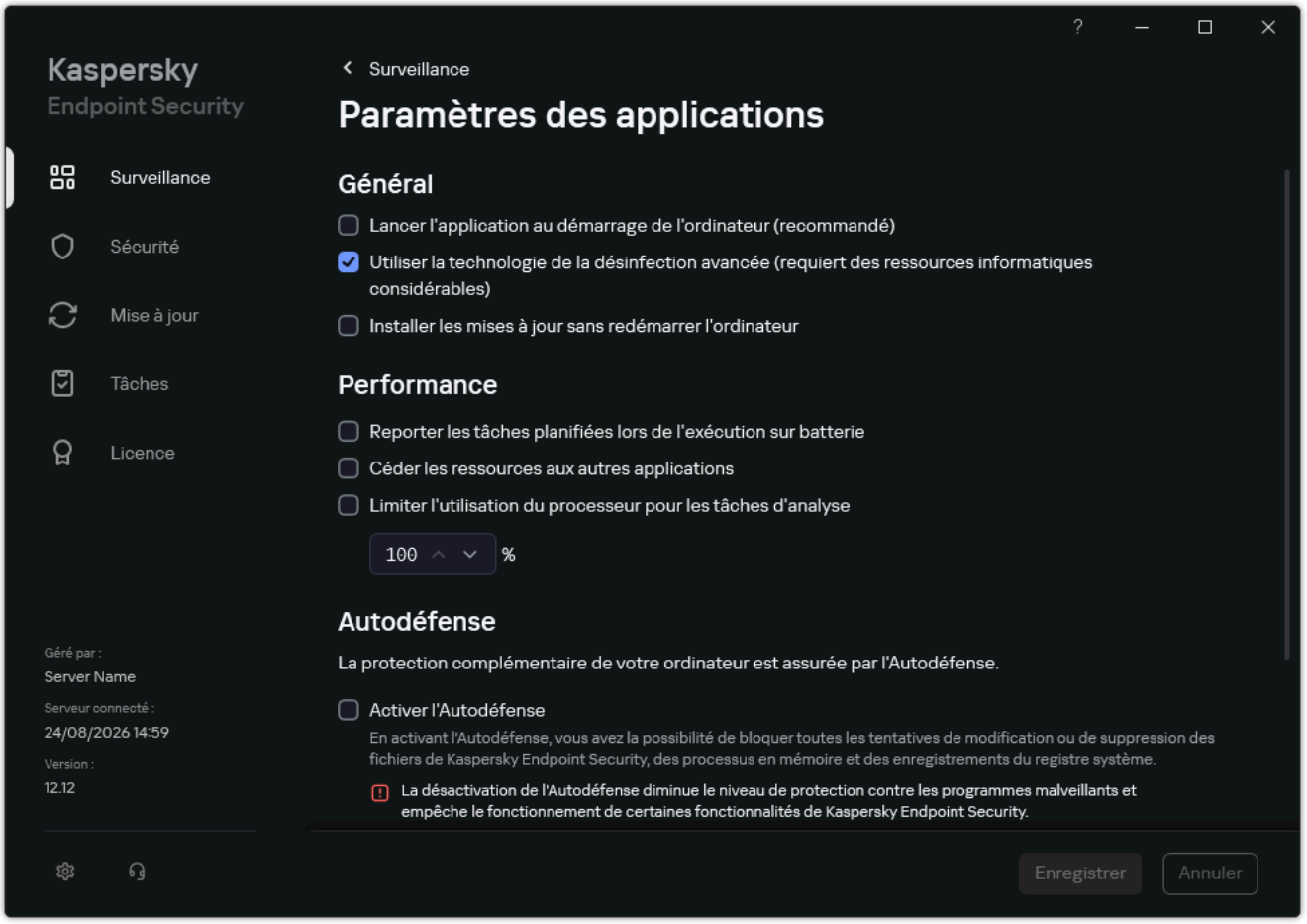
5. Dans le groupe **Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie**, utilisez la case **Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie (dépend du système d'exploitation)** pour activer ou désactiver le mode d'économie d'énergie.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le mode d'économie d'énergie 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. Dans le groupe **Performance**, utilisez la case **Reporter les tâches planifiées lors de l'exécution sur batterie** pour activer ou désactiver le mode d'économie d'énergie.

4. Enregistrez vos modifications.

Comment modifier le niveau de charge minimal en dessous duquel l'application suspend les mises à jour programmées des bases antivirus

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.14.2\environment`

   - Pour les systèmes d'exploitation 32 bits :
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Ouvrez `UpdaterAccumulatorThreshold` pour effectuer des modifications.

4. Spécifiez le niveau de charge minimal en dessous duquel l'application suspend les mises à jour programmées des bases antivirus.

Activation et désactivation du mode de transfert des ressources vers d'autres applications

La consommation des ressources de l'ordinateur par Kaspersky Endpoint Security lors de l'analyse d'un ordinateur peut augmenter la charge des sous-systèmes du processeur et du disque dur. Ce processus peut ralentir d'autres applications. Pour optimiser les performances, Kaspersky Endpoint Security propose un *mode de transfert des ressources vers d'autres applications*. Dans ce mode, le système d'exploitation peut réduire la priorité des tâches d'analyse de Kaspersky Endpoint Security lorsque la charge du processeur est élevée. Cette fonction permet de redistribuer les ressources du système d'exploitation à d'autres applications. Le processeur consacrera donc moins de ressources aux tâches d'analyse. Par conséquent, Kaspersky Endpoint Security mettra plus de temps à analyser l'ordinateur. Par défaut, l'application est configurée pour céder des ressources aux autres applications.

Comment activer ou désactiver la concession de ressources à d'autres applications dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.

4. Dans le groupe **Performance**, utilisez la case **Céder les ressources aux autres applications** pour activer ou désactiver la cession de ressources à d'autres applications.

5. Enregistrez vos modifications.

Comment activer ou désactiver la concession de ressources à d'autres applications dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Performances**.

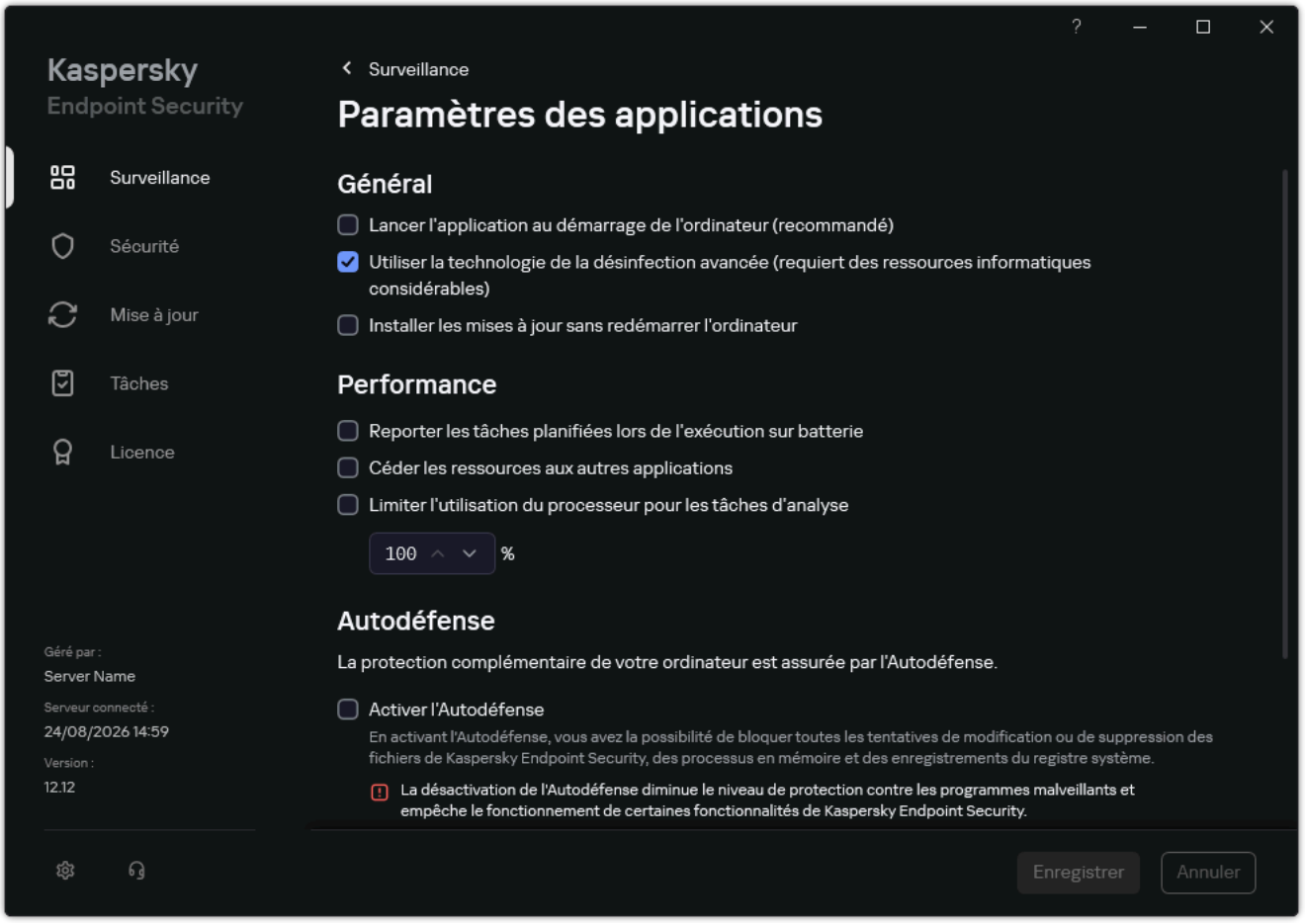
5. Dans le groupe **Céder les ressources aux autres applications**, utilisez le commutateur **Céder les ressources aux autres applications** pour activer ou désactiver la cession de ressources à d'autres applications.

6. Enregistrez vos modifications.

Comment activer ou désactiver la concession de ressources à d'autres applications 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. Dans le groupe **Performance**, utilisez la case **Céder les ressources aux autres applications** pour activer ou désactiver la cession de ressources à d'autres applications.

4. Enregistrez vos modifications.

Pratiques exemplaires pour optimiser les performances de Kaspersky Endpoint Security

Lors du déploiement de Kaspersky Endpoint Security for Windows, vous pouvez utiliser les recommandations suivantes pour configurer la protection de l'ordinateur et optimiser les performances. Pour en savoir plus sur les problèmes de performances informatiques, consultez la Base de connaissances du support technique.

Général

Configurez les paramètres généraux de l'application conformément aux recommandations suivantes :

1. Mettez à jour Kaspersky Endpoint Security vers la dernière version.

   Les versions plus récentes de l'application ont corrigé des erreurs, amélioré la stabilité et optimisé les performances.

2. Activez les modules de protection avec les paramètres par défaut.

   Les paramètres par défaut sont considérés comme optimaux. Ces paramètres sont recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources. Si nécessaire, vous pouvez rétablir les paramètres par défaut de l'application.

3. Activez les fonctionnalités d'optimisation des performances de l'application.

   L'application dispose de fonctionnalités d'optimisation des performances : mode d'économie d'énergie et concession de ressources à d'autres applications. Assurez-vous que ces options sont activées.

Analyse des logiciels malveillants sur les postes de travail

L'activation de l'Analyse en arrière-plan est recommandée pour l'analyse des logiciels malveillants sur les postes de travail. *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. Les paramètres d'analyse en arrière-plan sont considérés comme optimaux. Ces paramètres sont recommandés par les experts de Kaspersky. Ainsi, pour effectuer une analyse des logiciels malveillants sur l'ordinateur, vous pouvez utiliser uniquement le mode Analyse en arrière-plan sans utiliser d'autres tâches d'analyse.

Si l'analyse en arrière-plan ne répond pas à vos besoins, configurez la tâche *Analyse des logiciels malveillants* conformément aux recommandations suivantes :

1. Définissez une limite de consommation des ressources du processeur lorsque vous analysez l'ordinateur.

   Vous pouvez limiter l'utilisation du processeur par la tâche *Analyse des logiciels malveillants*. Pour ce faire, dans les paramètres de l'application, précisez le pourcentage de charge maximale du processeur pour tous les cœurs qui peuvent être utilisés lors de l'analyse de l'ordinateur. Il se peut alors que l'analyse de votre ordinateur prenne plus de temps.

2. Configurez la planification optimale de l'analyse de l'ordinateur.

Vous pouvez configurer la tâche de manière à ce qu'elle s'exécute lorsque l'ordinateur fonctionne sous une charge minimale. Par exemple, vous pouvez configurer la tâche de manière à ce qu'elle soit exécutée la nuit ou le week-end.

Si les utilisateurs éteignent l'ordinateur en dehors des heures de bureau, vous pouvez activer la fonction Wake-on-LAN. La fonctionnalité Wake-on-LAN autorise la mise sous tension à distance de l'ordinateur en envoyant un signal spécial sur le réseau local. Pour utiliser cette fonctionnalité, vous devez activer la fonctionnalité Wake-on-LAN dans les paramètres du BIOS. Vous pouvez également faire en sorte que l'ordinateur s'éteigne automatiquement une fois l'analyse terminée.

Si vous n'avez pas pu configurer une planification optimale de l'analyse, définissez des tâches à exécuter uniquement lorsque l'ordinateur est inactif. Kaspersky Endpoint Security lance la tâche d'analyse si l'ordinateur est verrouillé ou si l'écran de veille est activé. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue.

3. Définissez la zone d'analyse.

   Sélectionnez les objets suivants à analyser (ensemble minimum de zones d'analyse) :

   - Mémoire du noyau
   - Processus exécutés et objets de démarrage automatique
   - Secteurs d'amorçage
   - %systemroot% (n'inclut pas les sous-dossiers)
   - %systemroot%\System (n'inclut pas les sous-dossiers)
   - %systemroot%\System32 (n'inclut pas les sous-dossiers)
   - %systemroot%\System32\drivers (n'inclut pas les sous-dossiers)
   - %systemroot%\SysWOW64 (n'inclut pas les sous-dossiers)
   - %systemroot%\SysWOW64\drivers (n'inclut pas les sous-dossiers)

4. Activez les technologies iSwift et iChecker.

   - Technologie iSwift.

     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 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).

Vous pouvez activer les technologies iSwift et iChecker uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security. Vous ne pouvez pas activer ces technologies dans Kaspersky Security Center Web Console.

5. Désactivez l'analyse des archives protégées par un mot de passe.

   Si l'analyse des archives protégées par un mot de passe est activée, une demande de mot de passe s'affiche avant que l'archive soit analysée. Comme il est recommandé de planifier la tâche en dehors des heures de bureau, l'utilisateur ne peut pas saisir le mot de passe. Vous pouvez analyser manuellement les archives protégées par un mot de passe.

6. Désactivez le lancement simultané de plusieurs tâches d'analyse.

   Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur.

Analyse des logiciels malveillants sur les serveurs

Configurez la tâche *Analyse des logiciels malveillants* conformément aux recommandations suivantes :

1. Définissez une limite de consommation des ressources du processeur lorsque vous analysez l'ordinateur.

   Vous pouvez limiter l'utilisation du processeur par la tâche *Analyse des logiciels malveillants*. Pour ce faire, dans les paramètres de l'application, précisez le pourcentage de charge maximale du processeur pour tous les cœurs qui peuvent être utilisés lors de l'analyse de l'ordinateur. Il se peut alors que l'analyse de votre ordinateur prenne plus de temps.

2. Configurez la planification optimale de l'analyse de l'ordinateur.

   Vous pouvez configurer la tâche de manière à ce qu'elle s'exécute lorsque l'ordinateur fonctionne sous une charge minimale. Par exemple, vous pouvez configurer la tâche de manière à ce qu'elle soit exécutée la nuit ou le week-end.

3. Activez les technologies iSwift et iChecker.

   - Technologie iSwift.

     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 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).

Vous pouvez activer les technologies iSwift et iChecker uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security. Vous ne pouvez pas activer ces technologies dans Kaspersky Security Center Web Console.

4. Désactivez l'analyse des archives protégées par un mot de passe.

   Si l'analyse des archives protégées par un mot de passe est activée, une demande de mot de passe s'affiche avant que l'archive soit analysée. Comme il est recommandé de planifier la tâche en dehors des heures de bureau, l'utilisateur ne peut pas saisir le mot de passe. Vous pouvez analyser manuellement les archives protégées par un mot de passe.

5. Désactivez le lancement simultané de plusieurs tâches d'analyse.

   Kaspersky Endpoint Security mettra en file d'attente les nouvelles tâches d'analyse si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée 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 à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés.

Modifiez les paramètres de Kaspersky Security Network conformément aux recommandations suivantes :

1. Activez le mode étendu de 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.

2. Configurer Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) 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.

3. Activez le mode Cloud.

   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.

Analyse des logiciels malveillants

L'analyse des logiciels malveillants 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 Endpoint Security 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 recommandé d'utiliser une tâche d'analyse en arrière-plan au lieu d'une 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 système
- Objets chargés au lancement du système d'exploitation
- Sauvegarde du système d'exploitation
- Disques durs, disques amovibles et disques réseau
- N'importe quel fichier sélectionné

Analyse en arrière-plan

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 de l'application

Kaspersky Endpoint Security vérifie si les modules de l'application ont été endommagés ou modifiés.

Analyse de l'ordinateur

La recherche 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. 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 présente les tâches standard prédéfinies suivantes : *Analyse complète*, *Analyse des zones critiques* et *Analyse personnalisée*. Si votre organisation a déployé le système d'administration Kaspersky Security Center, vous pouvez créer une tâche *Analyse des logiciels malveillants* et configurer l'analyse.

Lancement d'une tâche d'analyse dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.

3. Sélectionnez la tâche d'analyse et ouvrez les propriétés de la stratégie d'un double-clic.

   Si nécessaire, créez la tâche *Analyse des logiciels malveillants*.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.

5. Configurez la tâche d'analyse (cf. tableau ci-après).

   Si nécessaire, configurez la planification des tâches d'analyse.

6. Enregistrez vos modifications.

7. Lancer la tâche de recherche de virus.

Kaspersky Endpoint Security commencera à analyser l'ordinateur. Si l'utilisateur a interrompu l'exécution de la tâche, par exemple en éteignant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où l'analyse a été interrompue.

Comment lancer une tâche d'analyse dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Configurez la tâche d'analyse (cf. tableau ci-après).

   Si nécessaire, configurez la planification des tâches d'analyse.

5. Enregistrez vos modifications.

6. Lancer la tâche de recherche de virus.

Kaspersky Endpoint Security commencera à analyser l'ordinateur. Si l'utilisateur a interrompu l'exécution de la tâche, par exemple en éteignant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où l'analyse a été interrompue.

Lancement d'une tâche d'analyse dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.

2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.

> Si la tâche d'analyse ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

> Dans l'interface de l'application, vous pouvez configurer uniquement les tâches d'analyse locales : *Analyse complète*, *Analyse des zones critiques*, *Analyse personnalisée*. Il n'est pas possible de configurer dans l'interface de l'application les tâches de groupe ajoutées via la Console de Kaspersky Security Center. Le bouton ⚙ ne s'affiche pas pour les tâches de groupe.

3. Configurez la tâche d'analyse (cf. tableau ci-après).

   Si nécessaire, configurez la planification des tâches d'analyse.

4. Enregistrez vos modifications.

5. Lancer la tâche de recherche de virus.

   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 **Arrêter**.

Pour optimiser les performances de Kaspersky Endpoint Security lors de l'analyse de l'ordinateur, vous pouvez gérer les paramètres avancés de la tâche *Analyse complète* et limiter l'utilisation des ressources du processeur.

Dans Kaspersky Security Center, vous pouvez également utiliser la tâche *Analyse en arrière-plan* au lieu de la tâche *Analyse complète* afin d'optimiser les performances de l'application. Le niveau de sécurité de l'ordinateur ne change pas. L'analyse en arrière-plan ne peut pas être configurée.

Par conséquent, Kaspersky Endpoint Security analyse l'ordinateur et, si une menace est détectée, exécute l'action configurée dans les paramètres de l'application. En général, l'application tente de désinfecter les fichiers infectés. En conséquence, les états suivants peuvent être attribués aux fichiers infectés :

- **Reporté**. Le fichier infecté n'a pas pu être désinfecté. L'application supprime le fichier infecté après le redémarrage de l'ordinateur.
- **Consigné dans le rapport**. Le fichier infecté n'a pas pu être désinfecté. L'application ajoute des informations sur les fichiers infectés détectés à la liste des menaces actives.
- **L'enregistrement n'est pas pris en charge** ou **Erreur d'écriture**. Le fichier infecté n'a pas pu être désinfecté. L'application n'a pas d'accès en écriture.
- **Traitement déjà exécuté**. L'application a détecté un fichier infecté plus tôt. L'application désinfecte ou supprime le fichier infecté après le redémarrage de l'ordinateur.

Paramètres d'analyse

Paramètre	Description
Niveau de sécurité	Kaspersky Endpoint Security peut utiliser différents groupes de paramètres pour lancer une analyse. Ces groupes de paramètres stockés dans l'application sont appelés *niveaux de sécurité* : • **Élevé**. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Minutieuse**. • **Recommandé**. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Moyenne**. • **Faible**. Kaspersky Endpoint Security analyse uniquement les formats de fichiers définis. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Superficielle**. 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.

Paramètre	Description
Action en cas de détection d'une menace	**Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. **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 échoue, 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, l'application 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.
Exécuter la désinfection avancée immédiatement *(disponible uniquement dans Kaspersky Security Center Console)*	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. Si la case est cochée, Kaspersky Endpoint Security désinfecte l'infection active dès qu'elle est détectée pendant l'exécution de la tâche de recherche de virus. Une fois que l'infection active est désinfectée, Kaspersky Endpoint Security redémarre l'ordinateur sans en avertir l'utilisateur. Si la case est décochée, Kaspersky Endpoint Security ne désinfecte pas l'infection active immédiatement après sa détection pendant l'exécution de la tâche de recherche de virus. Kaspersky Endpoint Security génère des événements d'infection active dans les rapports des applications locales et du côté de Kaspersky Security Center. L'infection active peut être désinfectée lorsque la tâche de recherche de virus est relancée et que la fonctionnalité de désinfection active est activée. De cette façon, l'administrateur système peut choisir le moment approprié pour lancer la procédure de désinfection de l'infection active et redémarrer ensuite les ordinateurs automatiquement.
Zone d'analyse	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, le disque dur, le disque amovible ou le disque, dossier ou fichier réseau. Dans Kaspersky Endpoint Security for Windows 12.12, la messagerie est exclue du champ d'application de l'analyse. L'analyse des messages entrants et sortants est effectuée par le module Protection contre les menaces par emails. Si vous utilisez une version antérieure du plug-in d'administration, l'application exclut les emails de la portée de l'analyse, même si la stratégie les inclut.
Planification de l'analyse	**Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. **Selon la planification**. Le mode d'exécution de la tâche d'analyse où l'application 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.
Après le démarrage de l'application, reporter le lancement de X minutes	Lancement différé de la tâche d'analyse après le lancement de l'application. Au démarrage du système d'exploitation, de nombreux processus sont en cours d'exécution, il est donc avantageux de reporter l'exécution de la tâche d'analyse au lieu de l'exécuter immédiatement après le lancement de Kaspersky Endpoint Security.
Lancer les tâches ignorées	Si la case est cochée, Kaspersky Endpoint Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.

Paramètre	Description
Exécuter uniquement lorsque l'ordinateur est inactif	Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.
Lancer l'analyse en tant que	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. 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 l'application et exécuter la tâche d'analyse sous le compte de cet utilisateur.
Types de fichiers	Les fichiers sans extension sont considérés par Kaspersky Endpoint Security comme des fichiers exécutables. L'application analyse toujours les fichiers exécutables, quel que soit le type de fichiers que vous avez sélectionné pour l'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, l'application 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, l'application analyse uniquement les fichiers infectables. Le format du fichier sera déterminé sur la base de son extension. Par défaut, Kaspersky Endpoint Security analyse les fichiers en fonction de leur format. L'analyse des fichiers en fonction de leur extension est moins sûre, car un fichier malveillant peut présenter une extension qui ne figure pas sur la liste des fichiers potentiellement infectables (par exemple, `.123`).
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 le fichier analysé pendant plus de X secondes	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.
Ne pas exécuter plusieurs tâches d'analyse en même temps	Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, vous avez planifié l'exécution de tâches d'analyse à 18 h 00 et à 20 h 00. Kaspersky Endpoint Security reportera la tâche d'analyse de 20 h 00 si celle prévue à 18 h 00 est toujours en cours d'exécution. L'application lancera une analyse une fois la tâche démarrée à 18 h 00 terminée. Cependant, Kaspersky Endpoint Security lance immédiatement une tâche d'analyse même si l'une des tâches d'analyse suivantes est en cours d'exécution : • Analyse des disques amovibles à la connexion. • Analyse depuis le menu contextuel. • Analyse des zones critiques qui a été lancée lors de la détection d'un indicateur de compromission (IoC). Si cette case est décochée, Kaspersky Endpoint Security vous permet d'exécuter plusieurs tâches d'analyse en même temps. L'exécution de plusieurs taches d'analyse nécessite davantage de ressources informatiques.
Analyser les archives	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les paquets de distribution	Analyse des paquets de distribution des applications tierces.
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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.

Paramètre	Description
Analyser les fichiers au format de messagerie	Analyse des fichiers au format de messagerie et de la base de données de messagerie. L'application analyse les fichiers PST et OST utilisés par les clients de messagerie MS Outlook et Windows Mail ainsi que les fichiers EML. Kaspersky Endpoint Security ne prend pas en charge la version 64 bits du client de messagerie Microsoft Outlook. Autrement dit, Kaspersky Endpoint Security n'analyse pas les fichiers Microsoft Outlook (fichiers PST et OST) si une version 64 bits de Microsoft Outlook est installée sur l'ordinateur, même si la messagerie est incluse dans la zone d'analyse. 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. Si la case est décochée, Kaspersky Endpoint Security analyse le fichier au format de messagerie comme un fichier unique. Lorsqu'un objet malveillant est détecté dans les fichiers PST ou OST, Kaspersky Endpoint Security le rend inoffensif conformément à l'action sélectionnée (par exemple, désinfection ou suppression du fichier). Si des objets malveillants sont détectés dans les fichiers d'autres clients de messagerie (par exemple, Mozilla Thunderbird), Kaspersky Endpoint Security ne désinfecte ni ne supprime ces fichiers afin d'éviter la suppression accidentelle de vos messages électroniques. Kaspersky Endpoint Security ajoute uniquement les informations relatives aux objets détectés à la liste des menaces actives. Vous devez prendre les mesures nécessaires pour supprimer les messages électroniques dont les pièces jointes contiennent des fichiers malveillants dans l'interface utilisateur de votre client de messagerie. Si, pour une raison quelconque, il est impossible de supprimer immédiatement les messages contenant des objets malveillants, vous pouvez traiter ces menaces dans l'interface utilisateur de Kaspersky Endpoint Security en ajoutant les objets détectés à la liste des exclusions de l'analyse.
Analyser les archives protégées par un mot de passe	Si la case est cochée, l'application 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. Si la case est décochée, l'application exclut de l'analyse les archives protégées par un mot de passe.
Ne pas décompresser les fichiers composés volumineux	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.
Machine learning et analyse sur la base de signature	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. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.
Analyse heuristique	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.
Technologie iSwift *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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 iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.
Technologie iChecker *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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 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.

Configuration de l'exécution de l'analyse des disques amovibles dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Tâches locales** → **Analyse des disques amovibles**.
4. Sélectionnez 'option **Analyse complète** ou **Analyse rapide** dans la liste **Action lorsqu'un disque amovible est connecté**.
5. Configurez les options avancées pour l'analyse des disques amovibles (cf. tableau ci-dessous).
6. Enregistrez vos modifications.

Configuration de l'exécution de l'analyse des disques amovibles dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse des disques amovibles**.
5. Utilisez le commutateur **Analyse des disques amovibles ACTIVÉE** pour activer ou désactiver le module.
6. Dans le groupe **Type d'analyse**, sélectionnez l'option **Analyse complète** ou **Analyse rapide**.
7. Configurez les options avancées pour l'analyse des disques amovibles (cf. tableau ci-dessous).
8. Enregistrez vos modifications.

Configuration de l'exécution de l'analyse des disques amovibles dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse 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. Configurez les options avancées pour l'analyse des disques amovibles (cf. tableau ci-dessous).

5. Enregistrez vos modifications.

Par conséquent, Kaspersky Endpoint Security exécute une analyse des disques amovibles pour les disques amovibles qui ne sont pas plus grands que la taille maximale définie. Si la tâche *Analyse des disques amovibles* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

Paramètres de la tâche Analyse des disques amovibles

Paramètre	Description
Type d'analyse	**Analyse complète**. Si cette option est sélectionnée, Kaspersky Endpoint Security analyse tous les fichiers à la connexion du disque amovible, y compris les fichiers imbriqués dans les objets composés, les archives, les paquets de distribution et les fichiers au format Office. Kaspersky Endpoint Security n'analyse pas les fichiers dans les formats de messagerie ou les archives protégées par mot de passe. **Analyse rapide**. Si cette option est sélectionnée, 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 (Mo)	Si la case est cochée, Kaspersky Endpoint Security exécute l'action sélectionnée sur les disques amovibles dont la taille est inférieure à la taille maximale définie. Si la taille du disque amovible dépasse la valeur configurée, Kaspersky Endpoint Security ignore l'analyse. Si la case est décochée, Kaspersky Endpoint Security exécute l'action sélectionnée sur les disques amovibles de toute taille.
Masquer la barre de progression de l'analyse	Si la case est cochée, Kaspersky Endpoint Security affiche la progression de l'analyse des disques amovibles dans une nouvelle fenêtre et dans la section **Tâches**. Si la case est décochée, Kaspersky Endpoint Security exécute l'analyse des disques amovibles en arrière-plan.
Empêcher les utilisateurs d'arrêter l'analyse	Si cette case est cochée, pour la tâche d'analyse des disques amovibles dans l'interface locale de Kaspersky Endpoint Security, le bouton **Arrêter** dans la section **Tâches** et le bouton **Arrêter** dans la fenêtre d'analyse des disques amovibles ne sont pas disponibles.

Analyse en arrière-plan

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.

Pour économiser les ressources de l'ordinateur, il est recommandé d'utiliser une tâche d'analyse en arrière-plan au lieu d'une tâche d'analyse complète. Le niveau de sécurité de l'ordinateur ne change pas. Ces tâches présentent la même zone d'analyse. Pour optimiser la charge exercée sur l'ordinateur, l'application n'exécute pas simultanément une tâche d'analyse complète et une tâche d'analyse en arrière-plan. Si vous avez déjà exécuté une tâche d'analyse complète, Kaspersky Endpoint Security ne lancera pas de tâche d'analyse en arrière-plan pendant sept jours après la fin de la tâche d'analyse complète.

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.

Activation des analyses en arrière-plan dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Tâches locales** → **Analyse en arrière-plan**.
4. Utilisez la case **Activer l'Analyse en arrière-plan** pour activer ou désactiver les analyses en arrière-plan.
5. Enregistrez vos modifications.

Activation d'une analyse en arrière-plan dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Sous **Analyse en arrière-plan**, utilisez le commutateur **Analyse en arrière-plan ACTIVÉE** pour activer ou désactiver l'analyse en arrière-plan.
6. Enregistrez vos modifications.

Activation des analyses en arrière-plan dans l'interface de l'application

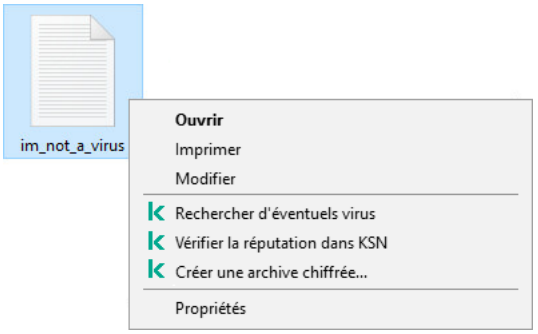
1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.
3. Utilisez le commutateur **Analyse en arrière-plan** pour activer ou désactiver les analyses en arrière-plan.
4. Enregistrez vos modifications.

Si la tâche *Analyse en arrière-plan* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

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

Configuration de l'analyse depuis le menu contextuel de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Tâches locales** → **Analyse depuis le menu contextuel**.
4. Configurer l'analyse depuis le menu contextuel (cf. tableau ci-dessous).
5. Enregistrez vos modifications.

Configuration de l'analyse depuis le menu contextuel dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Sous **Analyse depuis le menu contextuel**, configurez l'analyse depuis le menu contextuel (cf. tableau ci-dessous).
6. Enregistrez vos modifications.

Configuration de l'analyse depuis le menu contextuel dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.
3. Configurer l'analyse depuis le menu contextuel (cf. tableau ci-dessous).
4. Enregistrez vos modifications.

Si la tâche *Analyse depuis le menu contextuel* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

Paramètres de la tâche Analyse depuis le menu contextuel

Paramètre	Description
Niveau de sécurité	Kaspersky Endpoint Security peut utiliser différents groupes de paramètres pour lancer une analyse. Ces groupes de paramètres stockés dans l'application sont appelés *niveaux de sécurité* : • **Élevé**. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Minutieuse**. • **Recommandé**. Kaspersky Endpoint Security analyse tout type de fichiers. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Moyenne**. • **Faible**. Kaspersky Endpoint Security analyse uniquement les formats de fichiers définis. Lors de l'analyse des fichiers composés, l'application analyse les archives, les paquets de distribution, les fichiers aux formats Office, mais pas les archives protégées par mot de passe. Quand ce niveau de sécurité est défini, l'application utilise l'analyse heuristique avec le niveau de détail **Superficielle**.
Action en cas de détection d'une menace	**Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. **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 échoue, 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.
Types de fichiers	Les fichiers sans extension sont considérés par Kaspersky Endpoint Security comme des fichiers exécutables. L'application analyse toujours les fichiers exécutables, quel que soit le type de fichiers que vous avez sélectionné pour l'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, l'application 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, l'application analyse uniquement les fichiers infectables. Le format du fichier sera déterminé sur la base de son extension. Par défaut, Kaspersky Endpoint Security analyse les fichiers en fonction de leur format. L'analyse des fichiers en fonction de leur extension est moins sûre, car un fichier malveillant peut présenter une extension qui ne figure pas sur la liste des fichiers potentiellement infectables (par exemple, `.123`).
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 le fichier analysé pendant plus de X secondes	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

Paramètre	Description
Analyser les archives	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Analyser les fichiers au format de messagerie	Analyse des fichiers au format de messagerie et de la base de données de messagerie. L'application analyse les fichiers PST et OST utilisés par les clients de messagerie MS Outlook et Windows Mail ainsi que les fichiers EML. Kaspersky Endpoint Security ne prend pas en charge la version 64 bits du client de messagerie Microsoft Outlook. Autrement dit, Kaspersky Endpoint Security n'analyse pas les fichiers Microsoft Outlook (fichiers PST et OST) si une version 64 bits de Microsoft Outlook est installée sur l'ordinateur, même si la messagerie est incluse dans la zone d'analyse. 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. Si la case est décochée, Kaspersky Endpoint Security analyse le fichier au format de messagerie comme un fichier unique. Lorsqu'un objet malveillant est détecté dans les fichiers PST ou OST, Kaspersky Endpoint Security le rend inoffensif conformément à l'action sélectionnée (par exemple, désinfection ou suppression du fichier). Si des objets malveillants sont détectés dans les fichiers d'autres clients de messagerie (par exemple, Mozilla Thunderbird), Kaspersky Endpoint Security ne désinfecte ni ne supprime ces fichiers afin d'éviter la suppression accidentelle de vos messages électroniques. Kaspersky Endpoint Security ajoute uniquement les informations relatives aux objets détectés à la liste des menaces actives. Vous devez prendre les mesures nécessaires pour supprimer les messages électroniques dont les pièces jointes contiennent des fichiers malveillants dans l'interface utilisateur de votre client de messagerie. Si, pour une raison quelconque, il est impossible de supprimer immédiatement les messages contenant des objets malveillants, vous pouvez traiter ces menaces dans l'interface utilisateur de Kaspersky Endpoint Security en ajoutant les objets détectés à la liste des exclusions de l'analyse.
Analyser les archives protégées par un mot de passe	Si la case est cochée, l'application 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. Si la case est décochée, l'application exclut de l'analyse les archives protégées par un mot de passe.
Ne pas décompresser les fichiers composés volumineux	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.
Machine learning et analyse sur la base de signature	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. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.
Analyse heuristique	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.
Technologie iSwift	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 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).

Vérification de l'intégrité de l'application

Kaspersky Endpoint Security vérifie si les modules 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 de l'application* sert à vérifier les fichiers de l'application. Exécutez la tâche *Vérification de l'intégrité de l'application* si Kaspersky Endpoint Security a détecté un objet malveillant et ne l'a pas neutralisé.

Vous pouvez créer la tâche *Vérification de l'intégrité de l'application* dans Kaspersky Security Center 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.

Lancement de la vérification de l'intégrité d'une application via la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Vérification de l'intégrité de l'application**.

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. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Vérification de l'intégrité de l'application**.

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 **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. 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.

Exécution d'une vérification de l'intégrité dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Vérification de l'intégrité de l'application*, puis cliquez sur **Lancer**.

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. Si la tâche *Vérification de l'intégrité de l'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

Paramètres de la tâche de vérification de l'intégrité

Paramètre	Description
Planification de l'analyse	**Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. **Selon la planification**. Le mode d'exécution de la tâche d'analyse où l'application 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.
Lancer les tâches ignorées	Si la case est cochée, Kaspersky Endpoint Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Exécuter uniquement lorsque l'ordinateur est inactif	Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.

Modification de la zone d'analyse

La *Zone d'analyse* est une liste de chemins d'accès aux dossiers et aux chemins que Kaspersky Endpoint Security analyse lors de l'exécution de la tâche. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.

> Pour modifier la zone d'analyse, nous vous recommandons d'utiliser la tâche *Analyse personnalisée*. Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse des tâches *Analyse complète* et *Analyse des zones critiques*.

Kaspersky Endpoint Security dispose des objets prédéfinis suivants dans la zone d'analyse :

- **Mémoire système**.
- **Processus exécutés et objets de démarrage automatique**.

  Mémoire occupée par les processus et les fichiers exécutables des applications qui sont exécutés au démarrage du système.
- **Secteurs d'amorçage**.

  Secteurs d'amorçage des disques durs et des disques amovibles.
- **Sauvegarde système**.

  Contenu du dossier Stockage des sauvegardes système.
- **Tous les appareils externes**.
- **Tous les disques durs**.
- **Tous les disques réseau**.

  > Dans Kaspersky Endpoint Security for Windows 12.12, la messagerie est exclue du champ d'application de l'analyse. L'analyse des messages entrants et sortants est effectuée par le module Protection contre les menaces par emails. Si vous utilisez une version antérieure du plug-in d'administration, l'application exclut les emails de la portée de l'analyse, même si la stratégie les inclut.

  > Nous vous recommandons de créer une tâche d'analyse distincte pour analyser les disques réseau ou les dossiers partagés. Dans les paramètres de la tâche *Analyse des logiciels malveillants*, définissez un utilisateur qui dispose d'un accès en écriture à ce disque ; cette action est nécessaire pour atténuer les menaces détectées. Si le serveur sur lequel se trouve le disque réseau dispose de ses propres outils de sécurité, n'exécutez pas la tâche d'analyse pour ce disque. Vous pouvez ainsi éviter de vérifier l'objet deux fois et améliorer les performances du serveur.

Pour exclure des dossiers ou des fichiers de la zone d'analyse, ajoutez le dossier ou le fichier à la zone de confiance.

Modification d'une zone d'analyse dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Tâches**.

3. Sélectionnez la tâche d'analyse et ouvrez les propriétés de la stratégie d'un double-clic.

   Si nécessaire, créez la tâche *Analyse des logiciels malveillants*.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.

5. Dans la section **Zone d'analyse**, cliquez sur **Paramètres**.

6. Dans la fenêtre qui s'ouvre, sélectionnez les objets que vous souhaitez ajouter à la zone d'analyse ou exclure de celle-ci.

7. Si vous voulez ajouter un nouvel objet à la zone d'analyse, procédez comme suit :

   a. Cliquez sur **Ajouter**.

   b. Dans le champ **Objet**, saisissez le chemin d'accès au dossier ou au fichier.

      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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

      Vous pouvez utiliser des masques n'importe où dans un chemin de fichier ou de dossier. Par exemple, si vous souhaitez que la zone d'analyse inclue le dossier Téléchargements pour tous les comptes sur l'ordinateur, saisissez le masque `C:\Users\*\Downloads\`.

      L'objet **Cet ordinateur** dans la liste des ressources de fichiers de l'ordinateur contient les objets suivants : **Tous les disques durs**, **Tous les disques réseau** et **Tous les disques amovibles**.

   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. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Modification d'une zone d'analyse dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre. Si nécessaire, créez la tâche *Analyse des logiciels malveillants*.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Zone d'analyse**, sélectionnez les objets que vous souhaitez ajouter à la zone d'analyse ou exclure de celle-ci.

5. Si vous voulez ajouter un nouvel objet à la zone d'analyse, procédez comme suit :

   a. Cliquez sur **Ajouter**.

   b. Saisissez le chemin d'accès au dossier ou au fichier.

      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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

      Vous pouvez utiliser des masques n'importe où dans un chemin de fichier ou de dossier. Par exemple, si vous souhaitez que la zone d'analyse inclue le dossier Téléchargements pour tous les comptes sur l'ordinateur, saisissez le masque `C:\Users\*\Downloads\`.

   Dans la zone d'analyse, vous pouvez exclure un objet des analyses sans le supprimer de la liste des objets. Pour ce faire, mettez le commutateur situé à côté en position d'arrêt.

6. Enregistrez vos modifications.

Modification d'une zone d'analyse dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Analyse personnalisée*, puis cliquez sur **Sélectionner**.

   Vous pouvez également modifier la zone d'analyse pour d'autres tâches. Les experts de Kaspersky recommandent de ne pas modifier la zone d'analyse des tâches *Analyse complète* et *Analyse des zones critiques*.

3. Dans la fenêtre qui s'ouvre, sélectionnez les objets que vous souhaitez ajouter à la zone d'analyse.

4. Enregistrez vos modifications.

Si la tâche d'analyse ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

Exécution d'une analyse programmée

La recherche de programmes malveillants à l'aide de la tâche *Recherche de programmes malveillants* peut prendre beaucoup de temps et augmenter la consommation de ressources système par Kaspersky Endpoint Security. Il est donc recommandé de choisir le moment le plus approprié pour exécuter la tâche, afin de réduire au minimum son impact sur les performances des autres applications.

Par exemple, si les employés de votre entreprise ont une planification fixe, vous pouvez configurer une analyse des ordinateurs de manière à ce qu'elle s'exécute la nuit ou le week-end. 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 d'analyse ignorée dès que cela est possible. Cette fonction doit être utilisée avec prudence, car elle peut ralentir les applications sur l'ordinateur de l'utilisateur lorsque celui-ci est démarré le matin.

Si vous ne pouvez pas définir un calendrier d'analyse optimal adapté à vos besoins, vous pouvez configurer l'analyse de manière à ce qu'elle s'exécute dès qu'une des conditions spéciales suivantes est remplie :

- Après une mise à jour des bases de données.

  Kaspersky Endpoint Security analyse l'ordinateur avec les bases de données de signatures mises à jour.

- Après le lancement de l'application.

  Kaspersky Endpoint Security lance une analyse de l'ordinateur après un délai défini suivant le démarrage de l'application. Au démarrage du système d'exploitation, de nombreux processus sont en cours d'exécution, il est donc avantageux de reporter l'exécution de la tâche d'analyse au lieu de l'exécuter immédiatement après le lancement de Kaspersky Endpoint Security.

- Fonctionnalité Wake-on-LAN.

  Kaspersky Endpoint Security exécute une analyse de l'ordinateur selon la planification prévue, même si l'ordinateur est éteint. Pour ce faire, l'application utilise la fonctionnalité Wake-on-LAN du système d'exploitation. La fonctionnalité Wake-on-LAN autorise la mise sous tension à distance de l'ordinateur en envoyant un signal spécial sur le réseau local. Pour utiliser cette fonctionnalité, vous devez activer la fonctionnalité Wake-on-LAN dans les paramètres du BIOS.

  Vous pouvez configurer l'exécution de l'analyse à l'aide de la fonctionnalité Wake-on-LAN uniquement pour la tâche *Analyse des logiciels malveillants* de Kaspersky Security Center. Il est impossible d'activer la fonctionnalité Wake-on-LAN pour analyser l'ordinateur dans l'interface de l'application.

- Lorsque l'ordinateur est inactif.

  Kaspersky Endpoint Security effectue une analyse de l'ordinateur selon la planification prévue lorsque l'écran de veille est actif ou que l'écran est verrouillé. Si l'utilisateur déverrouille l'ordinateur, Kaspersky Endpoint Security interrompt l'analyse. Dans ce cas, l'Analyse complète peut durer plusieurs jours.

- Quand la tâche a été ignorée.

  Kaspersky Endpoint Security exécute la tâche ignorée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur.

Configuration d'une planification d'analyse dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

4. Configurez la planification 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.

6. Enregistrez vos modifications.

Configuration d'une planification d'analyse dans l'interface de l'application

Vous pouvez configurer la planification d'analyse uniquement si aucune stratégie n'est appliquée à l'ordinateur. Pour les ordinateurs sous contrat, vous pouvez configurer la planification des tâches *Analyse des logiciels malveillants* dans Kaspersky Security Center.

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.

2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.

   Vous pouvez configurer une planification pour l'exécution d'une analyse complète, d'une analyse des zones critiques ou d'une vérification de l'intégrité. Vous pouvez lancer une analyse personnalisée uniquement manuellement.

3. Cliquez sur **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.

6. Enregistrez vos modifications.

Paramètres de planification de l'analyse

Paramètre	Description
Planification de l'analyse	**Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. **Selon la planification**. Le mode d'exécution de la tâche d'analyse où l'application 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.
Après le démarrage de l'application, reporter le lancement de X minutes	Lancement différé de la tâche d'analyse après le lancement de l'application. Au démarrage du système d'exploitation, de nombreux processus sont en cours d'exécution, il est donc avantageux de reporter l'exécution de la tâche d'analyse au lieu de l'exécuter immédiatement après le lancement de Kaspersky Endpoint Security.
Lancer les tâches ignorées	Si la case est cochée, Kaspersky Endpoint Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.

Paramètre	Description
Exécuter uniquement lorsque l'ordinateur est inactif	Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.
Adopter un décalage aléatoire automatique pour les lancements de tâche *(disponible uniquement dans Kaspersky Security Center Console)*	Si la case est cochée, la tâche n'est pas exécutée strictement selon la planification, mais de manière aléatoire dans un certain intervalle, c'est-à-dire que les heures de lancement de la tâche sont étalées. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. La plage des heures de lancement aléatoires est calculée automatiquement lors de la création de la tâche, en fonction du nombre d'ordinateurs auxquels la tâche est assignée. Par la suite, la tâche est toujours exécutée à son heure de lancement calculée. Toutefois, lorsque les paramètres de la tâche sont modifiés ou que la tâche est exécutée manuellement, l'heure de lancement calculée change. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Arrêter la tâche si elle prend plus de (min.) *(disponible uniquement dans Kaspersky Security Center Console)*	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue. Pour réduire le temps d'exécution de la tâche, vous pouvez, par exemple, configurer la zone d'analyse ou optimiser l'analyse.
Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche (min.) *(disponible uniquement dans Kaspersky Security Center Console)*	Si la case est cochée, le système d'exploitation de l'ordinateur dispose d'un délai déterminé pour terminer le lancement avant l'exécution de la tâche. Le délai par défaut est de 5 minutes. Cochez la case si vous souhaitez exécuter la tâche sur tous les ordinateurs, y compris sur les ordinateurs éteints.
Arrêter les appareils après la fin de la tâche *(disponible uniquement dans Kaspersky Security Center Console)*	Si cette case est cochée, l'ordinateur s'éteint une fois la tâche terminée. Par exemple, vous pouvez activer cette fonctionnalité pour analyser l'ordinateur le vendredi après les heures de travail. Une fois la tâche terminée, l'application éteint l'ordinateur pour le week-end.
Suspendre la tâche	Vous pouvez définir un intervalle de temps pendant lequel l'exécution d'une tâche précédemment planifiée sera suspendue. Une fois la période définie écoulée, la tâche reprend. Cela peut s'avérer nécessaire, par exemple, pour limiter l'impact de Kaspersky Endpoint Security sur les performances de votre ordinateur pendant les périodes de forte utilisation.
Désactiver la planification à partir du	Si la case est cochée, Kaspersky Endpoint Security arrêtera l'exécution de la tâche planifiée à partir de la date indiquée. La tâche sera définie en mode **Manuellement**.

Exécution d'une analyse en tant qu'utilisateur différent

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. 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 l'application et exécuter la tâche d'analyse sous le compte de cet utilisateur.

Vous pouvez exécuter les analyses suivantes en tant qu'utilisateur différent :

- Analyse des zones critiques.
- Analyse complète.

- Analyse personnalisée.
- Analyse depuis le menu contextuel.

Vous ne pouvez pas configurer les droits d'utilisateurs pour exécuter une tâche Analyse des disques amovibles, Analyse en arrière-plan ou Vérification de l'intégrité.

Exécution d'une analyse en tant qu'utilisateur différent 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 **Tâches**.
4. Sélectionnez la tâche d'analyse et ouvrez les propriétés de la stratégie d'un double-clic.
5. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Compte utilisateur**.
6. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter une tâche d'analyse.
7. Enregistrez vos modifications.

Exécution d'une analyse en tant qu'utilisateur différent dans Web Console ou dans Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre.
3. Sélectionnez l'onglet **Configuration**.
4. Cliquez sur le bouton **Configuration** dans le groupe **Compte**.
5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter une tâche d'analyse.
6. Enregistrez vos modifications.

Exécution d'une analyse en tant qu'utilisateur différent dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.
3. Dans les propriétés de la tâche, sélectionnez **Paramètres avancés** → **Lancer l'analyse en tant que**.
4. Dans la fenêtre qui s'ouvre, saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter une tâche d'analyse.
5. Enregistrez vos modifications.

Si la tâche d'analyse ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

Optimisation de l'analyse

Limiter l'utilisation du processeur lors de l'analyse de l'ordinateur

Vous pouvez limiter l'utilisation du processeur par la tâche *Analyse des logiciels malveillants*. Il se peut alors que l'analyse de votre ordinateur prenne plus de temps.

Comment limiter l'utilisation du processeur lors de l'analyse de l'ordinateur dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Sous **Performance**, cochez la case **Limiter l'utilisation du processeur pour les tâches d'analyse** et saisissez la valeur moyenne de consommation des ressources du processeur en pourcentage.
5. Enregistrez vos modifications.

Comment limiter l'utilisation du processeur lors de l'analyse de l'ordinateur dans la Web Console

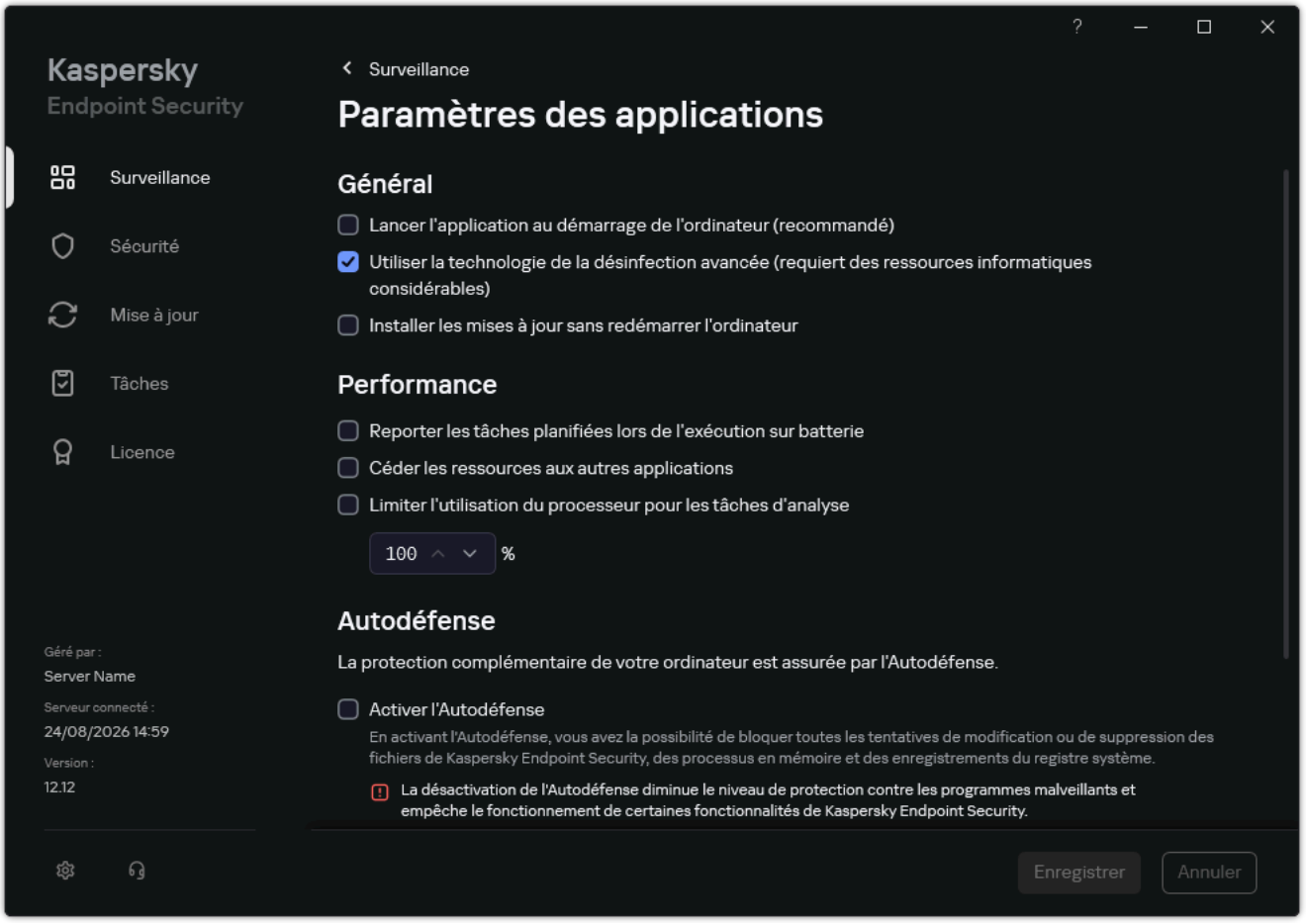
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Performances**.
5. Sous **Limitation de l'utilisation du processeur pour les tâches d'analyse**, définissez le commutateur sur **Limiter l'utilisation du processeur pour les tâches d'analyse** et saisissez la valeur moyenne de consommation des ressources du processeur en pourcentage.
6. Enregistrez vos modifications.

Comment limiter l'utilisation du processeur lors de l'analyse de l'ordinateur 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. Sous **Performance**, cochez la case **Limiter l'utilisation du processeur pour les tâches d'analyse** et saisissez la valeur moyenne de consommation des ressources du processeur en pourcentage.

4. Enregistrez vos modifications.

Configuration des paramètres de tâche avancés pour Analyse des logiciels malveillants.

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).

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.

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.

Optimisation des analyses dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Tâches**.

3. Sélectionnez la tâche d'analyse et ouvrez les propriétés de la stratégie d'un double-clic.

   Si nécessaire, créez la tâche *Analyse des logiciels malveillants*.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.

   La fenêtre contenant les paramètres de recherche de virus s'ouvre.

6. Dans le groupe **Optimisation**, configurez les paramètres d'analyse :

   - **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.

     Vous pouvez également configurer l'analyse des nouveaux fichiers par type. Par exemple, vous pouvez analyser tous les paquets de distribution et analyser uniquement les nouvelles archives et les fichiers au format Office.

   - **Ignorer les fichiers si l'analyse dure plus de X s**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

   - **Ne pas exécuter plusieurs tâches d'analyse en même temps**. Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, vous avez planifié l'exécution de tâches d'analyse à 18 h 00 et à 20 h 00. Kaspersky Endpoint Security reportera la tâche d'analyse de 20 h 00 si celle prévue à 18 h 00 est toujours en cours d'exécution. L'application lancera une analyse une fois la tâche démarrée à 18 h 00 terminée.

7. Cliquez sur **Avancé**.

   Cette action permet d'ouvrir la fenêtre des paramètres d'analyse des fichiers composés.

8. Dans le groupe **Limite selon la taille**, cochez la case **Ne pas décompresser les fichiers composés volumineux**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

   > Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.

9. Cliquez sur **OK**.

10. Rendez-vous dans l'onglet **Avancé**.

11. 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 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 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).

12. Enregistrez vos modifications.

Comment optimiser les analyses dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche d'analyse.

   La fenêtre des propriétés de la tâche s'ouvre. Si nécessaire, créez la tâche *Analyse des logiciels malveillants*.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans le groupe **Action en cas de détection d'une menace**, cochez la case **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.

   Vous pouvez également configurer l'analyse des nouveaux fichiers par type. Par exemple, vous pouvez analyser tous les paquets de distribution et analyser uniquement les nouvelles archives et les fichiers au format Office.

5. Dans le groupe **Optimisation de l'analyse**, cochez la case **Ne pas décompresser les fichiers composés volumineux**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

   > Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.

6. Cochez la case **Ne pas exécuter plusieurs tâches d'analyse en même temps**. Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, vous avez planifié l'exécution de tâches d'analyse à 18 h 00 et à 20 h 00. Kaspersky Endpoint Security reportera la tâche d'analyse de 20 h 00 si celle prévue à 18 h 00 est toujours en cours d'exécution. L'application lancera une analyse une fois la tâche démarrée à 18 h 00 terminée.

7. Dans le groupe **Paramètres avancés**, cochez la case **Ignorer un fichier si son analyse prend plus de (secondes)**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

8. Enregistrez vos modifications.

Optimisation des analyses dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Tâches**.

2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche d'analyse et cliquez sur le bouton ⚙.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Optimisation**, configurez les paramètres d'analyse :

   - **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.

     Vous pouvez également configurer l'analyse des nouveaux fichiers par type. Par exemple, vous pouvez analyser tous les paquets de distribution et analyser uniquement les nouvelles archives et les fichiers au format Office.

   - **Ignorer le fichier analysé pendant plus de X secondes**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

   - **Ne pas exécuter plusieurs tâches d'analyse en même temps**. Retarder les tâches d'analyse planifiées si une analyse planifiée lancée précédemment est toujours en cours. Kaspersky Endpoint Security mettra en file d'attente les tâches d'analyse planifiées si l'analyse en cours se poursuit. Cette mesure permet d'optimiser la charge exercée sur l'ordinateur. Par exemple, vous avez planifié l'exécution de tâches d'analyse à 18 h 00 et à 20 h 00. Kaspersky Endpoint Security reportera la tâche d'analyse de 20 h 00 si celle prévue à 18 h 00 est toujours en cours d'exécution. L'application lancera une analyse une fois la tâche démarrée à 18 h 00 terminée.

5. Dans le groupe **Limite selon la taille**, cochez la case **Ne pas décompresser les fichiers composés volumineux**. Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

   Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.

6. 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 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 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).

7. Enregistrez vos modifications.

Si la tâche d'analyse ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

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 fonctionnalités des mise à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) peuvent ne pas être disponibles dans le logiciel aux États-Unis.

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.

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.

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 concernant l'état actuel des bases de données de Kaspersky Endpoint Security sont affichées dans la fenêtre principale de l'application ou dans l'infobulle que vous voyez lorsque vous passez le curseur sur l'icône de l'application dans la zone de notification.

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.

Si l'application fonctionne en mode Light Agent, la mise à jour des bases et des modules de l'application doit faire l'objet de considérations particulières.

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 :

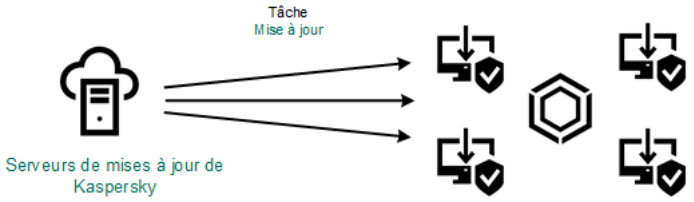
- Bases antivirus. Les bases antivirus contiennent les bases des signatures des programmes malveillants, la description des attaques réseau, les bases des adresses Internet malveillantes et de phishing, les bases des bannières, les bases antispam et d'autres données.

- 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 *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

2. Chargement du paquet de mises à jour dans un dossier partagé (facultatif).

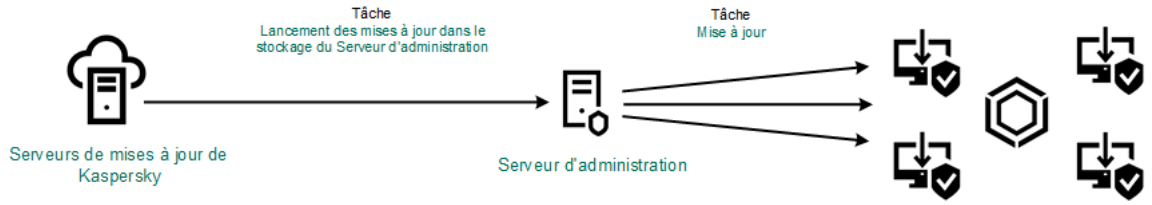
   Le chargement du paquet de mise à jour dans le dossier partagé peut s'opérer d'une des manières suivantes :

   - À l'aide de la tâche *Mise à jour des bases et des modules d'application* de Kaspersky Endpoint Security. La tâche est prévue pour un des ordinateurs du réseau local de l'organisation.

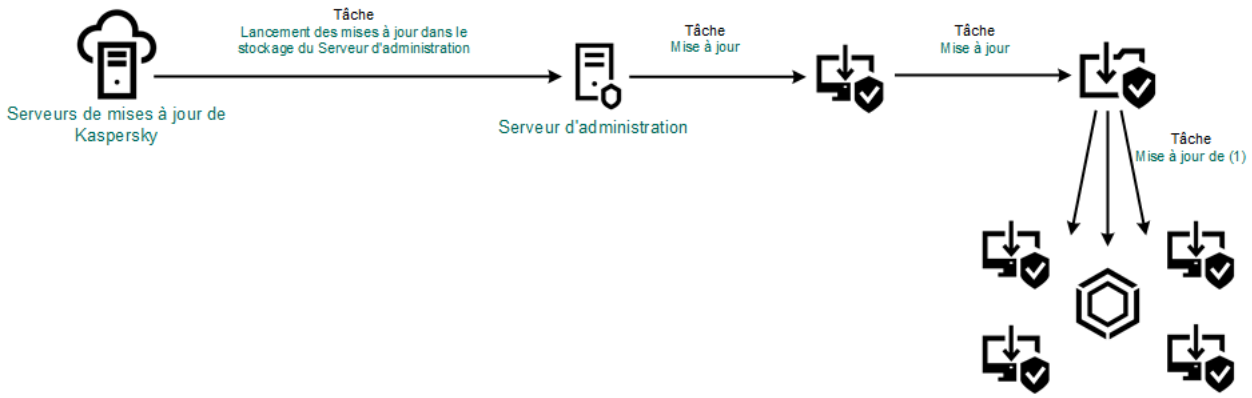
   - À l'aide de Kaspersky Update Utility. Les informations détaillées sur l'utilisation de Kaspersky Update Utility sont reprises dans la Base des connaissances de Kaspersky.

3. Diffusion du paquet de mise à jour sur les ordinateurs client.

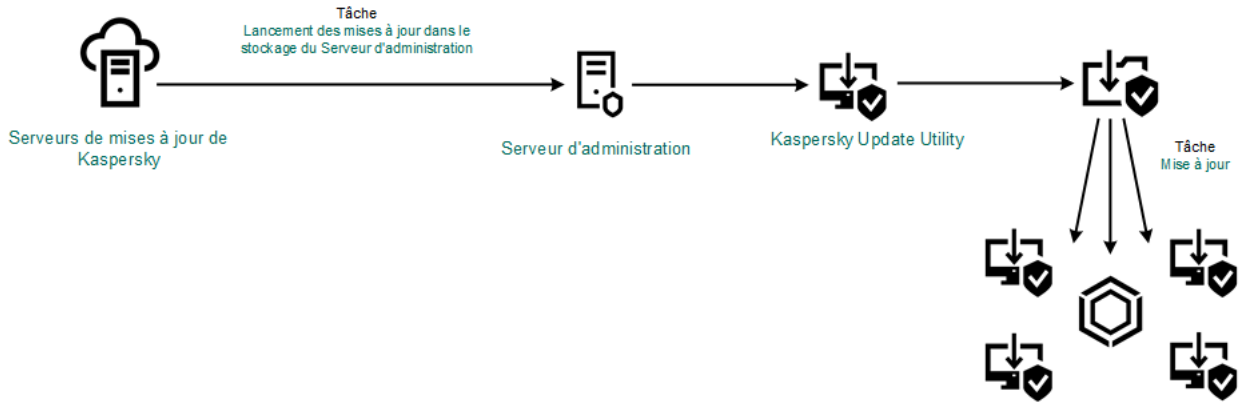
   La diffusion du paquet de mise à jour sur les ordinateurs client est garantie par la tâche *Mise à jour des bases et des modules d'application* de Kaspersky Endpoint Security. Vous pouvez créer un nombre illimité de tâches de mise à jour pour chacun des groupes d'administration.



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

Pour Kaspersky Security Center, 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 misse 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 (la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*).

   La tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration et n'existe qu'en un seul exemplaire. Par défaut, Kaspersky Security Center copie le paquet de mise à jour dans le dossier `\\<server name>\KLSHARE\Updates`. Pour en savoir plus sur le téléchargement des mises à jour dans le stockage du Serveur d'administration, consultez l'aide de Kaspersky Security Center.

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 des bases et des modules d'application*).

   Comment configurer la mise à jour de Kaspersky Endpoint Security depuis le dossier indiqué dans la Console d'administration (MMC)

   1. Ouvrez la Console d'administration de Kaspersky Security Center.

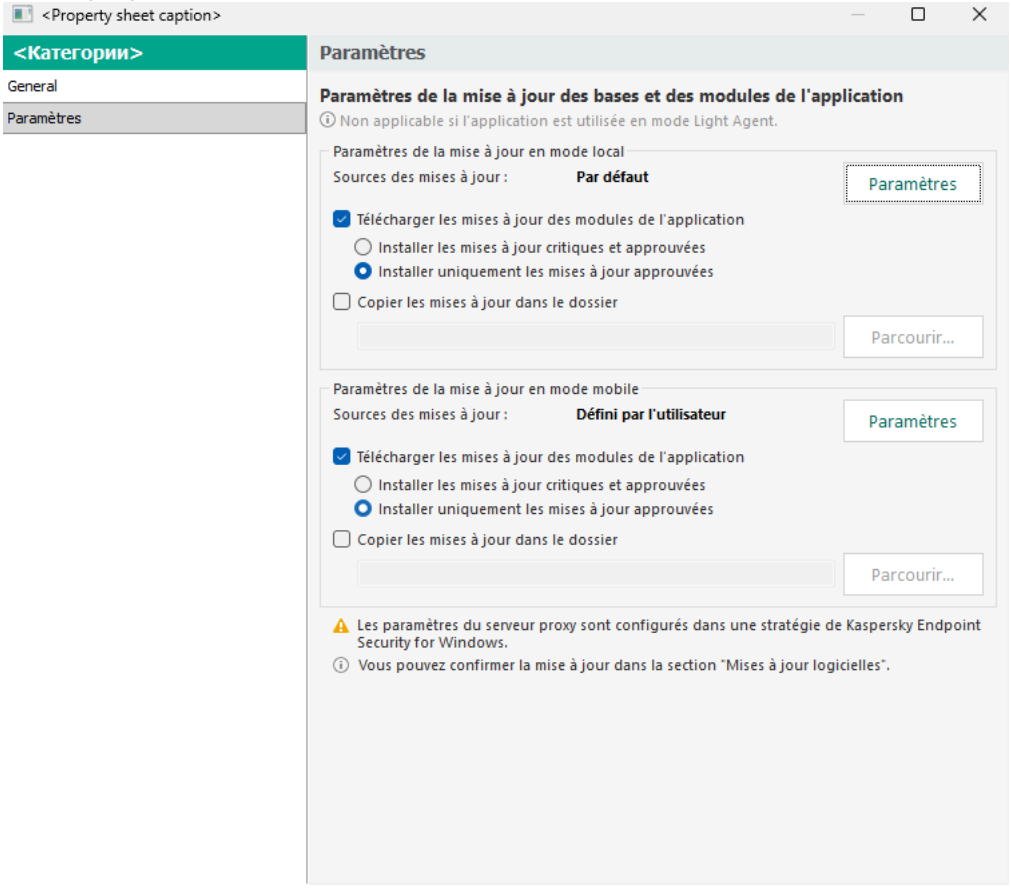
      Dans l'arborescence de la console, sélectionnez **Tâches**.

   2. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

      La fenêtre des propriétés de la tâche s'ouvre.

      La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

3. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la mise à jour en mode local**.

5. Dans la liste des sources de mises à jour, assurez-vous que la mise à jour à partir de la source de **Kaspersky Security Center** est activée. De plus, la source de **Kaspersky Security Center** doit présenter la priorité la plus élevée.

6. Si nécessaire, ajoutez les sources de mises à jour :

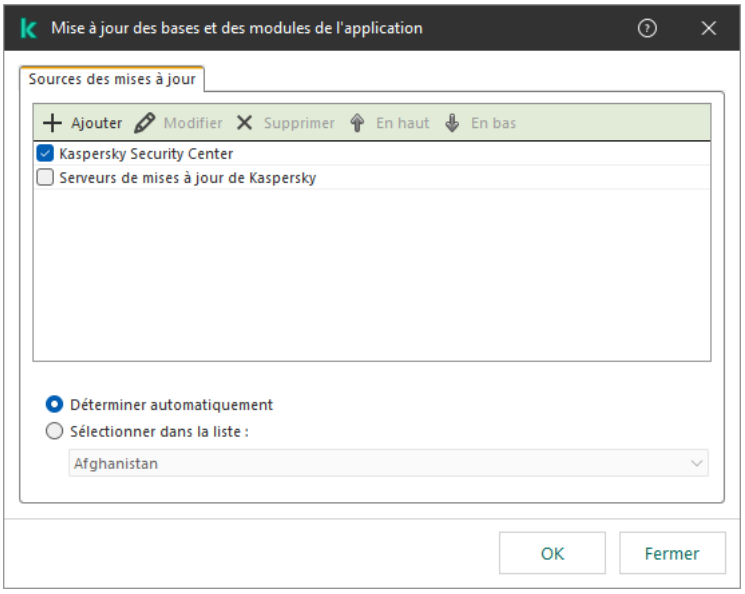
   a. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

   b. Dans le champ **Sources 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.

   > 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 (la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*).

   c. Cliquez sur le bouton **OK**.

Vous pouvez exclure la source de mise à jour sans la supprimer de la liste des sources de mises à jour. Pour ce faire, décochez la case à côté de l'objet.



Sources de mises à jour

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **En haut** et **En bas**.

   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.

8. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation** et configurez le mode d'exécution de la tâche.

9. Par défaut, Kaspersky Endpoint Security exécute la tâche en mode manuel.

10. Enregistrez vos modifications.

Comment configurer la mise à jour de Kaspersky Endpoint Security depuis le dossier indiqué dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** pour 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 du Serveur d'administration. Pour créer la tâche *Mise à jour* pendant l'exécution de l'Assistant, installez le plug-in d'administration 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, assurez-vous que la mise à jour à partir de la source de **Kaspersky Security Center** est activée. De plus, la source de **Kaspersky Security Center** doit présenter la priorité la plus élevée.

5. Si nécessaire, ajoutez les sources de mises à jour :

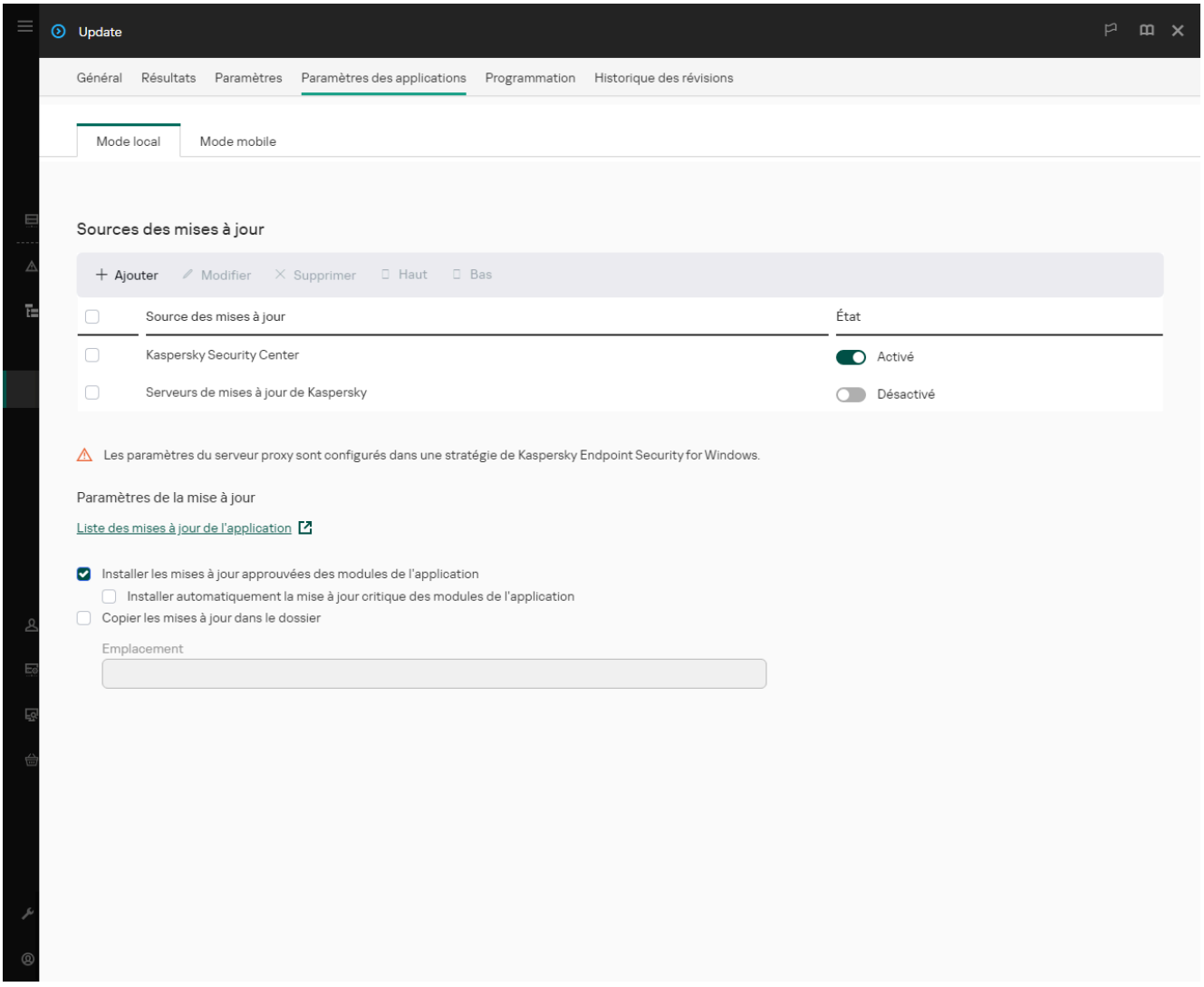
   a. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

   b. Dans le champ **Sources de mise 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.

   > 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 (la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*).

   c. Cliquez sur **Enregistrer**.

   Vous pouvez exclure la source de mise à jour sans la supprimer de la liste des sources de mises à jour. Pour ce faire, mettez le commutateur situé à côté en position d'arrêt.



Sources de mises à jour

6. Configurez les priorités des sources des mises à jour à l'aide des boutons **Monter** et **Descendre**.

   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.

7. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation** et configurez le mode d'exécution de la tâche.

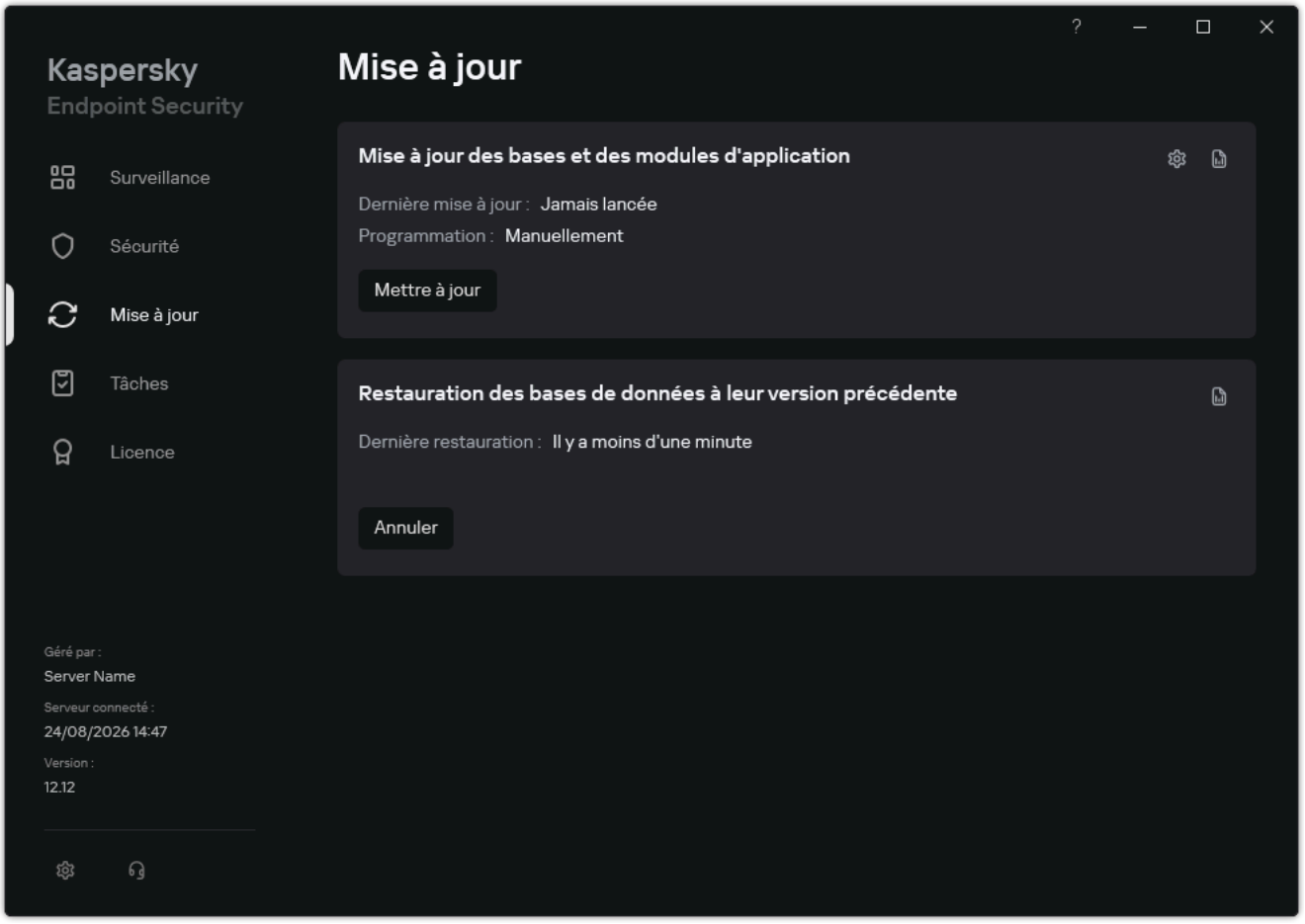
8. Par défaut, Kaspersky Endpoint Security exécute la tâche en mode manuel.

9. Enregistrez vos modifications.

Comment configurer la mise à jour de Kaspersky Endpoint Security depuis le dossier indiqué dans l'interface de l'application

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

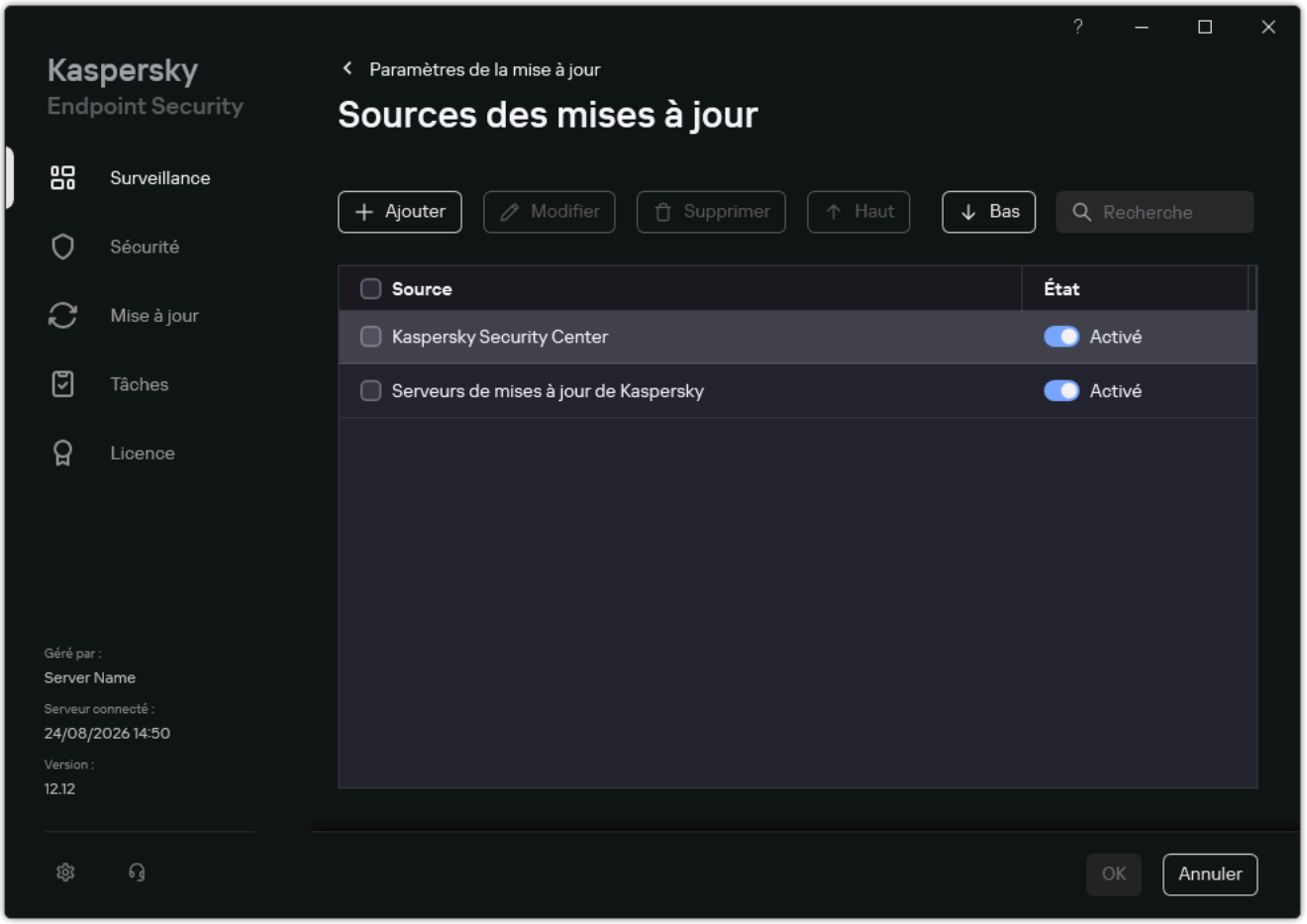
   La fenêtre des propriétés de la tâche s'ouvre.

3. Dans la fenêtre des propriétés de la tâche, cliquez sur **Sélectionner les sources des mises à jour**.

4. Dans la liste des sources de mises à jour, assurez-vous que la mise à jour à partir de la source de **Kaspersky Security Center** est activée. De plus, la source de **Kaspersky Security Center** doit présenter la priorité la plus élevée.

5. Si nécessaire, ajoutez les sources de mises à jour :

   a. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.



Sources de mises à jour

   a. Indiquez 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 (la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*).

   b. Cliquez sur **Sélectionner**.

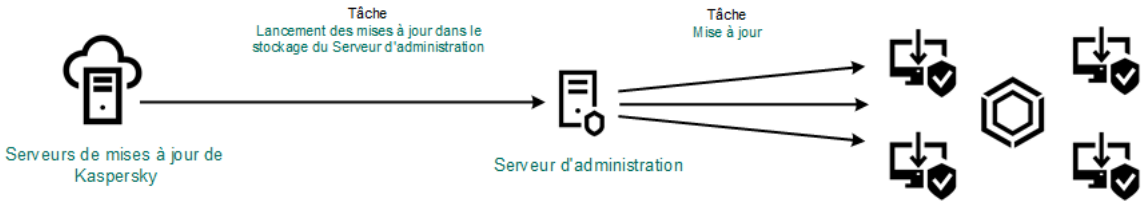
   Vous pouvez exclure la source de mise à jour sans la supprimer de la liste des sources de mises à jour. Pour ce faire, mettez le commutateur situé à côté en position d'arrêt.

6. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

   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.

Si un ordinateur est administré par Kaspersky Security Center, il n'est pas possible de configurer le mode d'exécution de la tâche *Mise à jour des bases et des modules d'application*. Vous pouvez uniquement lancer la tâche manuellement.

7. Enregistrez vos modifications.



Mise à jour depuis un stockage du serveur

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 version et la localisation de l'application Kaspersky Endpoint Security qui copie le paquet de mise à jour dans un dossier partagé doivent correspondre à la version et à la localisation de l'application qui met à jour les bases de données à partir du dossier partagé. Si les versions ou les localisations des applications ne correspondent pas, la mise à jour de la base de données peut se solder par une erreur.

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 local d'entreprise.

   Activation de la copie du paquet de mise à jour dans le dossier partagé de la Console d'administration (MMC)

   1. Ouvrez la Console d'administration de Kaspersky Security Center.

   2. Dans l'arborescence de la console, sélectionnez **Tâches**.

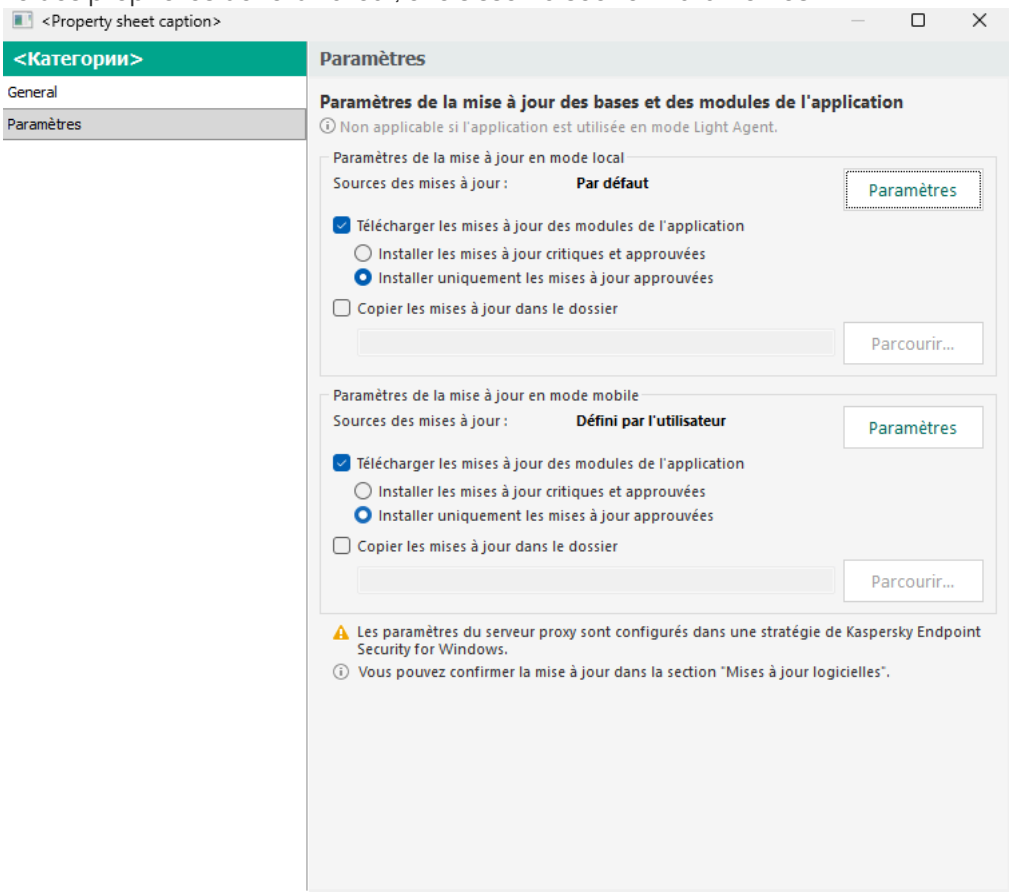
   La tâche *Mise à jour des bases et des modules d'application* doit être affectée à un ordinateur qui sera considéré comme la source des mises à jour.

   3. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la mise à jour en mode local**.

6. 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.

7. Cochez la case **Copier les mises à jour dans le dossier**.

8. Dans le champ **Chemin d'accès au dossier**, saisissez le chemin UNC du dossier partagé (par exemple, `\\<server name>\KLSHARE\Updates`).

   Si le champ n'est pas rempli, Kaspersky Endpoint Security copiera le paquet de mise à jour dans le dossier `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Enregistrez vos modifications.

Activation de la copie du paquet de mise à jour dans le dossier partagé de Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

La tâche *Mise à jour* doit être affectée à un ordinateur qui sera considéré comme la source des mises à jour.

2. Cliquez sur la tâche **Mise à jour** pour 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 du Serveur d'administration. Pour créer la tâche *Mise à jour* pendant l'exécution de l'Assistant, installez le plug-in d'administration 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 name>\KLSHARE\Updates`).

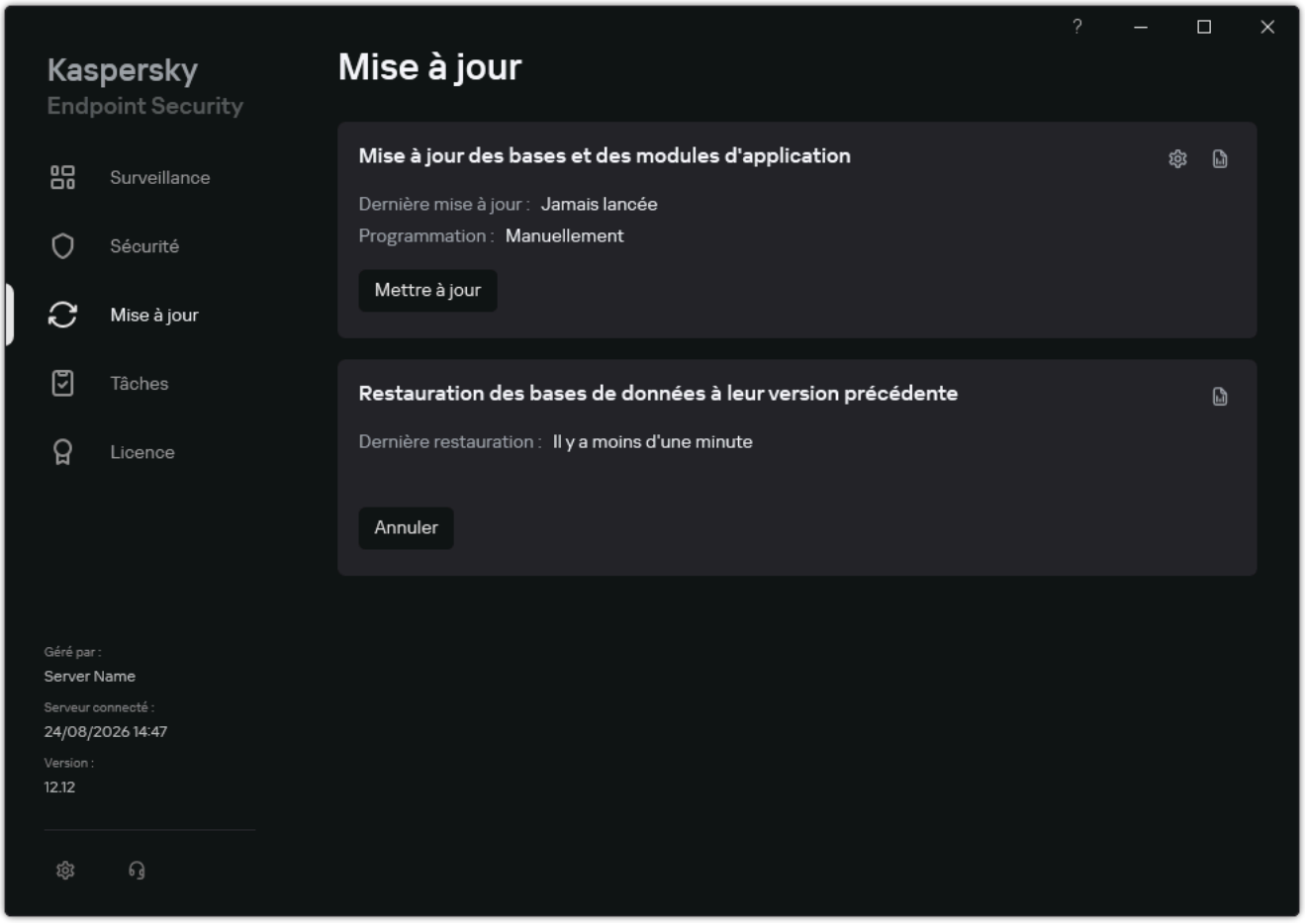
   Si le champ n'est pas rempli, Kaspersky Endpoint Security copiera le paquet de mise à jour dans le dossier `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Enregistrez vos modifications.

Activation de la copie du paquet de mise à jour dans le dossier partagé dans l'interface de l'application

> Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

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 name>\KLSHARE\Updates`).

5. Enregistrez vos modifications.

3. 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.

Configuration des mises à jour à partir du dossier partagé dans la Console d'administration (MMC)

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Mise à jour des bases et des modules d'application**.

4. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

5. Cliquez sur **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 (14.2)** → **Mise à jour des bases et des modules d'application**.

Étape 2. Sélection des sources de mise à jour

Ajoutez une nouvelle source de mise à jour : un dossier partagé. L'adresse de la source doit correspondre à l'adresse renseignée au préalable dans le champ **Chemin d'accès au dossier** lors de la configuration du mode de copie du paquet de mise à jour dans le dossier partagé. Configurez les priorités des sources des mises à jour à l'aide des boutons **En haut** et **En bas**.

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.

La tâche *Mise à jour des bases et des modules d'application* doit être attribuée aux ordinateurs restants du réseau local de l'organisation, à l'exception de l'ordinateur considéré comme source de mises à jour.

Étape 4. Sélection du compte utilisateur pour lancer la tâche

Sélectionnez un compte pour exécuter la tâche de *Mise à jour des bases et des modules d'application*. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

Étape 5. 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 6. Définition du nom de la tâche

Saisissez le nom de la tâche, par exemple *Mise à jour depuis un dossier partagé*.

Étape 7. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. La tâche de mise à jour est alors exécutée sur les ordinateurs des utilisateurs conformément à la planification définie.

Configuration des mises à jour à partir du dossier partagé dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   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 **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

   > La tâche *Mise à jour* doit être attribuée aux ordinateurs restants 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, puis passez à l'étape suivante.

5. Quittez l'Assistant.

   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. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.

8. Cliquez sur le bouton **Ajouter** dans le groupe **Sources de mise à jour**.

9. 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 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).

10. Cliquez sur **OK**.

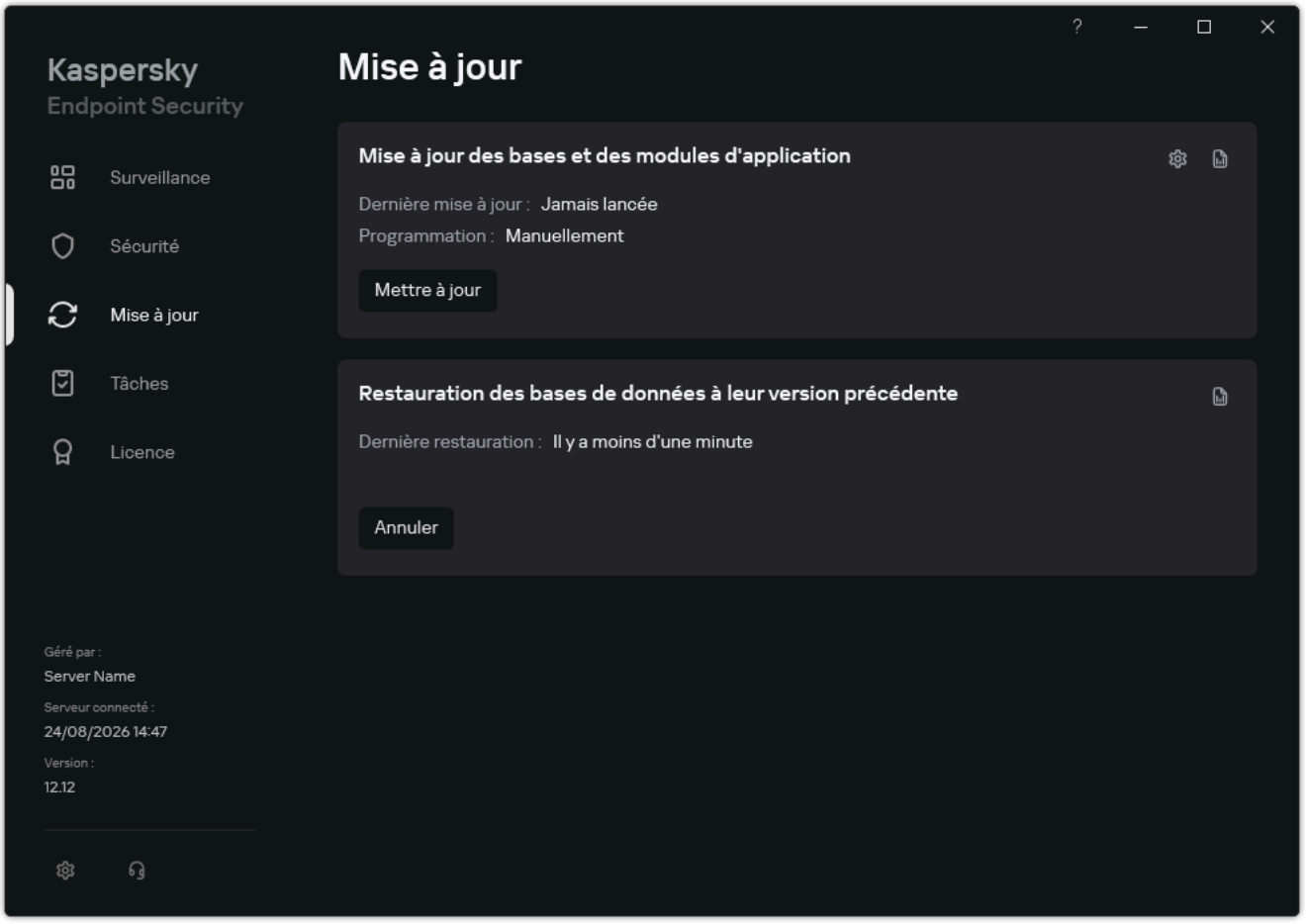
11. Configurez les priorités des sources des mises à jour à l'aide des boutons **Monter** et **Descendre**.

12. Enregistrez vos modifications.

Configuration des mises à jour à partir du dossier partagé dans l'interface de l'application

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Cliquez sur **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.

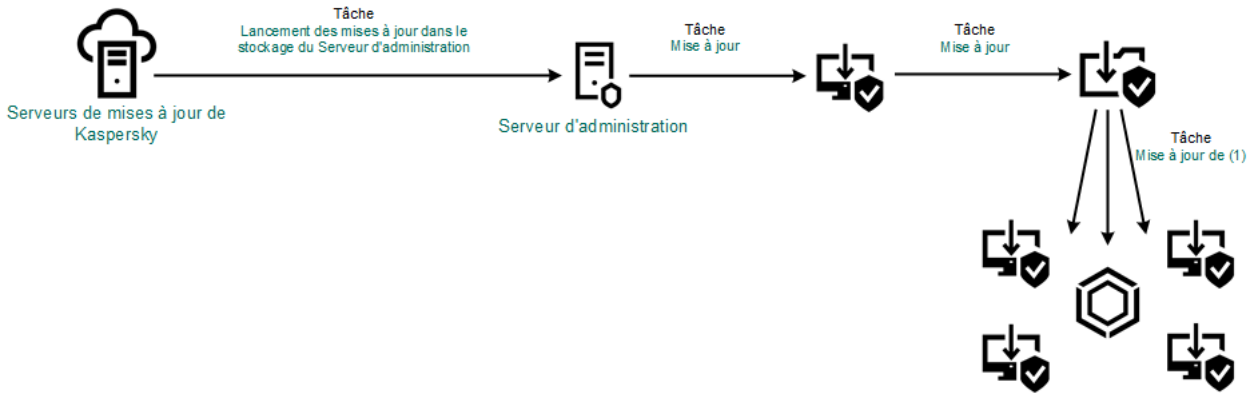
   L'adresse de la source doit correspondre à l'adresse renseignée au préalable lors de la configuration du mode de copie du paquet de mise à jour dans le dossier partagé (cf. les instructions ci-dessus).

6. Cliquez sur **Sélectionner**.

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

   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.

8. Enregistrez vos modifications.



Mise à jour depuis un dossier partagé

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 version et la localisation de l'application Kaspersky Endpoint Security qui copie le paquet de mise à jour dans un dossier partagé doivent correspondre à la version et à la localisation de l'application qui met à jour les bases de données à partir du dossier partagé. Si les versions ou les localisations des applications ne correspondent pas, la mise à jour de la base de données peut se solder par une erreur.

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.

   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.

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.

Configuration des mises à jour à partir du dossier partagé dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

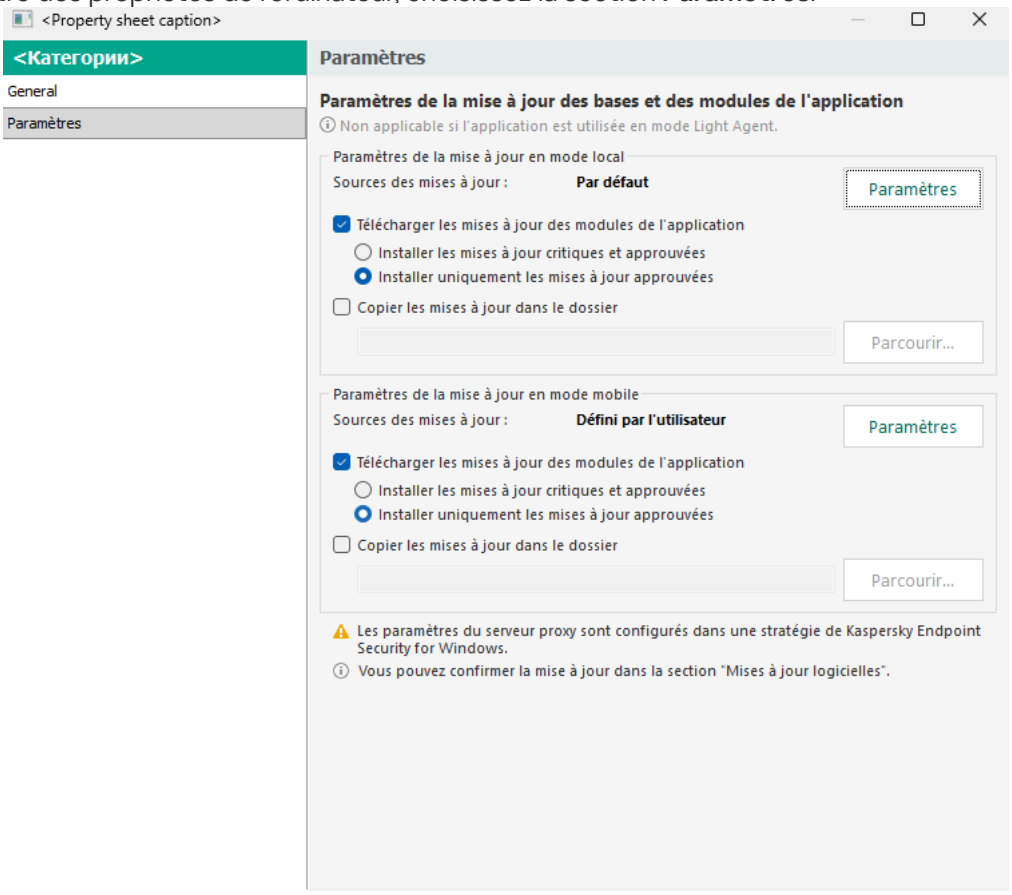
2. Dans l'arborescence de la console, sélectionnez **Tâches**.

3. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la mise à jour en mode local**.

6. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

7. Dans la fenêtre qui s'ouvre, saisissez le chemin UNC du dossier partagé (par exemple, `\\<server name>\KLSHARE\Updates`).

   L'adresse de la source doit correspondre à l'adresse spécifiée dans les paramètres de Kaspersky Update Utility.

8. Cliquez sur **OK**.

9. Configurez les priorités des sources des mises à jour à l'aide des boutons **En haut** et **En bas**.

   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.

10. Enregistrez vos modifications.

Configuration des mises à jour à partir du dossier partagé dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** pour 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 du Serveur d'administration. Pour créer la tâche *Mise à jour* pendant l'exécution de l'Assistant, installez le plug-in d'administration 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 la fenêtre qui s'ouvre, saisissez le chemin UNC du dossier partagé (par exemple, `\\<server name>\KLSHARE\Updates`).

   > L'adresse de la source doit correspondre à l'adresse spécifiée dans les paramètres de Kaspersky Update Utility.

6. Cliquez sur **OK**.

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **En haut** et **En bas**.

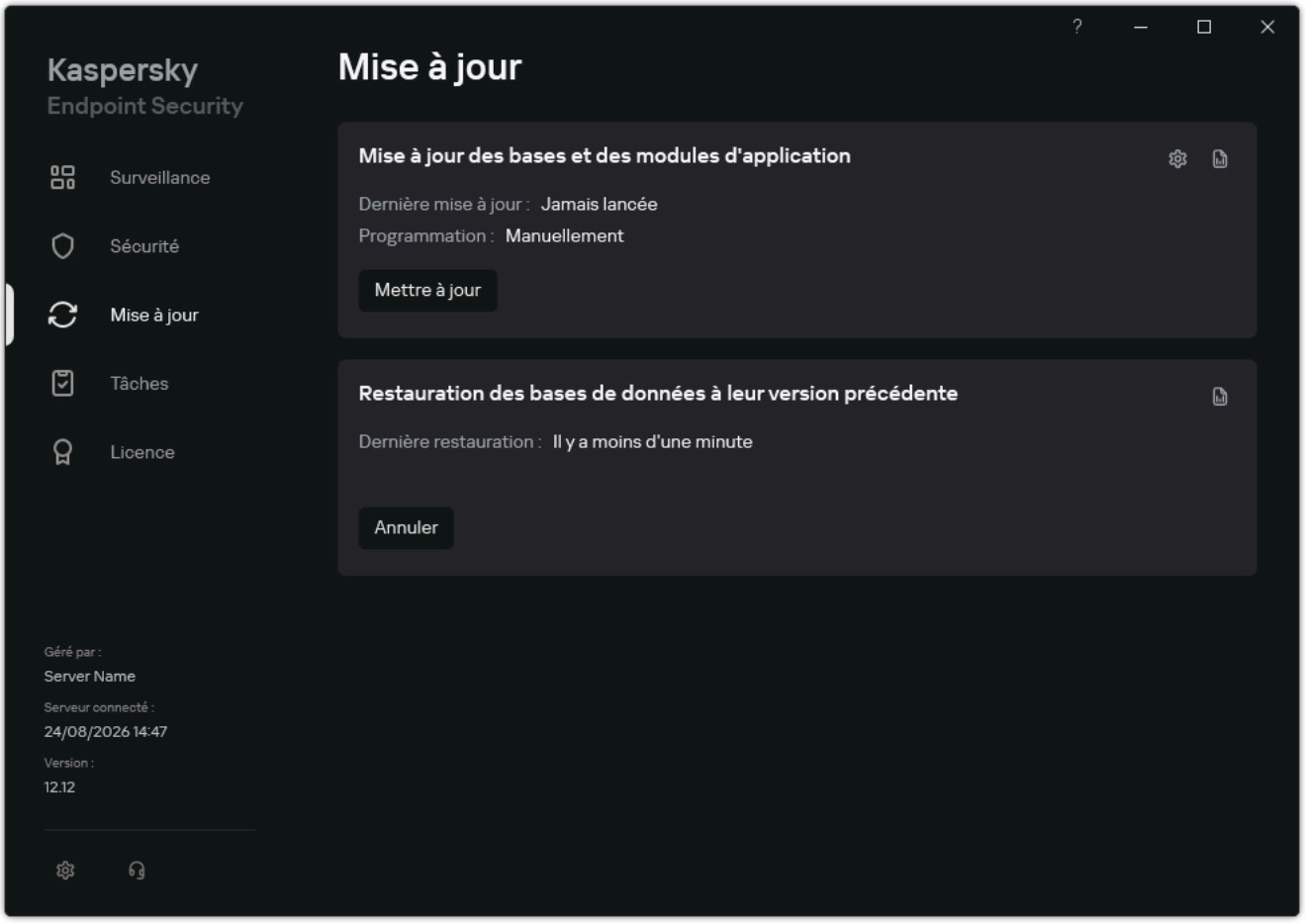
   Si la mise à jour ne peut pas être exécutée depuis la première source de mises à jour, Kaspersky Endpoint Security passe automatiquement à la suivante.

8. Enregistrez vos modifications.

Configuration des mises à jour à partir du dossier partagé dans l'interface de l'application

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



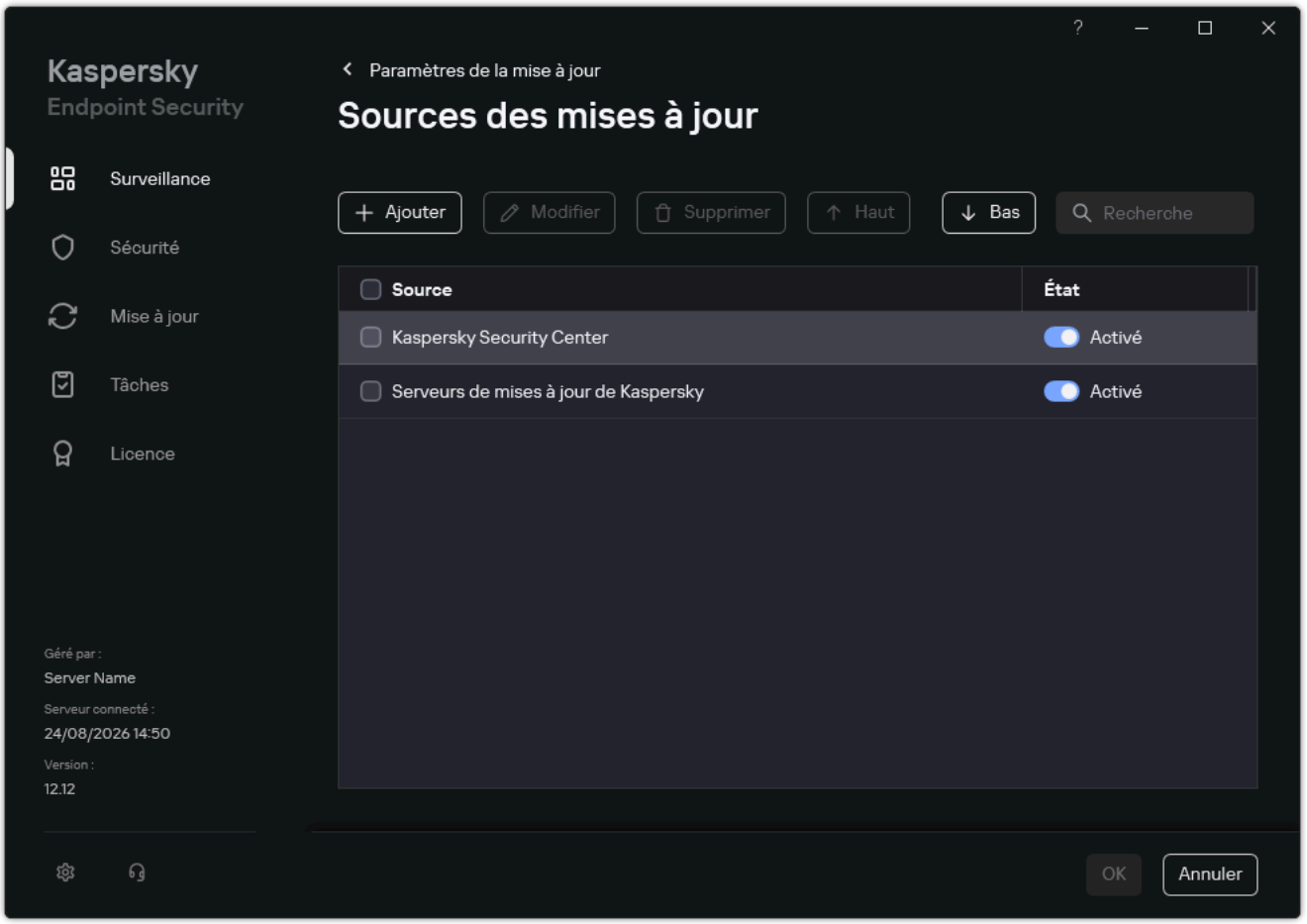
Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Dans la fenêtre des propriétés de la tâche, cliquez sur **Sélectionner les sources des mises à jour**.

4. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.



Sources de mises à jour

5. Saisissez le chemin UNC du dossier partagé (par exemple, `\\<server name>\KLSHARE\Updates`).

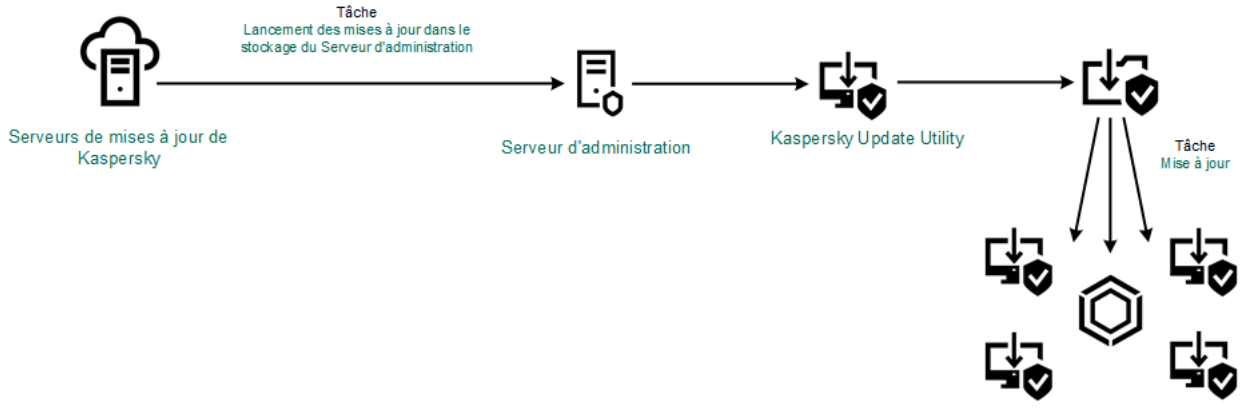
> L'adresse de la source doit correspondre à l'adresse spécifiée dans les paramètres de Kaspersky Update Utility.

6. Cliquez sur **Sélectionner**.

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Haut** et **Bas**.

   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.

8. Enregistrez vos modifications.



Mise à jour à l'aide de Kaspersky Update Utility

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 autonomes, 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.

Configuration des paramètres de mise à jour pour le mode mobile dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

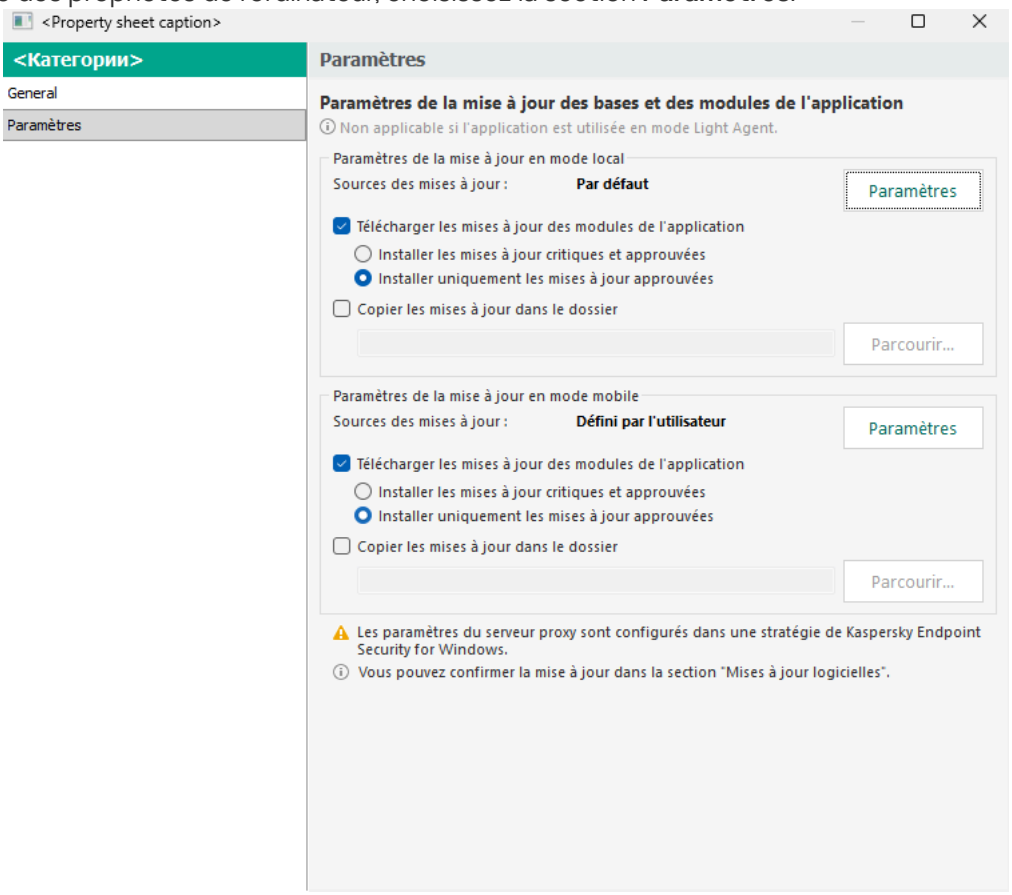
2. Dans l'arborescence de la console, sélectionnez **Tâches**.

3. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la mise à jour en mode mobile**.

6. 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.

7. Enregistrez vos modifications.

Configuration des paramètres de mise à jour pour le mode mobile dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** pour 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 du Serveur d'administration. Pour créer la tâche *Mise à jour* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode mobile**.

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 ou d'autres serveurs FTP ou HTTP, ainsi que des dossiers locaux ou réseau.

5. Enregistrez vos modifications.

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, accédez à la section **Mise à jour**.

2. Dans la mosaïque **Mise à jour des bases et des modules d'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 arrêter la tâche à tout moment en cliquant sur le bouton **Arrêter la mise à jour**.

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.

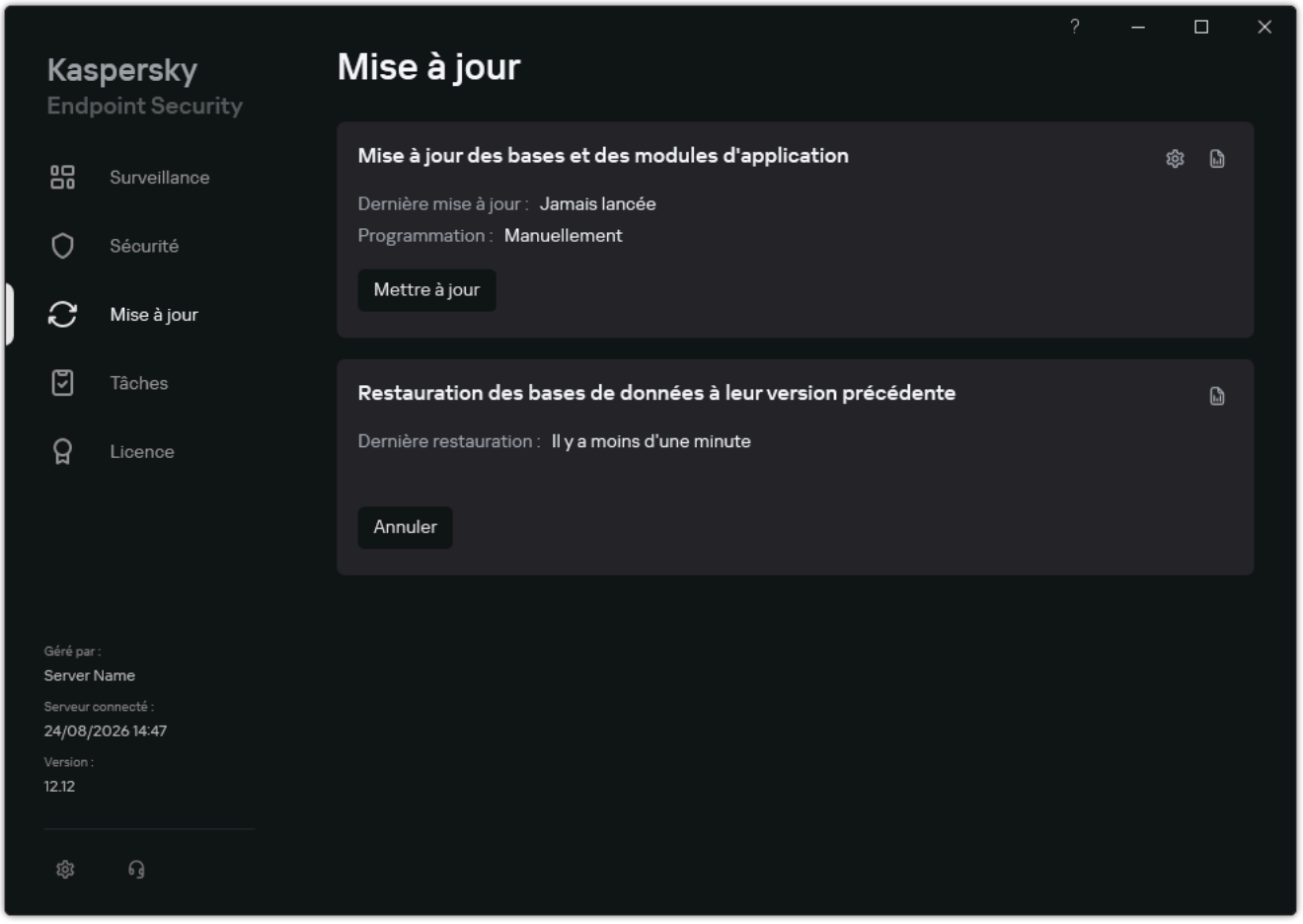
Lancement de la tâche de mise à jour avec les privilèges d'un autre utilisateur

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 l'application 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 :

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Cliquez sur **Lancer les mises à jour des bases avec les privilèges d'utilisateur**.

4. Dans la fenêtre qui s'ouvre, sélectionnez **Autre 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

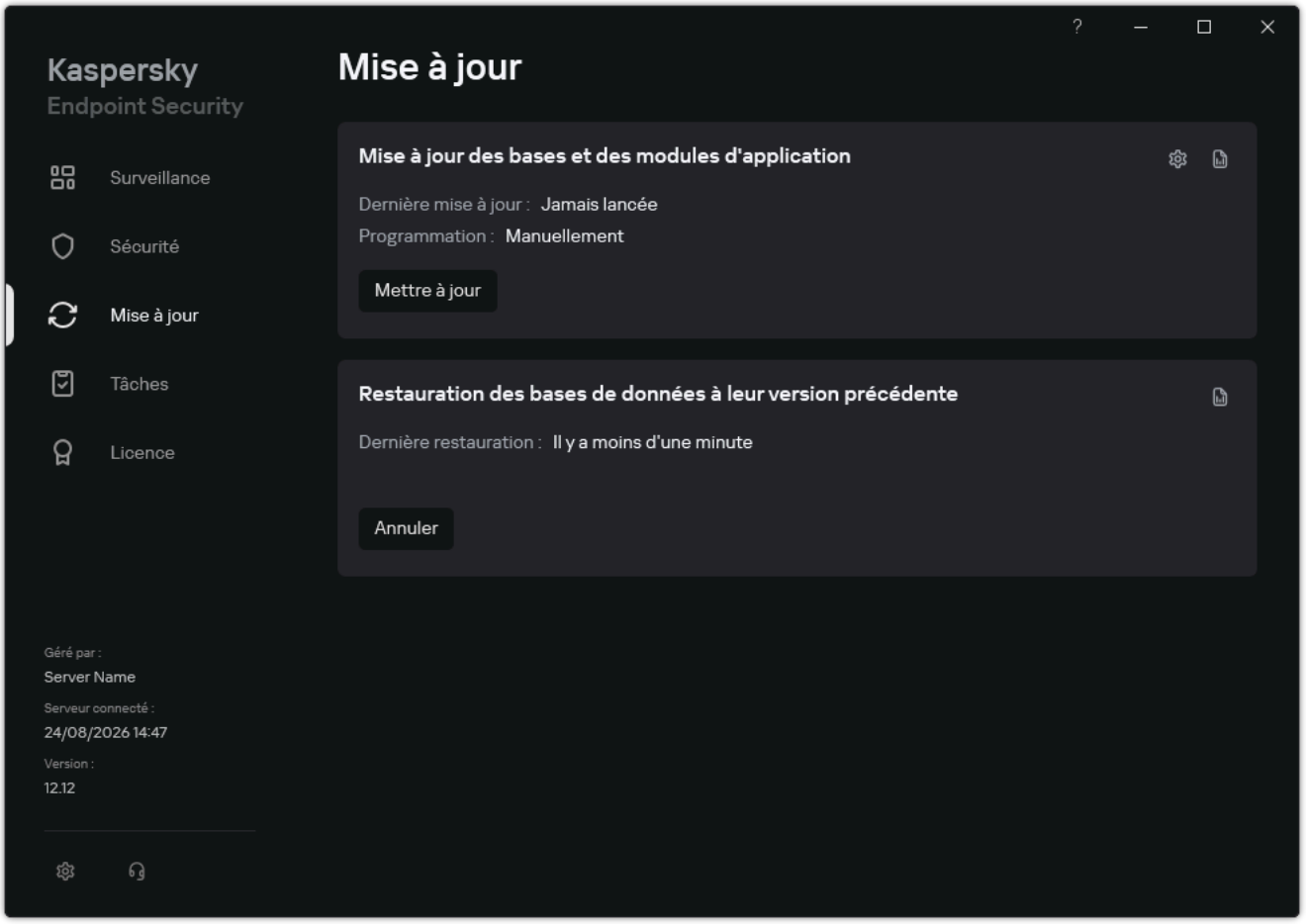
Si l'exécution de la tâche est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

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 planification** 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 :

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Cliquez sur **Mode d'exécution**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le mode d'exécution de la tâche de mise à jour :

   - Sélectionnez l'option **Automatiquement**, 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 **Manuellement** pour lancer la tâche de mise à jour manuellement.

   - Si vous souhaitez configurer une planification pour l'exécution de la tâche de mise à jour, sélectionnez d'autres options. Configurez les paramètres avancés pour lancer la tâche de mise à jour :

     - Dans le champ **Après le démarrage de l'application, reporter le lancement de X minutes**, saisissez l'intervalle de temps pour lequel vous souhaitez reporter le lancement de la tâche de mise à jour après le lancement de Kaspersky Endpoint Security.

     - 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 de mise à jour manquées à la première occasion. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur.

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.

En cas d'indisponibilité des serveurs de mise à jour de Kaspersky, Kaspersky Endpoint Security peut utiliser d'autres domaines pour mettre à jour ses bases de données et ses modules logiciels. Pour en savoir plus, consultez la Base des connaissances du Support Technique.

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.

Par défaut, Kaspersky Endpoint Security utilise le serveur Kaspersky Security Center comme première source de mise à jour. Il est ainsi possible de réduire le trafic lors des mises à jour. Si une stratégie n'est pas appliquée à l'ordinateur, les serveurs Kaspersky sont sélectionnés comme première source de mise à jour dans les paramètres de la tâche locale *Mise à jour des bases et des modules d'application* parce que l'application n'a peut-être pas accès au serveur de Kaspersky Security Center.

Si l'application s'exécute en mode Light Agent, un dossier sur la SVM est sélectionné comme source des mises à jour.

Ajout d'une source de mises à jour dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

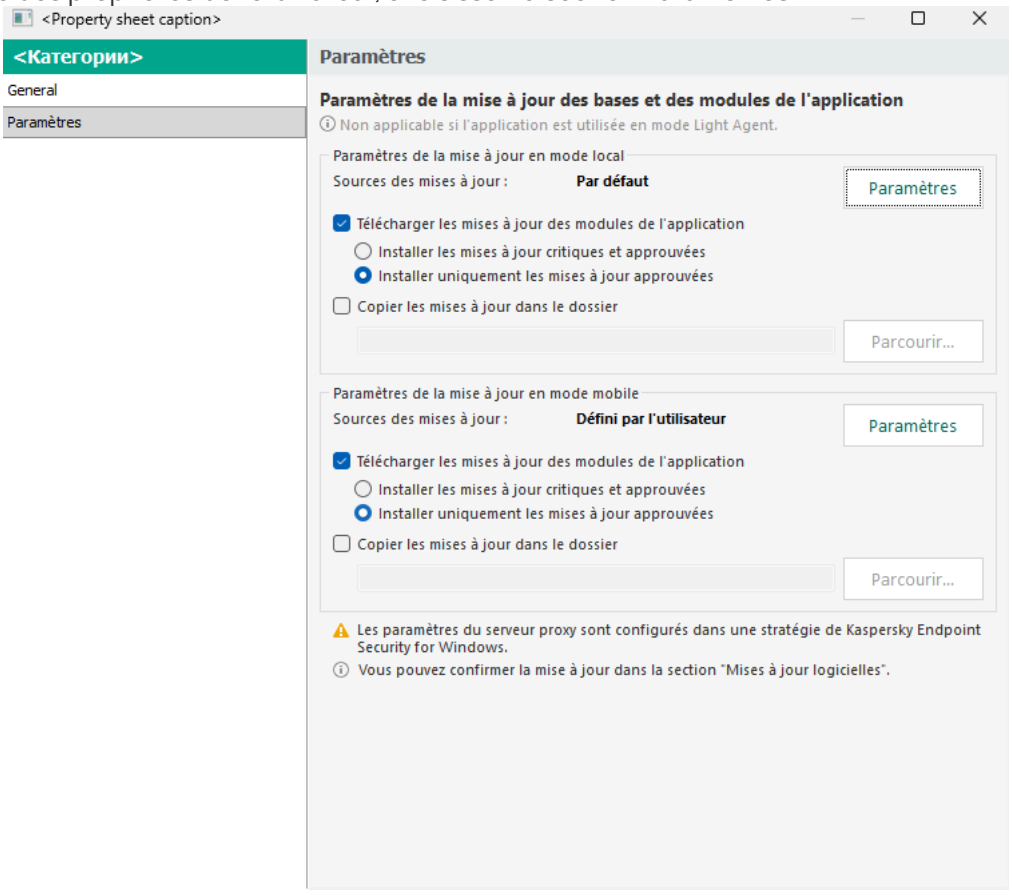
   Dans l'arborescence de la console, sélectionnez **Tâches**.

2. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

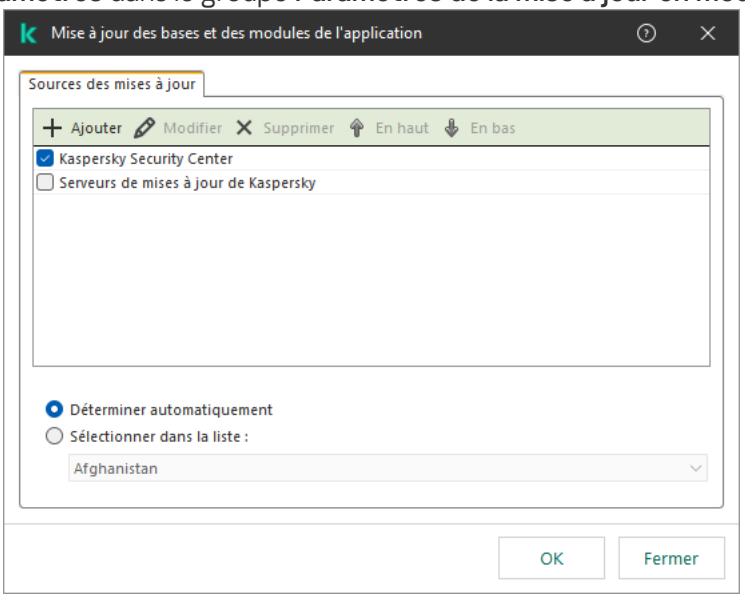
   La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

3. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la mise à jour en mode local**.



Sources de mises à jour

5. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.

6. Dans le champ **Sources des mises à jour**, renseignez l'adresse du serveur FTP ou HTTP, le dossier réseau ou local qui contient le paquet 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://dnl-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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

   Vous pouvez exclure la source de mise à jour sans la supprimer de la liste des sources de mises à jour. Pour ce faire, décochez la case à côté de l'objet.

7. Cliquez sur **OK**.

8. Configurez les priorités des sources des mises à jour à l'aide des boutons **En haut** et **En bas**.

   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.

9. Si nécessaire, ajoutez une source de mise à jour pour le 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*).

10. Enregistrez vos modifications.

Comment ajouter une source de mises à jour dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

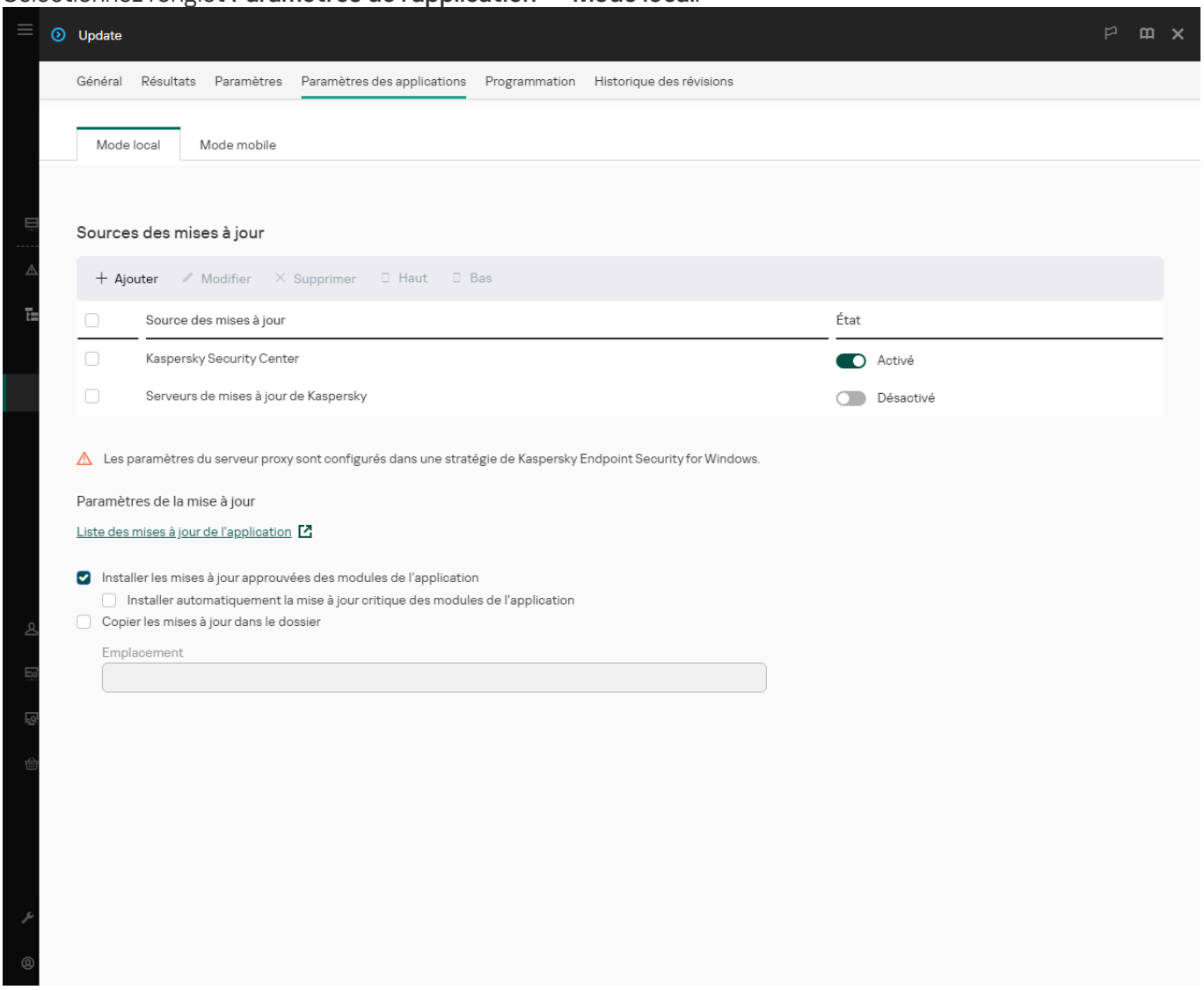
   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** pour 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 du Serveur d'administration. Pour créer la tâche *Mise à jour* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.



Sources de mises à jour

4. Dans la liste des sources de mises à jour, 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://dnl-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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

Vous pouvez exclure la source de mise à jour sans la supprimer de la liste des sources de mises à jour. Pour ce faire, mettez le commutateur situé à côté en position d'arrêt.

6. Cliquez sur **OK**.

7. Configurez les priorités des sources des mises à jour à l'aide des boutons **Monter** et **Descendre**.

   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.

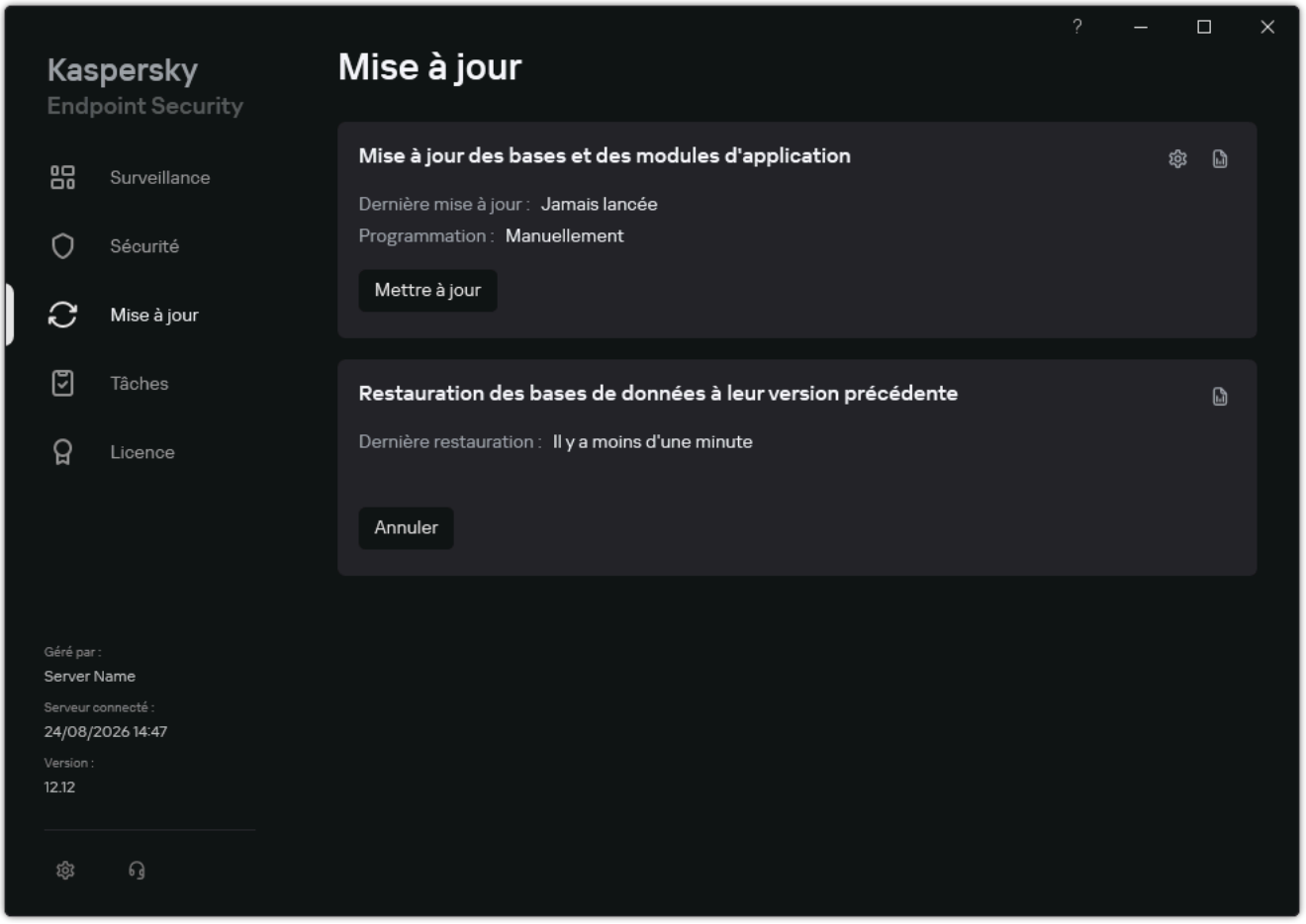
8. Si nécessaire, ajoutez une source de mise à jour pour le mode mobile. Le *mode mobile* est un mode de fonctionnement de Kaspersky Endpoint Security qui s'applique aux situations où l'ordinateur quitte le périmètre du réseau de l'organisation (*ordinateur déconnecté*).

9. Enregistrez vos modifications.

Ajout d'une source de mises à jour dans l'interface de l'application

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



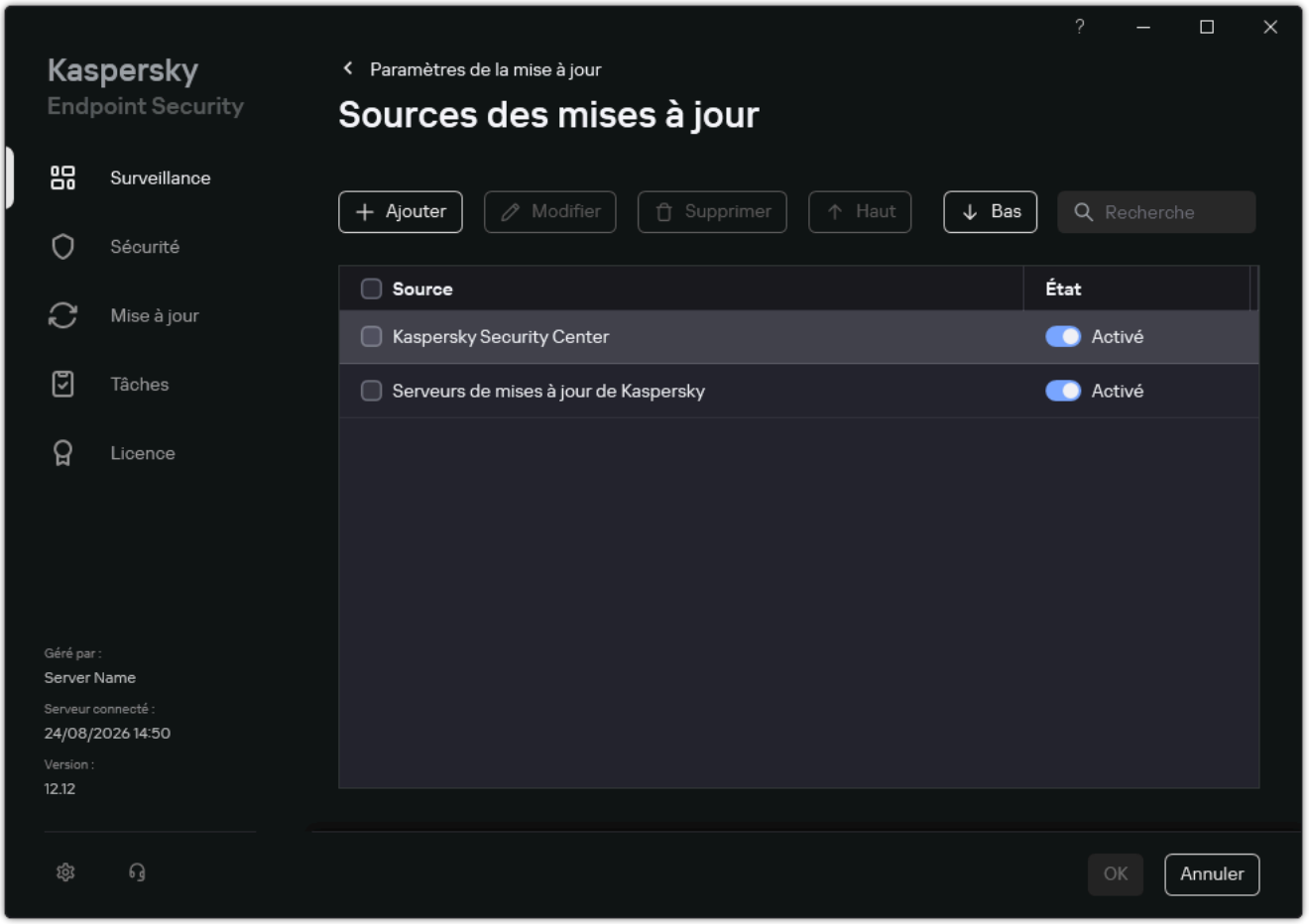
Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Cliquez sur **Sélectionner les sources des mises à jour**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.



Sources de mises à jour

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://dnl-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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

6. Cliquez sur **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. Dès qu'une mise à jour est disponible, l'application affiche une notification dans la fenêtre principale de Kaspersky Endpoint Security : . 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.

Après que vous avez installé une mise à jour de l'application, il peut vous être demandé de redémarrer votre ordinateur.

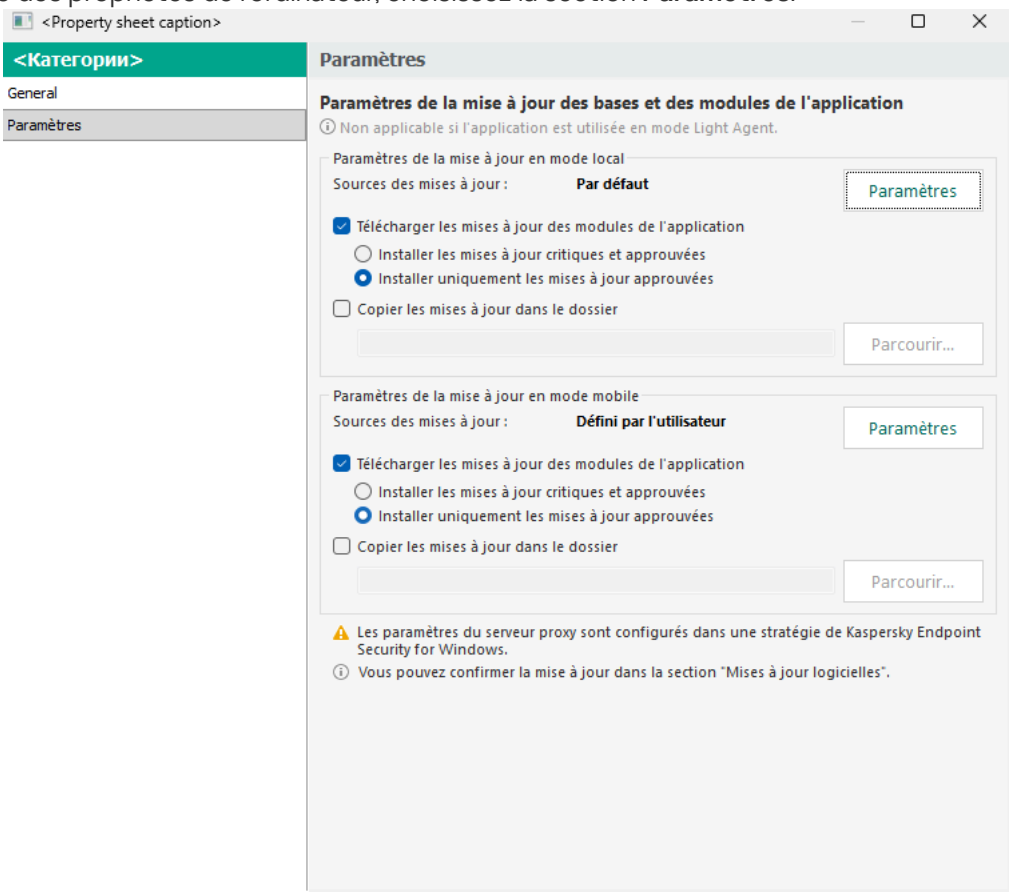
Configuration des mises à jour du module d'application dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.
3. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.



Paramètres de la tâche Mise à jour des bases et des modules d'application

5. Dans le groupe **Paramètres de la mise à jour en mode local**, cochez la case **Télécharger les mises à jour des modules de l'application**.

   Si vous voulez empêcher le téléchargement des mises à jour des modules de l'application, décochez la case **Télécharger les mises à jour des modules de l'application** et interdisez l'utilisation des tâches locales par l'utilisateur.

6. 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.

7. En cas de nécessité, configurez les mises à jour du module de l'application pour le 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*).

8. Enregistrez vos modifications.

Configuration des mises à jour du module d'application dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

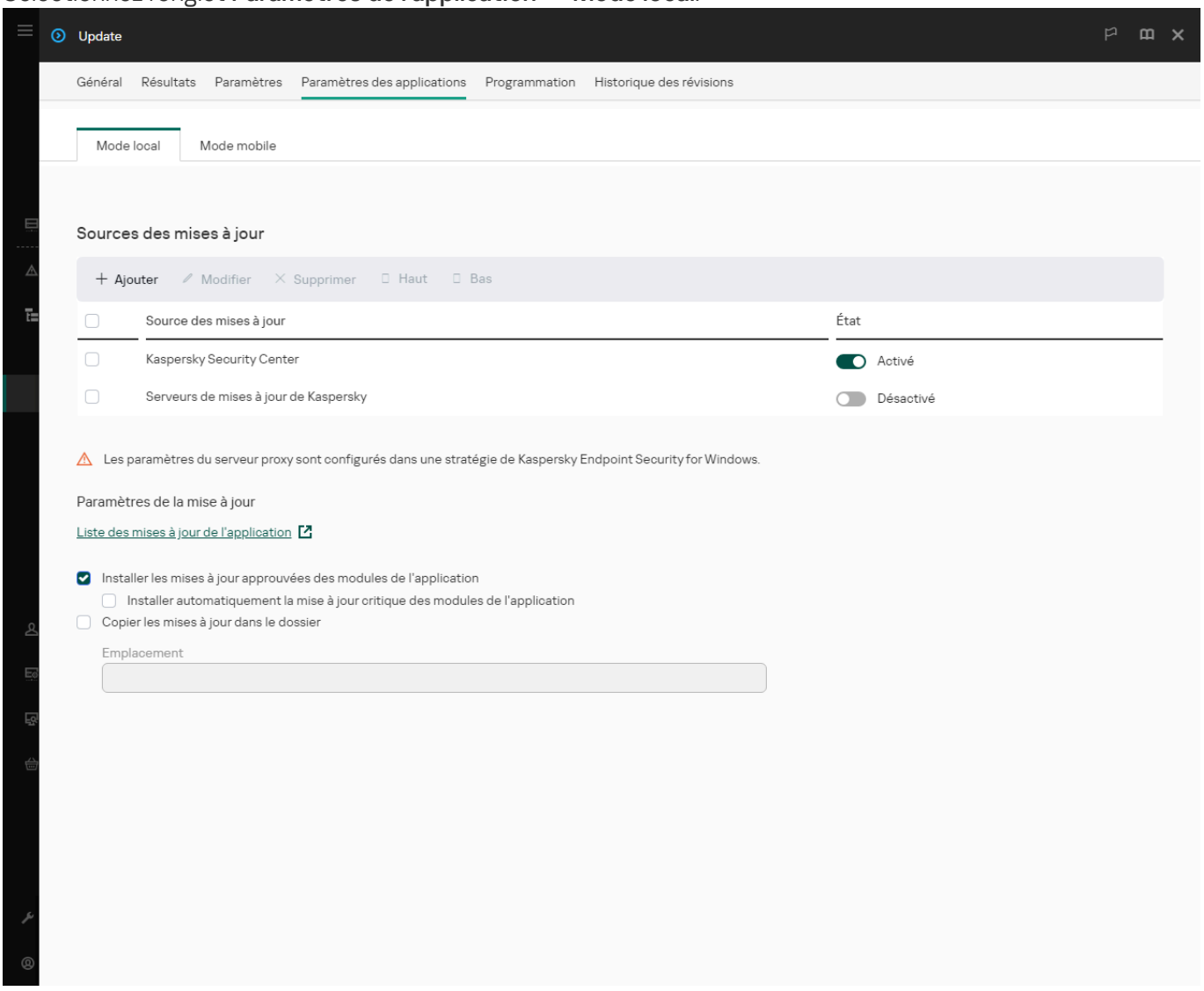
   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour des bases et des modules d'application** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour des bases et des modules d'application* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Pour créer la tâche *Mise à jour des bases et des modules d'application* pendant l'exécution de l'Assistant, installez le plug-in d'administration de Kaspersky Endpoint Security for Windows.

3. Sélectionnez l'onglet **Paramètres de l'application** → **Mode local**.



Paramètres de la tâche Mise à jour

4. Sous **Paramètres de mise à jour**, sélectionnez les mises à jour du module de l'application que vous souhaitez installer :

   - **Installer les mises à jour approuvées des modules d'application**. 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.

   - **Installer automatiquement les mises à jour critiques des modules d'application**. 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.

Si vous voulez empêcher le téléchargement des mises à jour des modules de l'application, décochez la case **Installer les mises à jour approuvées des modules d'application** et **Installer automatiquement les mises à jour critiques des modules d'application** cases à cocher et interdire l'utilisation des tâches locales par l'utilisateur.

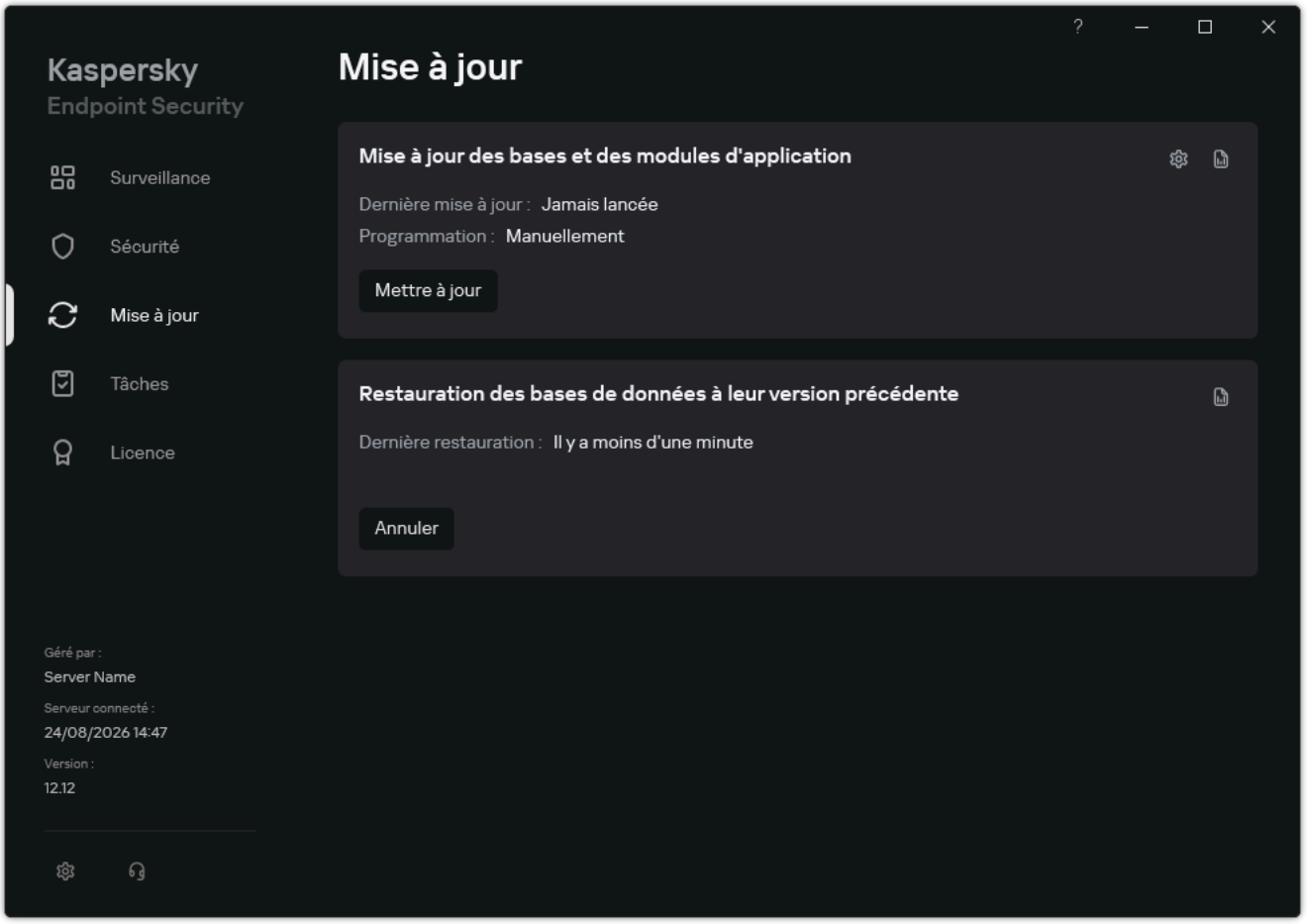
5. En cas de nécessité, configurez les mises à jour du module de l'application pour le mode mobile. Le *mode mobile* est un mode de fonctionnement de Kaspersky Endpoint Security qui s'applique aux situations où l'ordinateur quitte le périmètre du réseau de l'organisation (*ordinateur déconnecté*).

6. Enregistrez vos modifications.

Configuration d'une planification d'analyse dans l'interface de l'application

Vous ne pouvez pas configurer la tâche de groupe *Mise à jour des bases et des modules d'application* dans l'interface de l'application. Seule une tâche de mise à jour locale, *Mise à jour des bases et des modules d'application*, est disponible pour l'utilisateur. Si la tâche *Mise à jour des bases et des modules d'application* ne s'affiche pas, cela signifie que l'administrateur a interdit l'utilisation de tâches locales dans la stratégie.

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. La liste des tâches s'ouvre. Sélectionnez la tâche *Mise à jour des bases et des modules d'application*, puis cliquez sur ⚙.

   La fenêtre des propriétés de la tâche s'ouvre.

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. Enregistrez vos modifications.

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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Serveur proxy**.

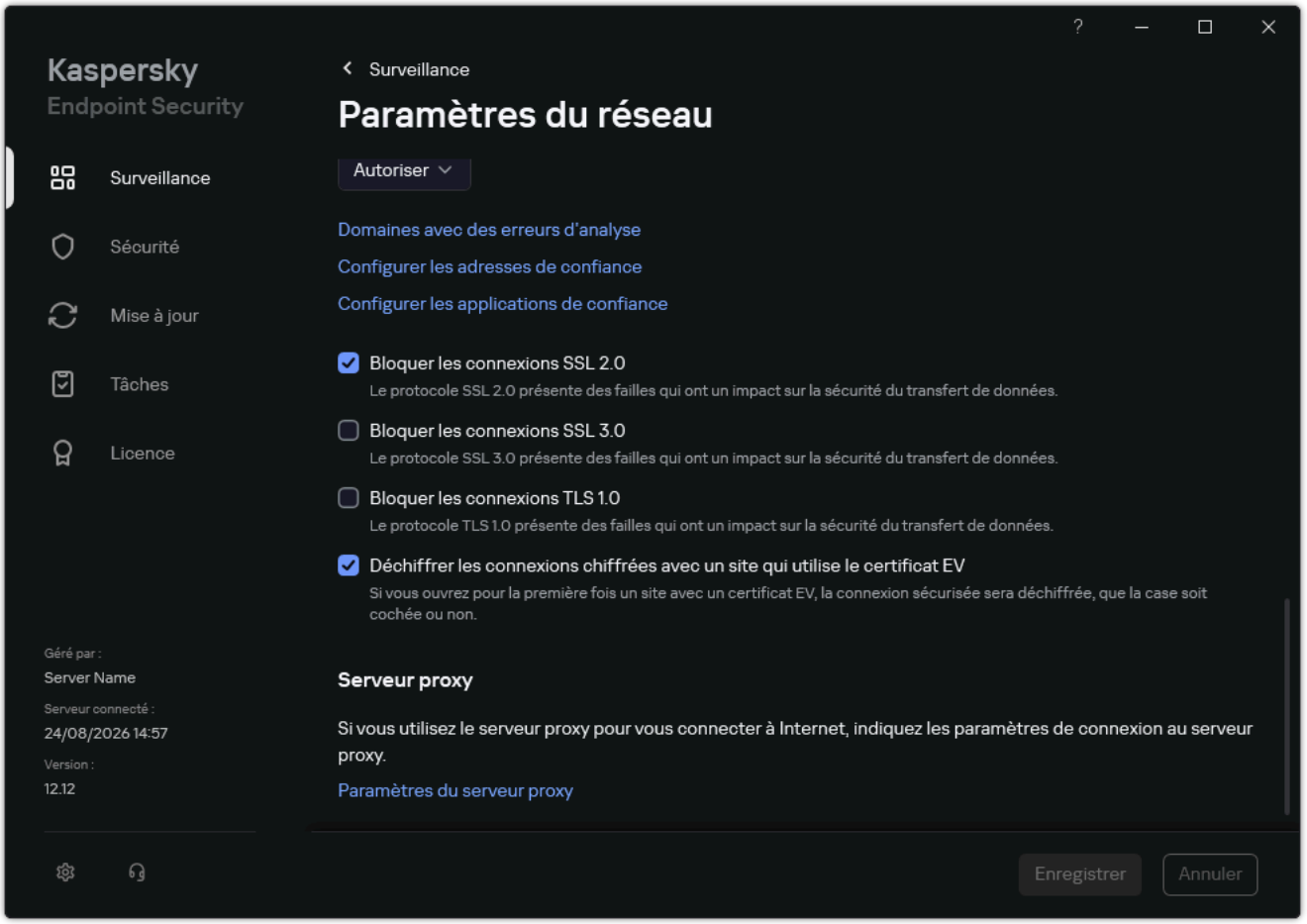
6. Dans la fenêtre qui s'ouvre, cochez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.

7. Enregistrez vos modifications.

Pour configurer les paramètres du serveur proxy dans l'interface de l'application, procédez comme suit :

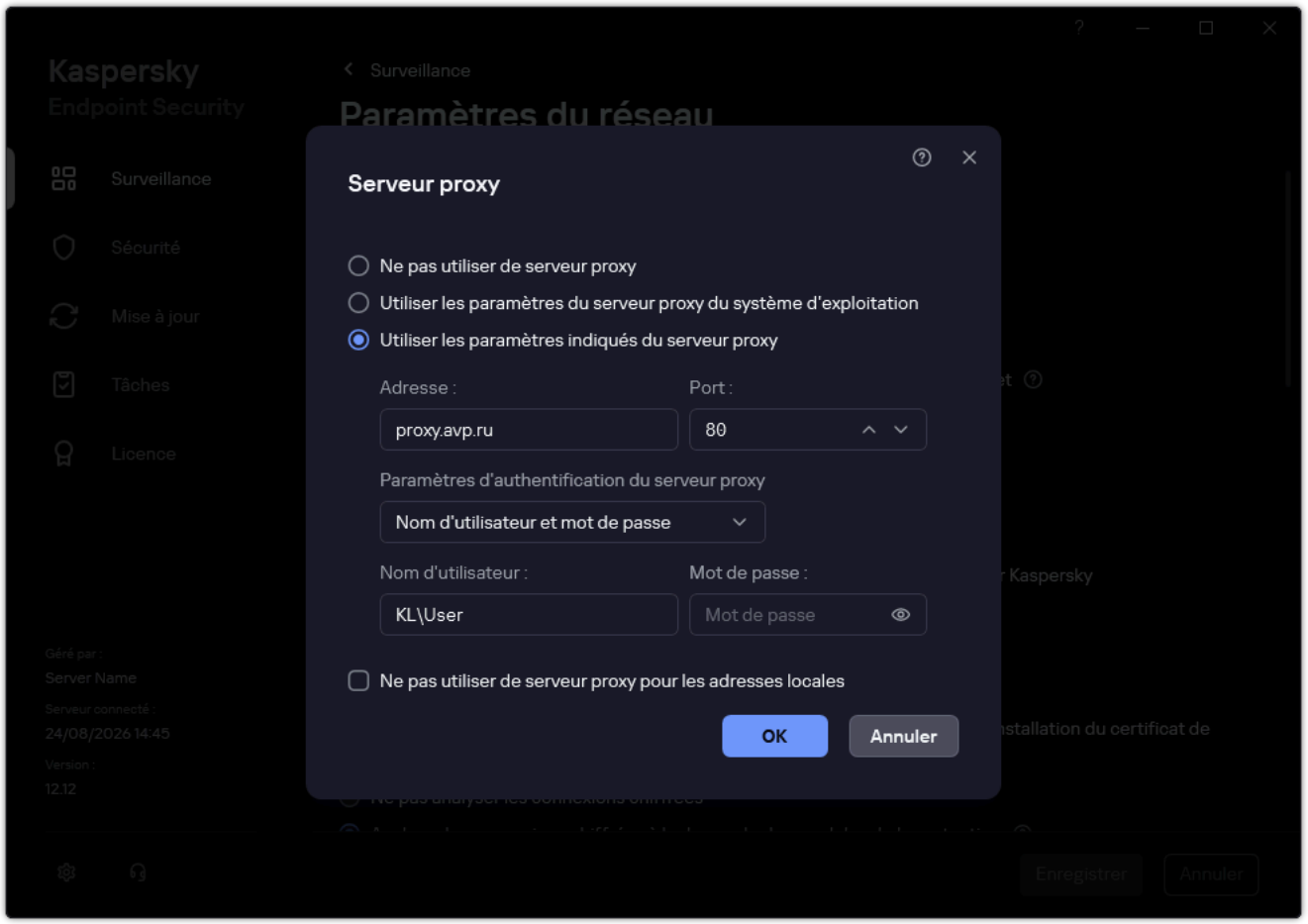
1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.



Paramètres réseau des applications

3. Dans le groupe **Serveur proxy**, cliquez sur le lien **Paramètres du serveur proxy**.



Paramètres de connexion du serveur proxy

4. Dans la fenêtre qui s'ouvre, choisissez une des options suivantes pour déterminer l'adresse du serveur proxy :

   - **Utiliser les paramètres du serveur proxy du système d'exploitation**.

     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. Sélectionnez le mode d'authentification de l'application sur le serveur proxy. Par défaut, l'application utilise l'authentification NTLM du domaine de l'utilisateur actuel.

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.

Restauration de la dernière mise à jour

Après la deuxième mise à jour des bases et modules d'application, la fonction de restauration des bases et modules d'application vers leurs versions précédentes devient disponible.

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. Il peut être utile de revenir à une version antérieure, par exemple si une nouvelle version de la base de données provoque un faux positif qui amène Kaspersky Endpoint Security à bloquer une application inoffensive.

Kaspersky Endpoint Security en mode Light Agent ne prend pas en charge la tâche *Annulation de la mise à jour*.

Comment revenir à la dernière mise à jour dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Nouvelle tâche**.

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

Étape 1. Sélection du type de tâche

1. Choisissez **Kaspersky Endpoint Security for Windows (14.2)** → **Annulation de la mise à jour**.

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

Configurez la planification de la tâche, par exemple, manuellement.

Étape 4. Définition du nom de la tâche

Saisissez un nom pour la tâche.

Étape 7. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment revenir à la dernière mise à jour dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Retour en arrière**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Restauration de la mise à jour*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

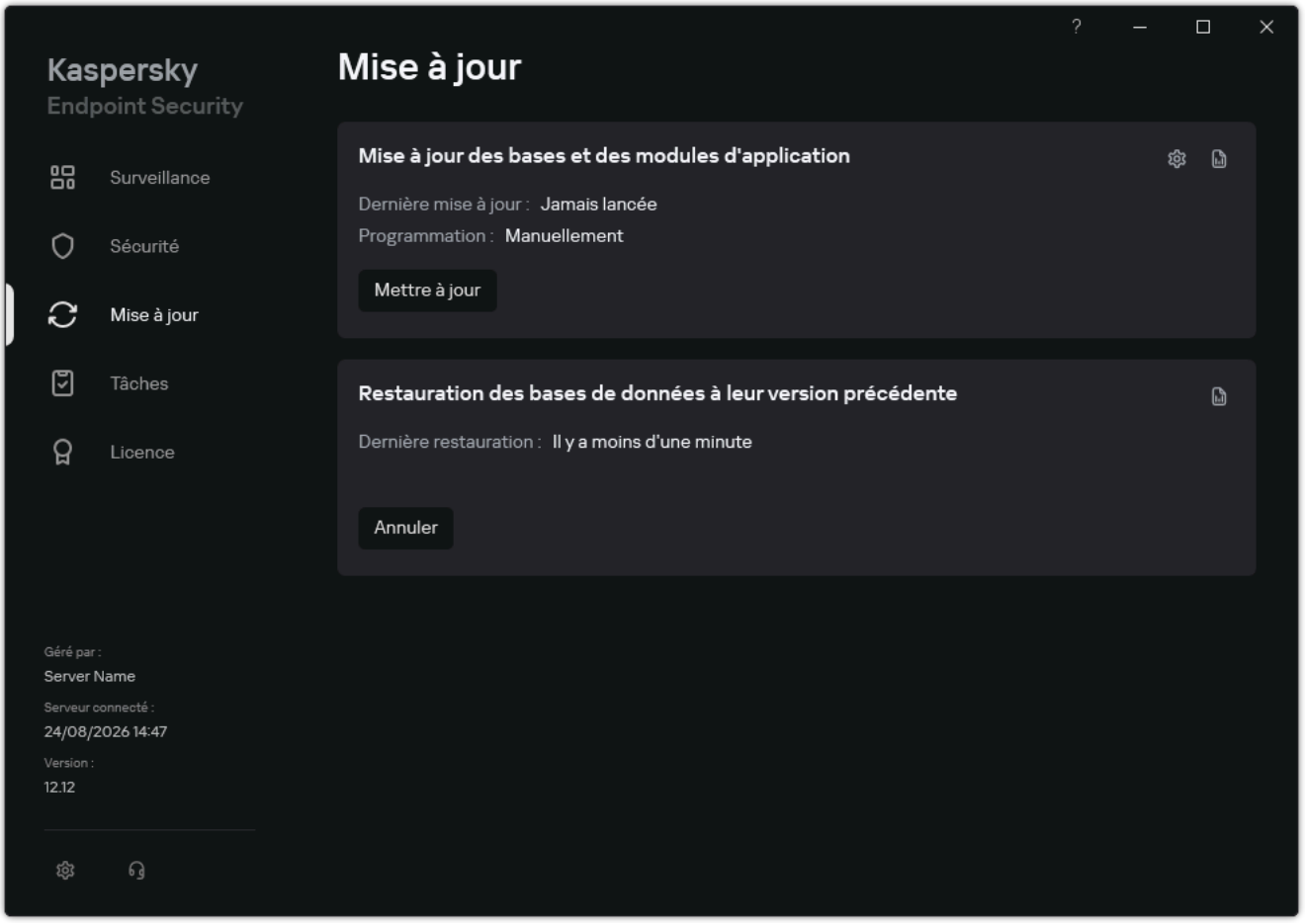
7. La nouvelle tâche apparaît dans la liste des tâches.

8. Cochez la case en regard de la tâche.

9. Cliquez sur **Démarrer**.

Comment revenir à la dernière mise à jour dans l'interface de l'application

1. Dans la fenêtre principale de l'application, accédez à la section **Mise à jour**.



Tâches de mise à jour locales

2. Dans la mosaïque **Restauration des bases de données à leur version précédente**, cliquez sur le bouton **Annuler**.

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 arrêter la tâche à tout moment en cliquant sur le bouton **Arrêter la mise à jour**.

Technologie de désinfection avancée

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 désinfection active dans les paramètres de la tâche *Analyse des logiciels malveillants* et dans les paramètres de l'application.

Si Kaspersky Endpoint Security ne peut pas arrêter l'exécution d'une application malveillante, vous pouvez utiliser la technologie de désinfection active. Pour les ordinateurs soumis à la stratégie, la désinfection avancée est désactivée par défaut, car cette technologie utilise une quantité importante de ressources informatiques. Pour les ordinateurs non soumis à la stratégie, la désinfection avancée est activée par défaut.

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 avancée immédiate dans les propriétés de la tâche *Analyse des logiciels malveillants*. Ce prérequis n'est pas nécessaire pour utiliser la technologie sur les postes de travail.

Procédure d'activation ou de désactivation de la technologie de désinfection active dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Dans le groupe **Général**, cochez ou décochez la case **Appliquer la technologie de désinfection avancée** pour activer ou désactiver la technologie de désinfection avancée.
5. Enregistrez vos modifications.

Procédure d'activation ou de désactivation de la technologie de désinfection active dans Web Console et Cloud Console

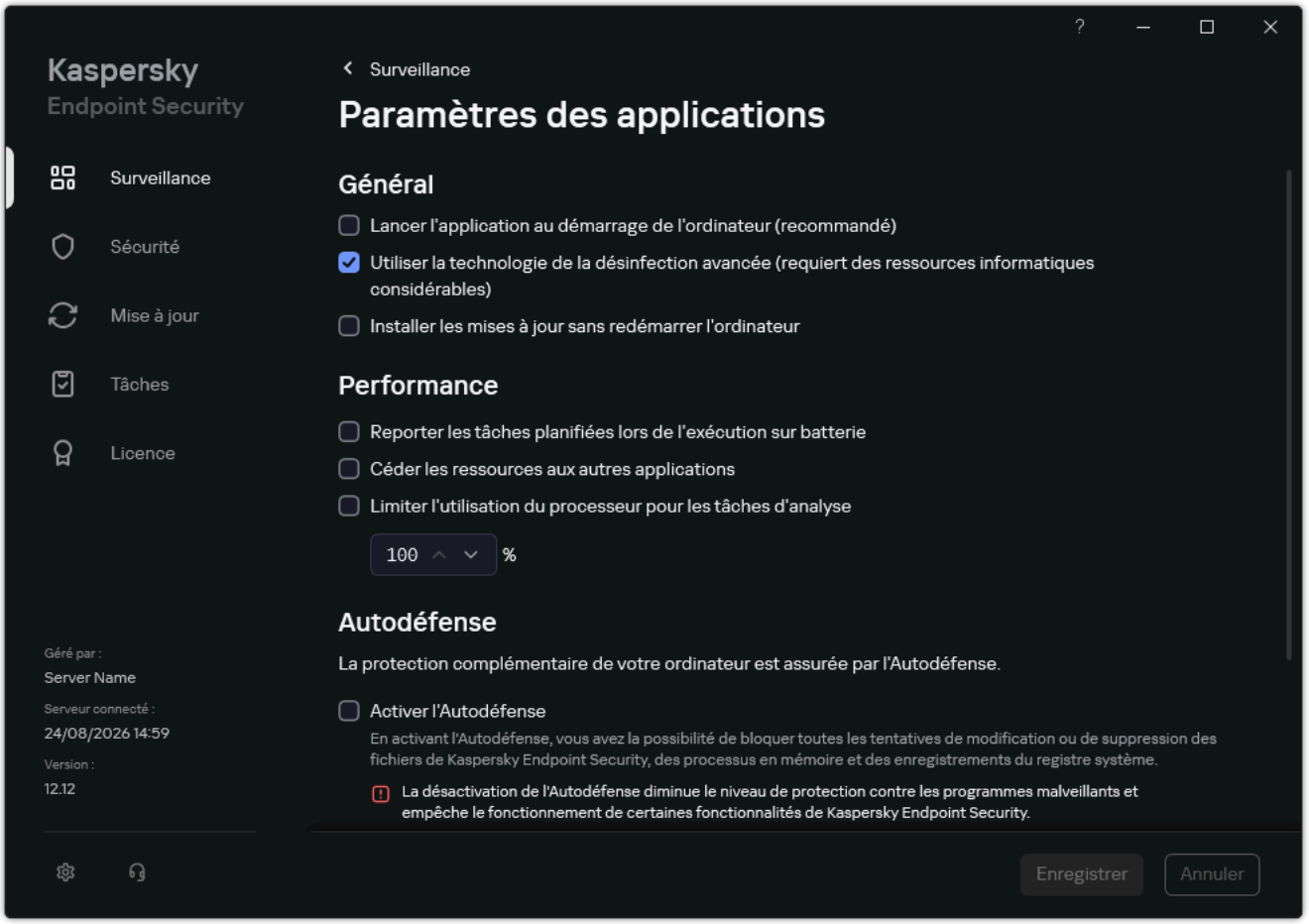
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Choisissez **Paramètres généraux** → **Paramètres de détection**.
5. Dans le groupe **Technologie de désinfection avancée**, utilisez le commutateur **Technologie de désinfection avancée ACTIVÉE** pour activer ou désactiver la technologie de désinfection avancée.
6. Enregistrez vos modifications.

Procédure d'activation ou de désactivation de la technologie de désinfection active 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

3. Dans le groupe **Général**, cochez ou décochez la case **Utiliser la technologie de la désinfection avancée (requiert des ressources informatiques considérables)** pour activer ou désactiver la technologie de désinfection avancée.

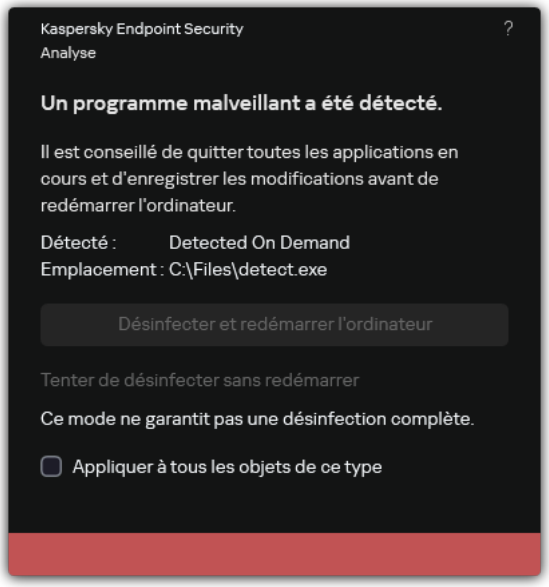
4. Enregistrez vos modifications.

Il en résulte que l'utilisateur ne peut pas utiliser la plupart des fonctionnalités du système d'exploitation pendant que la désinfection avancée est en cours. Lorsque la désinfection est terminée, l'ordinateur redémarre.

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 *Analyse des logiciels malveillants*. Il existe une case **Exécuter la désinfection avancée immédiatement** 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

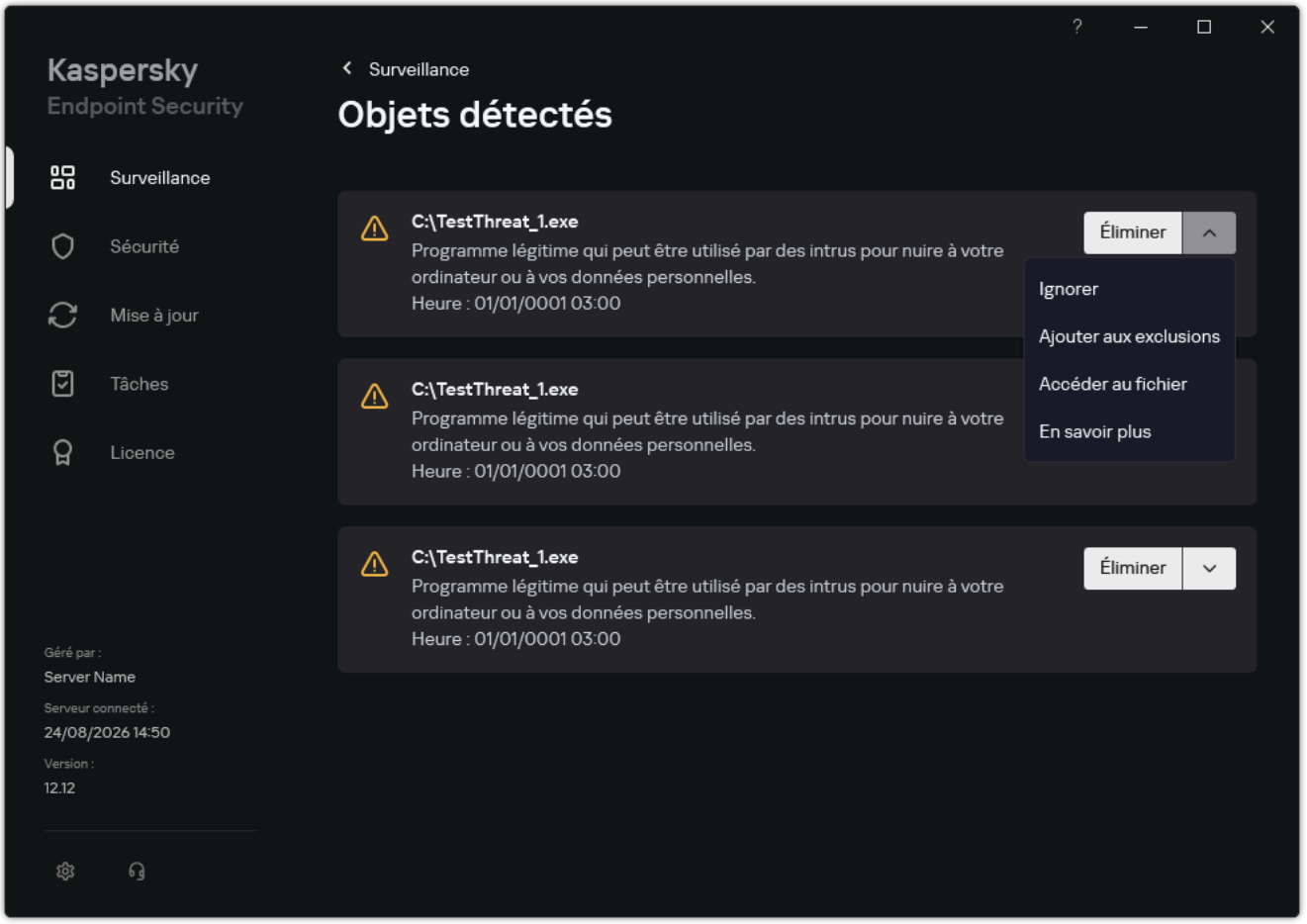
Pour traiter les menaces actives sur les serveurs, vous devez procéder comme suit :

- activer la technologie de désinfection active dans les paramètres de l'application ;
- activer la désinfection active immédiate dans les propriétés de la tâche *Analyse des logiciels malveillants*.

Si Kaspersky Endpoint Security est installé sur un ordinateur fonctionnant sous Windows for Servers, Kaspersky Endpoint Security n'affiche pas la notification. Par conséquent, vous ne pouvez pas sélectionner une action pour désinfecter une menace active. Pour désinfecter une menace, vous devez appliquer la technologie de désinfection avancée dans les paramètres de l'application et activer la désinfection immédiate de l'infection active dans les paramètres de la tâche *Analyse des logiciels malveillants*. Ensuite, vous devez démarrer la tâche *Analyse des logiciels malveillants*.

Élimination des menaces non traitées

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 (cf. ill. ci-après).



Une liste de menaces actives

Un fichier infecté est considéré comme *traité* si Kaspersky Endpoint Security a désinfecté le fichier ou supprimé la menace dans le cadre de l'analyse de l'ordinateur à la recherche de virus et d'autres programmes malveillants.

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 les paramètres de la tâche *Analyse des logiciels malveillants*, l'action sur la détection des menaces est définie sur **Informer**. Ensuite, lorsque la notification du fichier infecté s'est affichée à l'écran, l'utilisateur a sélectionné **Ignorer**.

S'il y a des menaces non traitées, Kaspersky Endpoint Security change l'icône en . Dans la fenêtre principale de l'application, la notification de menace s'affiche (cf. ill. ci-après). Dans la console de Kaspersky Security Center, l'état de l'ordinateur passe à *Critique* – .

Traitement d'une menace dans la Console d'administration (MMC)

1. Dans la Console d'administration, accédez au dossier **Serveur d'administration** → **Avancé** → **Stockages** → **Menaces actives**.

   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 :

   - **Réparer**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Supprimer**. Si cette option a été sélectionnée, l'application supprimera les fichiers infectés détectés du stockage actif des menaces. Dans ce cas, l'application conserve le fichier détecté dans la mémoire de l'ordinateur. Pour éliminer la menace de l'ordinateur, sélectionnez **Réparer**.

Traitement d'une menace dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages** → **Menaces actives**.

   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 :

   - **Réparer**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Supprimer**. Si cette option a été sélectionnée, l'application supprimera les fichiers infectés détectés du stockage actif des menaces. Dans ce cas, l'application conserve le fichier détecté dans la mémoire de l'ordinateur. Pour éliminer la menace de l'ordinateur, sélectionnez **Réparer**.

Traitement d'une menace dans l'interface de l'application

1. Dans la fenêtre principale de l'application, dans la section **Surveillance**, cliquez sur la mosaïque **La protection est menacée**.

   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, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Ajouter aux exclusions**. Si cette action est sélectionnée, Kaspersky Endpoint Security propose d'ajouter le fichier à la liste des exclusions d'analyse. Les paramètres de l'exclusion sont configurés automatiquement. S'il est impossible d'ajouter une exclusion, cela signifie que l'administrateur a désactivé l'ajout d'exclusions dans les paramètres de la stratégie.

   - **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.

- **En savoir plus**. Si cette option est sélectionnée, Kaspersky Endpoint Security ouvre le site Internet Base de données des vulnérabilités et des menaces de Kaspersky.

Pour traiter les menaces actives dans la console de Kaspersky Security Center, vous devez activer le transfert des informations sur les fichiers non traités vers le Serveur d'administration. Le transfert de données est activé par défaut.

Activation du transfert des données de fichiers non traitées dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Transfert des données au Serveur d'administration**.
5. Cochez la case **Fichiers non traités**.
6. Enregistrez vos modifications.

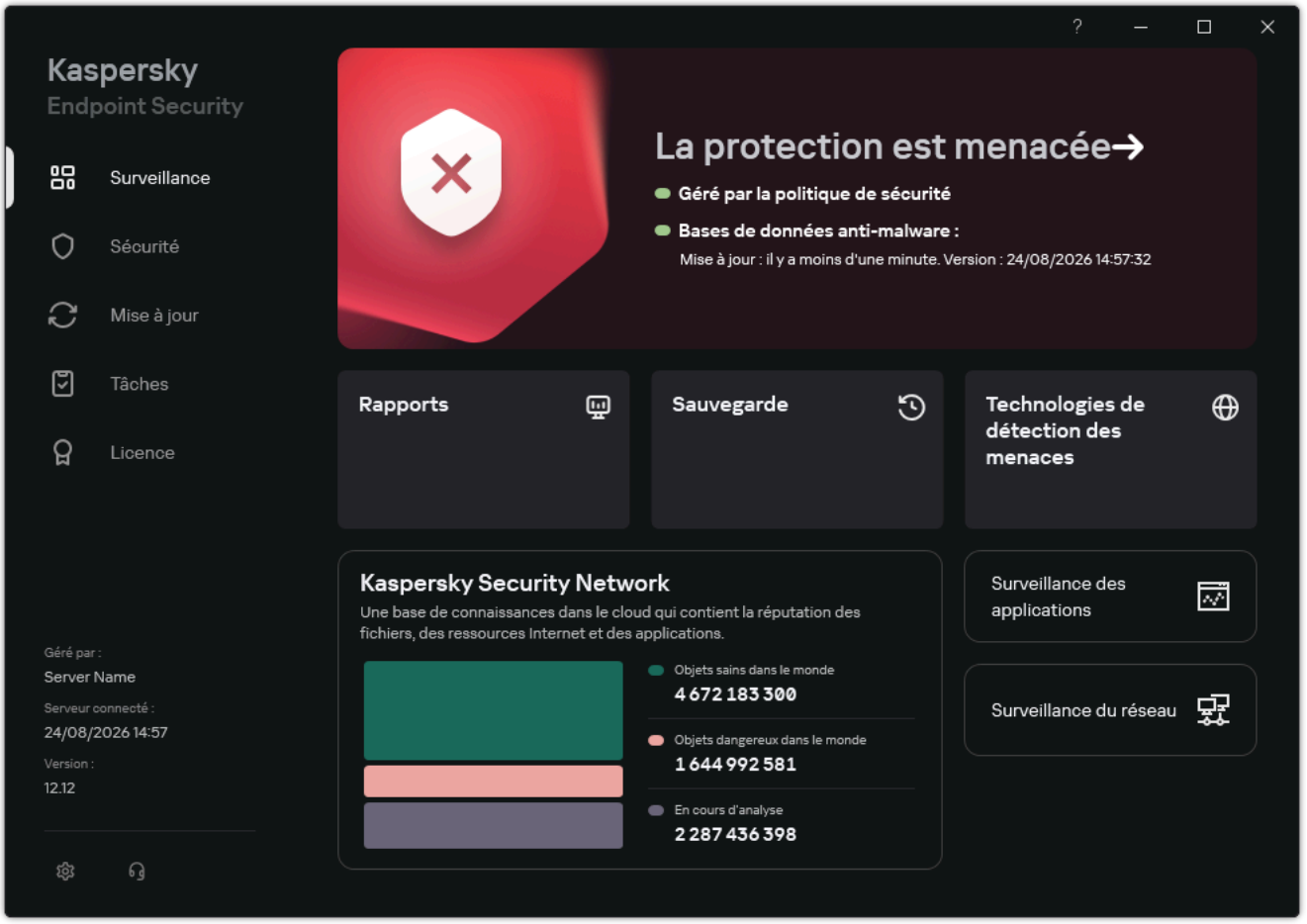
Activation du transfert des données de fichiers non traitées dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.

5. Dans le groupe **Transfert des données au Serveur d'administration**, cochez la case **À propos des fichiers non traités**.

6. Enregistrez vos modifications.



Fenêtre principale de l'application lorsqu'une menace est détectée

Protection de l'ordinateur

État de la Protection en temps réel

Kaspersky Endpoint Security transmet le paramètre **État de la protection en temps réel** au Serveur d'administration de Kaspersky Security Center. La valeur de ce paramètre dépend de l'état actuel des modules de protection de l'application sur l'ordinateur protégé (consultez le tableau ci-dessous).

Kaspersky Endpoint Security détermine l'état de la protection en temps réel en fonction de l'état des modules suivants de l'application :

- Protection contre les fichiers malicieux.
- Protection contre les menaces Internet.
- Protection contre les menaces par emails.
- Protection AMSI.
- Protection BadUSB.
- Protection contre les menaces réseau.
- Pare-feu.
- Protection contre les Exploits.
- Détection comportementale.
- Réparation des actions malicieuses.
- Prévention des intrusions.

Vous pouvez vérifier l'état de la protection en temps réel de l'application dans une console de Kaspersky Security Center.

Comment connaître l'état de la Protection en temps réel dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Appareils administrés**.

   L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de la protection en temps réel**. Si la colonne **État de la protection en temps réel** est absente, gérez les paramètres des colonnes en cliquant sur le lien **Ajouter ou supprimer des colonnes**.

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Appareils administrés**.

L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de la protection en temps réel**. Si la colonne **État de la protection en temps réel** est absente, gérez les paramètres des colonnes en cliquant sur le lien **Ajouter ou supprimer des colonnes**.

Comment connaître la Protection en temps réel de l'ordinateur dans Web Console

Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de protection en temps réel ;**. Si la colonne **État de protection en temps réel ;** est absente, gérez les paramètres des colonnes (⚙).

Valeurs possibles du paramètre État de la protection en temps réel

Valeur	Description
Inconnu	Le Serveur d'administration ne dispose d'aucune information sur l'état de la protection en temps réel de cet ordinateur.
Non installé(e)	Aucun module n'est installé.
Non pris en charge par la licence	L'application n'est pas activée ou la licence ne permet pas aux modules installés de fonctionner.
Échec	Un ou plusieurs modules présentent un dysfonctionnement.
Arrêté(e)	Un ou plusieurs modules sont désactivés.
Suspendu(e)	Un ou plusieurs modules sont suspendus.
En cours de démarrage	Un ou plusieurs modules sont en cours d'activation.
En cours d'exécution	Les modules de l'application sont opérationnels.

Si la valeur du paramètre **État de la protection en temps réel** dans Kaspersky Security Center est différente de *En cours d'exécution*, vérifiez que les modules installés de Kaspersky Endpoint Security figurant dans la liste sont activés et que l'application est activée.

Protection contre les fichiers malicieux

Le module Protection contre les fichiers malicieux vous permet d'empêcher l'infection du système de fichiers de l'ordinateur. Par défaut, le module Protection contre les fichiers malicieux réside en permanence dans la mémoire vive (RAM) de l'ordinateur et analyse en temps réel tous les fichiers ouverts, enregistrés ou exécutés. Ce module analyse les fichiers sur tous les disques de l'ordinateur, y compris 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 un utilisateur ou une 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.

Lorsque vous essayez d'accéder à un fichier dont le contenu se trouve dans le stockage cloud 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. Ces groupes de paramètres stockés dans l'application sont appelés *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.

Le module Protection contre les fichiers malicieux utilise les données reçues d'autres modules de l'application. L'activation de ces modules est facultative. Les modules qui fournissent des données supplémentaires sont les suivants :

- Kaspersky Security Network.
- Prévention des intrusions.
- Détection comportementale.

Procédure d'activation ou de désactivation du module Protection contre les fichiers malicieux dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.
4. Utilisez la case **Protection contre les fichiers malicieux** pour activer ou désactiver le module.
5. Si vous avez activé le module, réalisez l'une des opérations suivantes dans le groupe **Niveau de sécurité** :
   - 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.
     - **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** et définissez vos propres paramètres du module (voir le tableau ci-dessous).

  Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Par défaut**.

6. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

   - **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier.

   - **Bloquer**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.

   - **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, l'application 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.

7. Enregistrez vos modifications.

Procédure d'activation ou de désactivation du module Protection contre les fichiers malicieux dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.

5. Utilisez le commutateur **Protection contre les fichiers malicieux ACTIVÉE** pour activer ou désactiver le module.

6. Si vous voulez ajouter un nouvel objet à la zone de protection, procédez comme suit :

   a. Sous les **Paramètres avancés**, sélectionnez l'onglet **Zone de protection**.

   b. Cliquez sur **Ajouter**.

   c. Dans la fenêtre qui s'ouvre, sélectionnez les objets que vous souhaitez ajouter à la zone de protection.

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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Vous pouvez utiliser des masques n'importe où dans un chemin de fichier ou de dossier. Par exemple, si vous souhaitez que la zone d'analyse inclue le dossier Téléchargements pour tous les comptes sur l'ordinateur, saisissez le masque `C:\Users\*\Downloads\`.

Dans la zone de protection, vous pouvez exclure un objet de la protection sans le supprimer de la liste des objets. Pour ce faire, mettez le commutateur situé à côté en position d'arrêt.

d. Enregistrez vos modifications.

7. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

- **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

- **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier.

- **Bloquer**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.

Avant de tenter de désinfecter ou de supprimer un fichier infecté, l'application 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.

8. Si nécessaire, modifiez les paramètres avancés de la Protection contre les fichiers malicieux.

9. Enregistrez vos modifications.

Comment activer ou désactiver le module Protection contre les fichiers malicieux 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 **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 le groupe **Niveau de sécurité** :

   - 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.

     - **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 (voir le tableau ci-dessous).

     Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut**.

5. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

   - **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier.

   - **Interdire**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.

   - **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, l'application 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.

6. 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, l'application 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	**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.
Utiliser la technologie iSwift	**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 iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.
Utiliser la 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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Analyser les fichiers au format de messagerie	**Activé**	Analyse les fichiers au format de messagerie. L'application analyse les fichiers MSG et EML. Les fichiers au format de messagerie incluent également des objets OLE et des fichiers MHT. Kaspersky Endpoint Security analyse les fichiers au format de messagerie dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Mode d'analyse	**Mode intelligent**	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 la désinfection est impossible**	Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **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, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier.

   - **Interdire**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer.

   Avant de tenter de désinfecter ou de supprimer un fichier infecté, l'application 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur **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, l'application 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, l'application 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 **Ajouter**.

      L'arborescence des dossiers s'ouvre.

   b. Dans le champ **Chemin**, saisissez le chemin d'accès au dossier ou au fichier.

      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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

      Vous pouvez utiliser des masques n'importe où dans un chemin de fichier ou de dossier. Par exemple, si vous souhaitez que la zone d'analyse inclue le dossier Téléchargements pour tous les comptes sur l'ordinateur, saisissez le masque `C:\Users\*\Downloads\`.

      L'objet **Cet ordinateur** dans la liste des ressources de fichiers de l'ordinateur contient les objets suivants : **Tous les disques durs**, **Tous les disques réseau** et **Tous les disques amovibles**.

   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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur **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 : **Superficielle**, **Moyenne** ou **Minutieuse**.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur **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 :

   - **Utiliser la technologie iSwift**. 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 iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.

   - **Utiliser la 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Optimisation**, 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 ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR et ICE, 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.
3. Cliquez sur **Paramètres avancés**.
4. 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 de messagerie ou 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 volumineux**.

     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 volumineux** 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Mode d'analyse**, sélectionnez le mode requis :

   - **Mode intelligent**. 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.

   - **Ouverture et 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.

   - **Ouverture**. 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.

   - **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.

Analyser les conteneurs.

Un *conteneur* est un environnement isolé dans lequel une application peut s'exécuter sans interagir directement avec le système d'exploitation. L'utilisation de conteneurs comporte les risques suivants :

- Les pirates peuvent être en mesure d'exploiter les vulnérabilités de la conteneurisation pour compromettre les applications à l'intérieur du conteneur.
- Les pirates informatiques peuvent exploiter une configuration non sécurisée de l'environnement du conteneur pour obtenir un accès non autorisé aux données de l'ordinateur ou pour compromettre l'intégrité du système.
- Une attaque réussie sur un conteneur peut permettre à un pirate d'accéder aux données de l'ordinateur.
- Les pirates informatiques sont susceptibles d'exploiter les vulnérabilités du réseau pour en intercepter le trafic.

Kaspersky Endpoint Security analyse les fichiers non seulement sur les disques, mais aussi à l'intérieur des conteneurs. Autrement dit, Kaspersky Endpoint Security est un outil externe permettant de détecter les outils malveillants à l'intérieur des conteneurs. Cela permet de maintenir les performances des conteneurs et d'éviter les conflits avec d'autres applications à l'intérieur des conteneurs. L'installation de Kaspersky Endpoint Security à l'intérieur du conteneur n'est pas prise en charge.

En plus d'assurer la sécurité des conteneurs, Kaspersky Endpoint Security permet de gérer les applications à l'intérieur des conteneurs à l'aide du Contrôle des applications. Le Contrôle des applications est configuré pour les conteneurs de la même manière que pour les applications installées sur l'ordinateur. Contrôle de l'intégrité du système prend également en charge les conteneurs.

Exigences relatives au conteneur

- Le conteneur doit être un conteneur Docker. Les autres outils de conteneurisation ne sont pas pris en charge.
- Le conteneur doit fonctionner en mode d'isolation du processus. Le mode d'isolation de Hyper-V n'est pas pris en charge.
- Le conteneur doit être placé sur un serveur Windows Serveur 2016, 2019 ou 2022 (Docker Host).
- Le conteneur doit inclure une image système Windows (Docker Image). Windows 10 et 11 ne sont pas pris en charge. Les images Linux ne sont pas prises en charge.

Action en cas de détection d'une menace

Si une menace est détectée à l'intérieur d'un conteneur, l'application applique l'action sélectionnée pour le module de Protection contre les menaces sur les fichiers. Analyser les conteneurs présente des paramètres supplémentaires (voir les instructions ci-dessous). Si une menace est détectée, l'application bloque l'activité malveillante et exécute l'action sélectionnée (par exemple, tente de désinfecter l'objet). Kaspersky Endpoint Security peut arrêter le conteneur si l'objet détecté ne peut pas être désinfecté. Par défaut, la fonctionnalité d'arrêt des conteneurs est désactivée.

Comment configurer l'analyse des conteneurs dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les fichiers malicieux**.
4. Cliquez sur **Paramètres**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Avancé**.
6. Dans le groupe **Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows**, configurer les paramètres d'analyse des conteneurs :
   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.
   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.
7. Enregistrez vos modifications.

Comment configurer l'analyse des conteneurs dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**.
5. Sous les **Paramètres avancés**, sélectionnez l'onglet **Performances**.
6. Dans le groupe **Optimisation de l'analyse**, configurer les paramètres d'analyse des conteneurs :
   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.
   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.
7. Enregistrez vos modifications.

Comment configurer l'analyse des conteneurs 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 **Protection principale** → **Protection contre les fichiers malicieux**.

3. Dans le groupe **Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows**, configurer les paramètres d'analyse des conteneurs :

   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.

   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.

4. 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 *privilèges 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 module 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. 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.

Activation et désactivation de la Prévention des intrusions

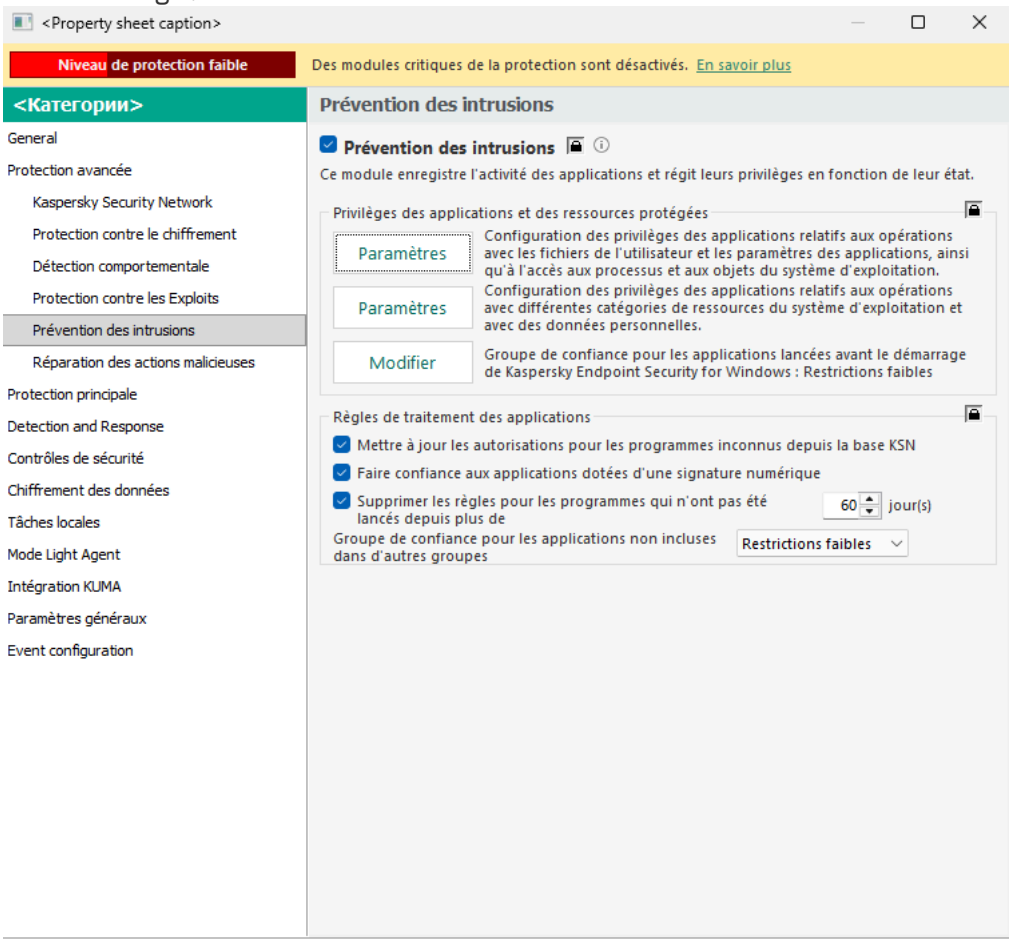
Par défaut, le module Prévention des intrusions est activé et fonctionne dans le mode recommandé par les experts de Kaspersky.

Procédure d'activation ou de désactivation du module Prévention des intrusions dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Utilisez la case **Prévention des intrusions** pour activer ou désactiver le module.

5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Utilisez le commutateur **Prévention des intrusions ACTIVÉE** 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 sélectionner un groupe de confiance dans lequel Kaspersky Endpoint Security placera automatiquement toutes les applications inconnues. Les applications qui étaient exécutées avant le démarrage de Kaspersky Endpoint Security sont automatiquement placées dans le groupe de confiance défini dans les paramètres de prévention des intrusions sur l'hôte.

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.

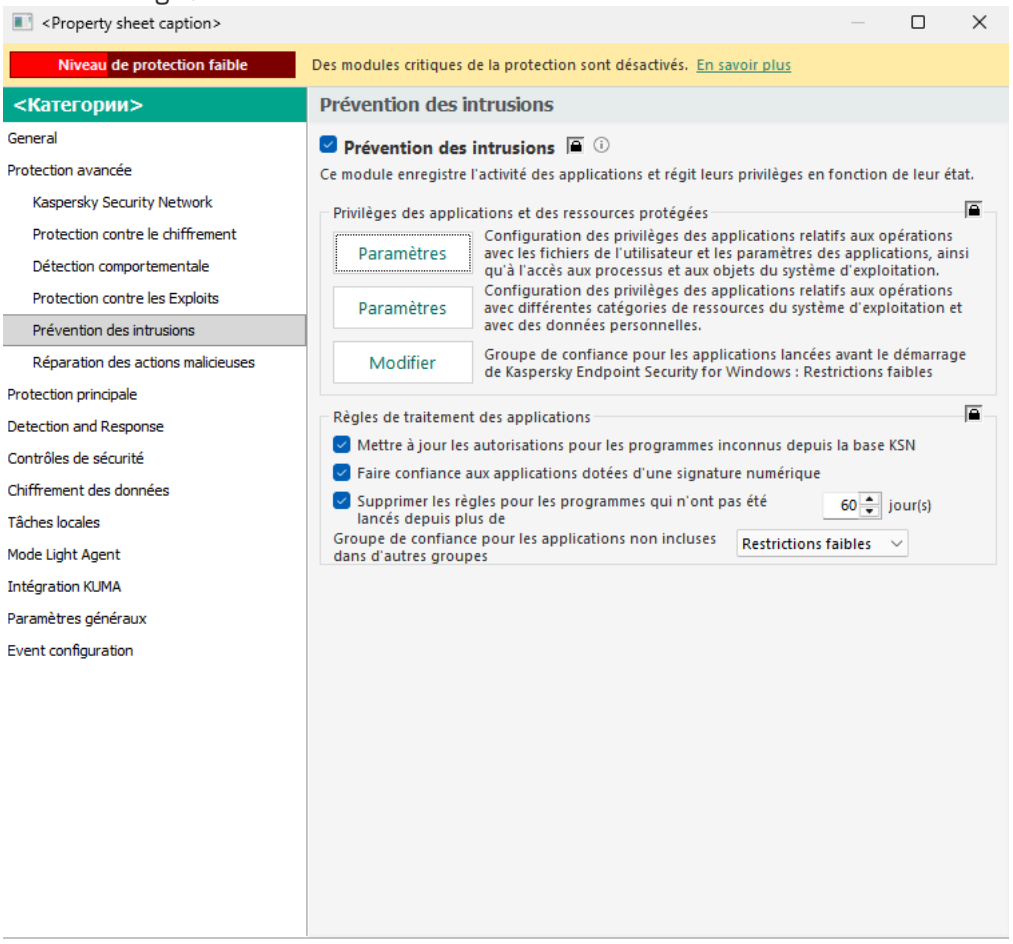
Les experts de Kaspersky déconseillent de déplacer les applications du groupe de confiance défini automatiquement dans un autre groupe de confiance. Au lieu de cela, modifiez le cas échéant les privilèges de l'application en question.

Procédure de modification du groupe de confiance d'une application dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Cliquez sur le bouton **Paramètres** dans le groupe **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

5. Sélectionnez l'onglet **Privilèges des applications**.

6. Cliquez sur **Ajouter**.

7. 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.

8. Cliquez sur **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.

9. Sélectionnez l'application requise.

10. Dans la liste déroulante **Ajoutez l'application sélectionnée au groupe de confiance**, sélectionnez le groupe de confiance nécessaire pour l'application.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Procédure de modification du groupe de confiance d'une application dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.
5. Dans le groupe **Privilèges des applications et des ressources protégées**, cliquez sur le lien **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.
6. Sélectionnez 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 **Ajouter**.

   Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.
8. Sélectionnez le groupe de confiance pertinent pour l'application.
9. Sélectionnez le type **Application**. Passez à l'étape suivante.

   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.

    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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.
3. Cliquez sur **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, cliquez sur **Restrictions** → **<groupe de confiance>**.

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 *(défini par l'utilisateur)* 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

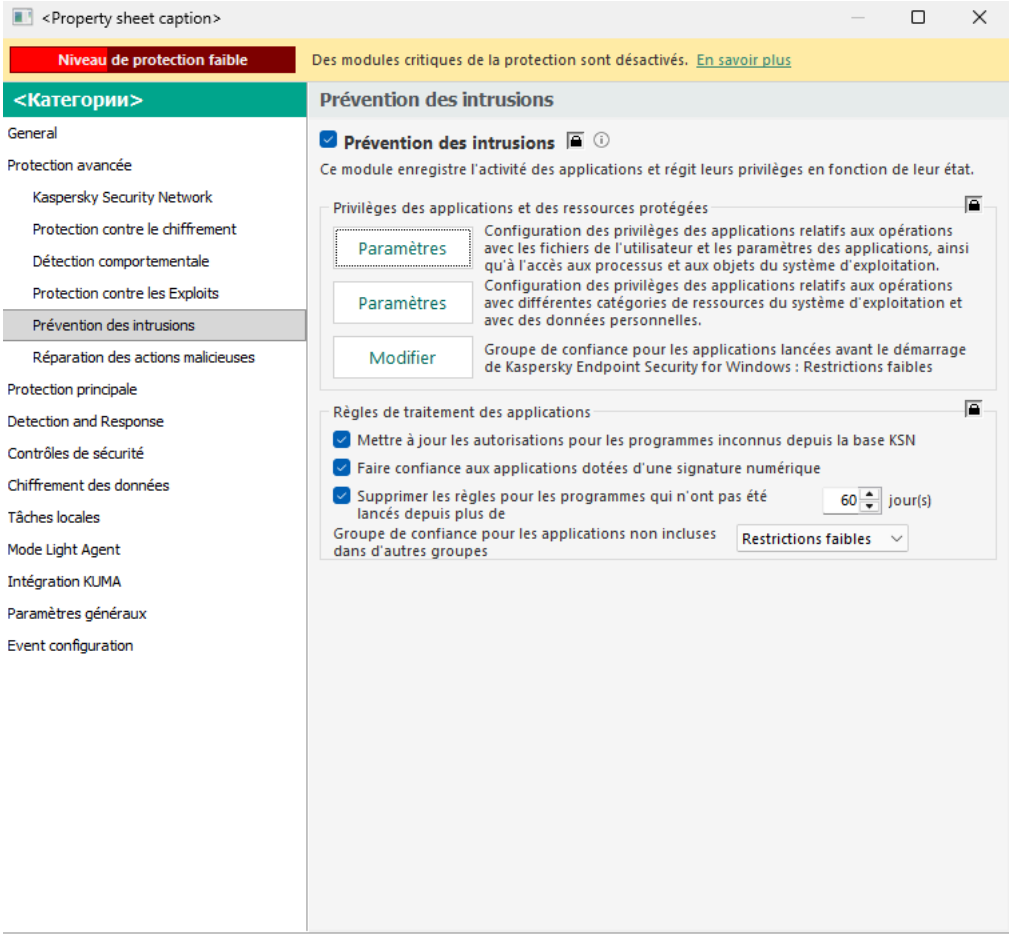
Les privilèges d'application optimaux sont créés par défaut pour différents groupes de confiance. Les paramètres des privilèges de groupes d'applications qui font partie du groupe de confiance héritent des valeurs des paramètres des privilèges des groupes de confiance.

Modification des privilèges des groupes de confiance dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Cliquez sur le bouton **Paramètres** dans le groupe **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

5. Rendez-vous dans l'onglet **Privilèges des applications**.

6. Sélectionnez le groupe de confiance requis.

7. Dans le menu contextuel du groupe de confiance, sélectionnez l'option **Privilèges des groupes**.

   Cette action ouvre les propriétés du groupe de confiance.

8. 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 **Fichiers et registre système**.

   - 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 module Pare-feu à l'aide de *règles réseau*.

9. 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** (⊘).

10. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Consigner 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. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Dans le groupe **Privilèges des applications et des ressources protégées**, cliquez sur le lien **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

6. Rendez-vous dans 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 registre système**.

   - 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 module 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** ( ), **Bloquer** ( ).

10. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Consigner 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. Dans la fenêtre principale de l'application, cliquez sur le bouton .

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.

3. Cliquez sur **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 **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 module 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 **Consigner 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 personnalisés*) sera attribué au groupe de confiance.

Sélection du groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security

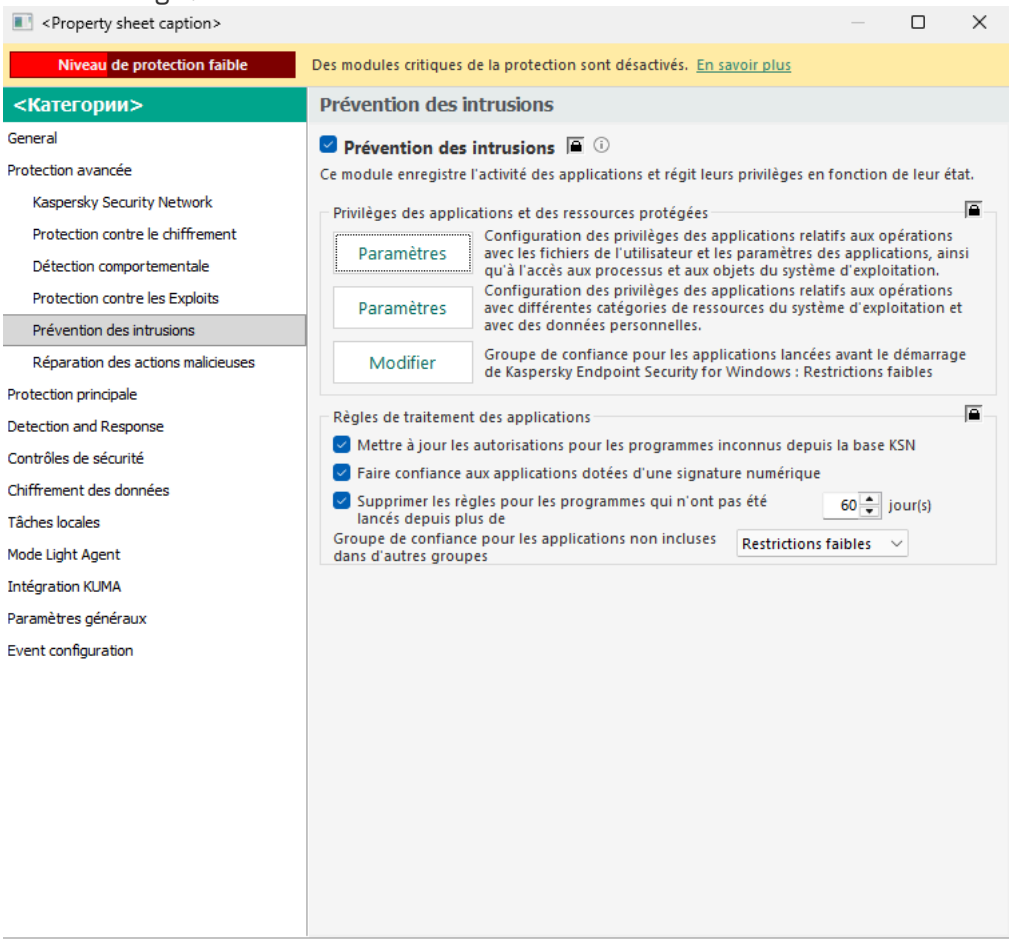
S'agissant des applications lancées avant Kaspersky Endpoint Security, le contrôle porte uniquement sur leur activité réseau. Le contrôle s'opère selon les règles réseau définies dans les paramètres du pare-feu. Pour désigner les règles réseau qui doivent régir le contrôle de l'activité réseau de ces 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Cliquez sur le bouton **Modifier** dans le groupe **Privilèges des applications et des ressources protégées**.

5. Pour le paramètre **Groupe de confiance pour les applications lancées avant que Kaspersky Endpoint Security**, sélectionnez le groupe de confiance approprié.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Pour le paramètre **Groupe de confiance pour les applications lancées avant que Kaspersky Endpoint Security**, sélectionnez le groupe de confiance approprié.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.

3. Dans le groupe **Groupe de confiance pour les applications lancées avant le démarrage de Kaspersky Endpoint Security**, sélectionnez le groupe de confiance approprié.

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

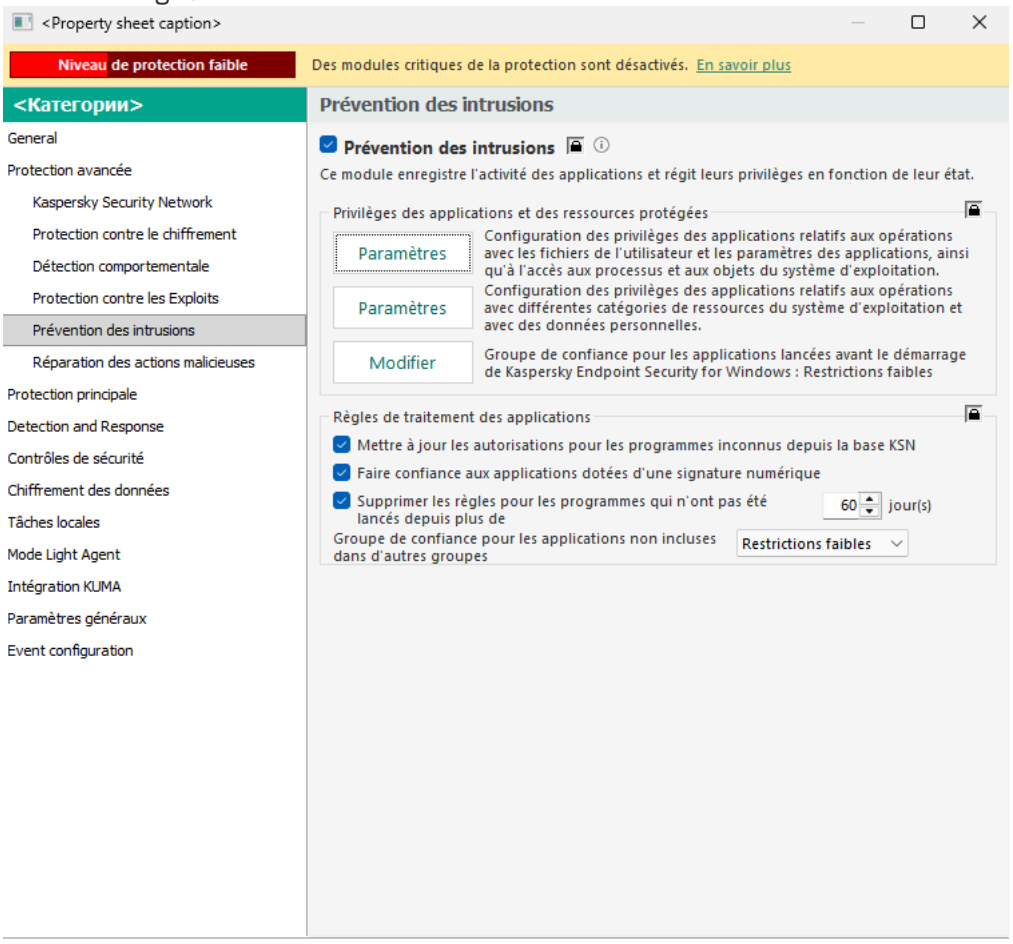
Lors du premier démarrage d'une application, le module Prévention des intrusions détermine le groupe de confiance pour l'application. Si vous n'avez pas accès Internet ou si Kaspersky Security Network ne dispose d'aucune information à propos de cette application, Kaspersky Endpoint Security placera l'application 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Dans le groupe **Règles de traitement des applications**, utilisez la liste déroulante **Groupe de confiance pour les applications non incluses dans 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.

5. Utilisez la case **Mettre à jour les autorisations pour les programmes inconnus depuis la base KSN** pour configurer la mise à jour automatique des privilèges des applications inconnues.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Dans le groupe **Règles de traitement des applications**, utilisez la liste déroulante **Groupe de confiance pour les applications non incluses dans 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 autorisations pour les programmes inconnus depuis la base 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.

3. Dans le groupe **Règles de traitement des applications**, 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 règles pour les programmes inconnus jusqu'ici de 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

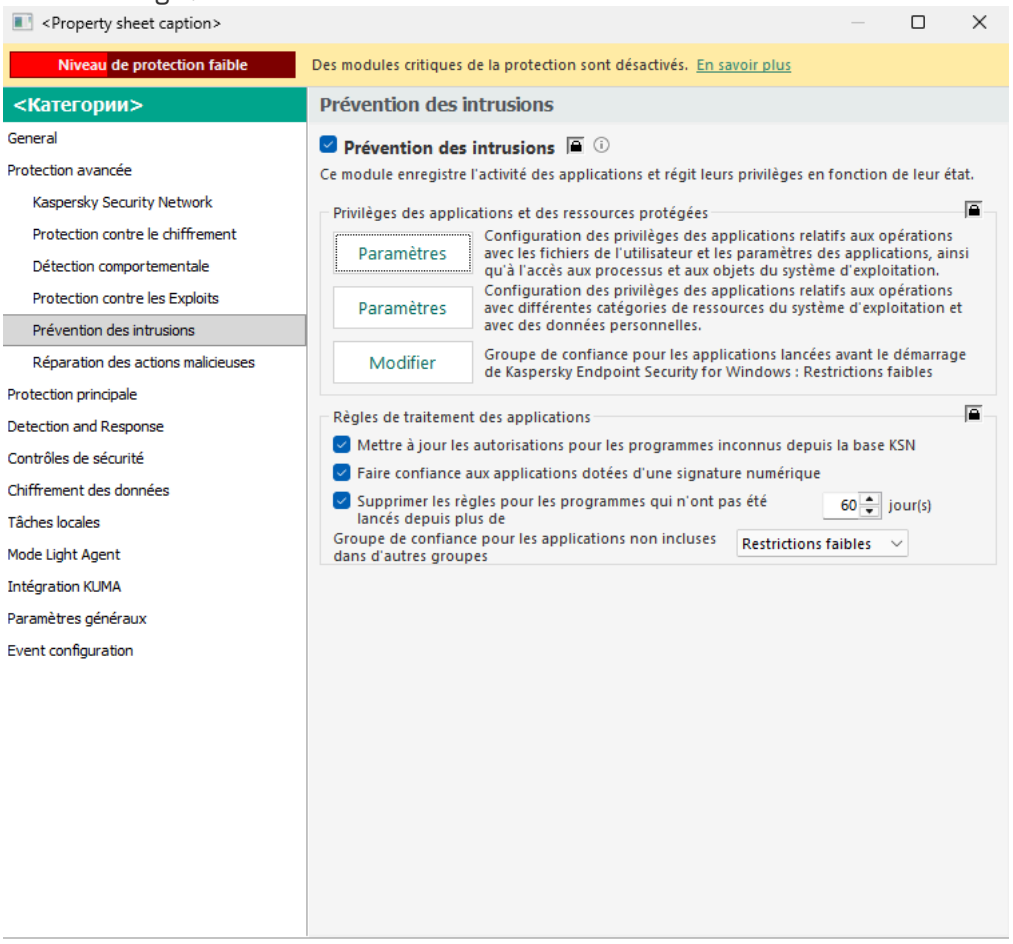
Kaspersky Endpoint Security place toujours les applications signées par des certificats Microsoft ou des certificats Kaspersky dans le groupe *De confiance*.

Comment sélectionner un groupe de confiance pour les applications dotées d'une signature numérique dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. 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 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.

5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **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 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 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.

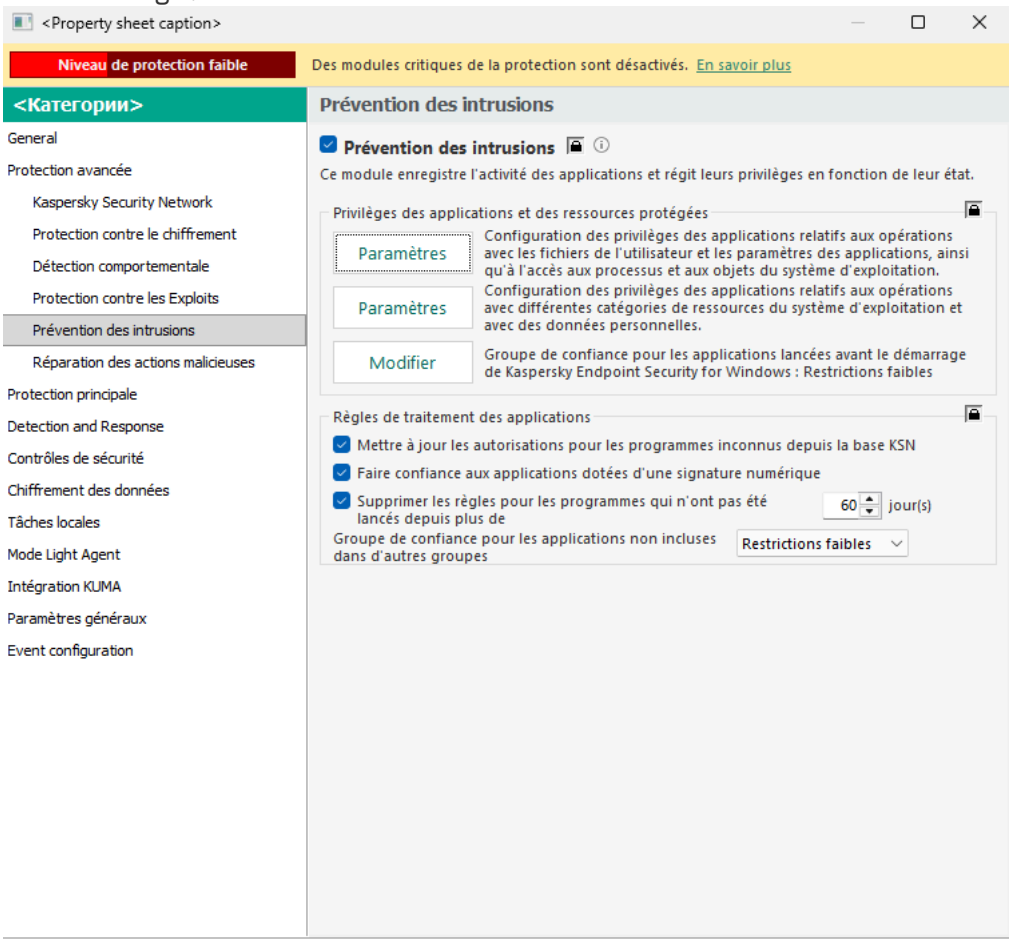
Les règles que vous créez pour les applications sont héritées par des applications enfants. Par exemple, si vous avez interdit toute activité réseau au programme cmd.exe, cette interdiction s'appliquera au programme notepad.exe s'il a été exécuté avec cmd.exe. Lorsqu'une application n'est pas un enfant 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Cliquez sur le bouton **Paramètres** dans le groupe **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

5. Rendez-vous dans l'onglet **Privilèges des applications**.

6. Cliquez sur **Ajouter**.

7. 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.

8. Cliquez sur **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.

9. Sélectionnez l'application requise.

10. Dans la liste déroulante **Ajoutez l'application sélectionnée au groupe de confiance**, sélectionnez **Groupes par défaut**, puis cliquez sur **OK**.

    L'application sera ajoutée au groupe par défaut.

11. Sélectionnez l'application concernée, puis sélectionnez **Privilèges des applications** dans le menu contextuel de l'application.

    Les propriétés de l'application s'ouvrent.

12. 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 **Fichiers et registre système**.

    - 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 module Pare-feu à l'aide de *règles réseau*.

13. 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** (⊘).

14. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Consigner 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.

15. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Modification des privilèges des applications dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Dans le groupe **Privilèges des applications et des ressources protégées**, cliquez sur le lien **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

6. Rendez-vous dans 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 **Ajouter**.

   Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.

8. Sélectionnez le groupe de confiance pertinent pour l'application.

9. Sélectionnez le type **Application**. Passez à l'étape suivante.

   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.

    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 registre système**.

    - 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 module 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** ( ), **Bloquer** ( ).

15. Si vous souhaitez surveiller l'utilisation des ressources informatiques, sélectionnez **Consigner 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. Dans la fenêtre principale de l'application, cliquez sur le bouton .

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.

3. Cliquez sur **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 **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**.

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 **Consigner 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 par l'application	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. Vous pouvez configurer le contrôle de l'activité des applications pour différents modules de Kaspersky Endpoint Security : • **Ne pas surveiller les modules de protection et de contrôle**. 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 surveiller pour Managed Detection and Response et Endpoint Detection and Response**. L'activité de l'application est surveillée par l'agent MDR intégré et l'agent EDR (KATA) intégré. • **Ne pas intercepter les entrées interactives de la console pour Endpoint Detection and Response**. Kaspersky Endpoint Security n'envoie pas de données télémétriques sur la gestion de l'application dans la console. Les données de télémétrie sont utilisées par Kaspersky Anti Targeted Attack Platform (EDR).
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 applications enfants	Kaspersky Endpoint Security ne surveille pas l'activité des fichiers ni du réseau des applications qui sont lancées par cette application. Vous pouvez appliquer l'exclusion de manière récursive. Ainsi, l'application ne surveille pas l'activité de toute la chaîne d'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 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. Kaspersky Endpoint Security version 14.0 ou antérieure ne permet pas d'exclure le trafic réseau si un hachage est spécifié pour une application de confiance à la place d'un chemin d'accès.

Protection des ressources du système d'exploitation et des données personnelles

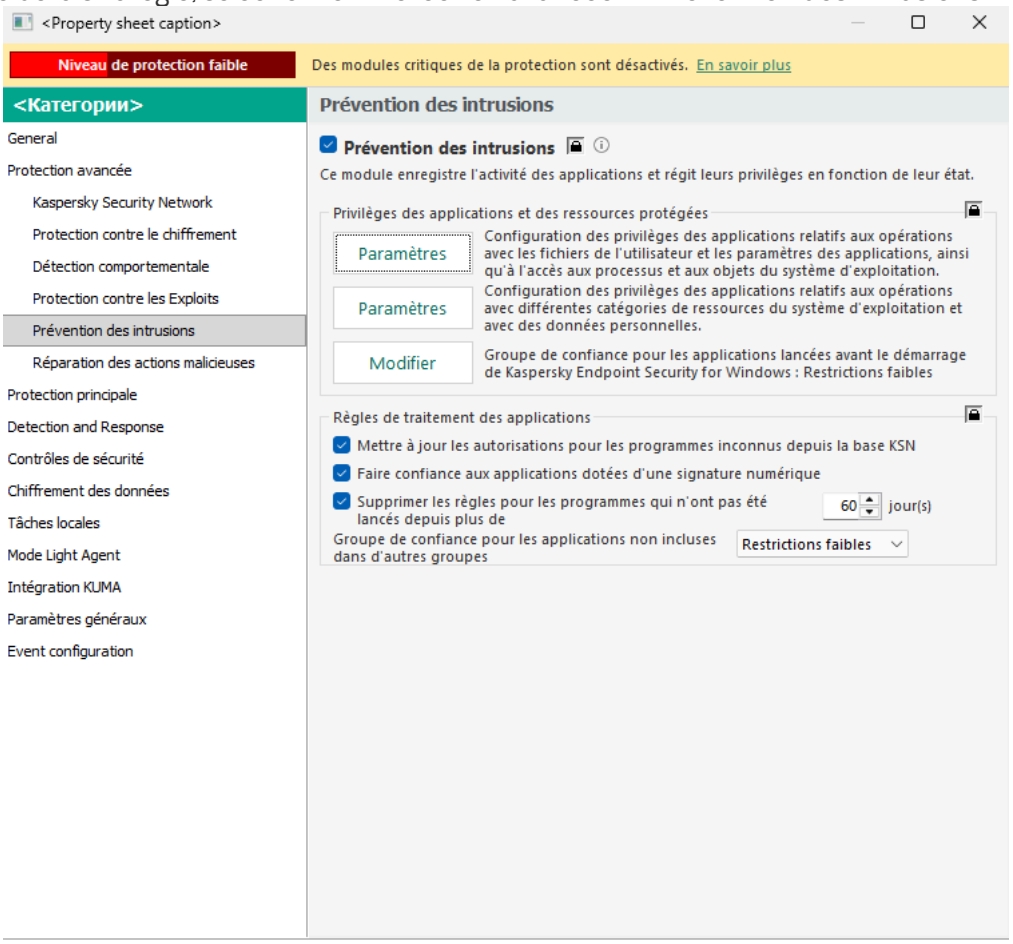
Le module Prévention des intrusions gère les privilèges des applications relatifs aux opérations sur différentes catégories de ressources du système d'exploitation et de données personnelles. Les experts de Kaspersky ont sélectionné des catégories de ressources à protéger. Par exemple, la catégorie *Système d'exploitation* comporte une sous-catégorie *Paramètres de lancement automatique* 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. Cliquez sur le bouton **Paramètres** dans le groupe **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

5. Rendez-vous dans 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.

6. 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**.

7. Appuyez sur le bouton **Ajouter**. Dans la liste déroulante, sélectionnez le type de ressource que vous souhaitez ajouter : **Fichier ou dossier**, ou **Clé de registre**.

8. 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.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Prévention des intrusions**.

5. Dans le groupe **Privilèges des applications et des ressources protégées**, cliquez sur le lien **Privilèges des applications et des ressources protégées**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

6. Rendez-vous dans 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 **Ajouter**.

   L'Assistant de nouvelles ressources démarre.

8. Dans le bloc **Nom du groupe**, sélectionnez 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.

    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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection avancée** → **Prévention des intrusions**.

3. Cliquez sur **Administration des 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. Appuyez 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 **Activer 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).

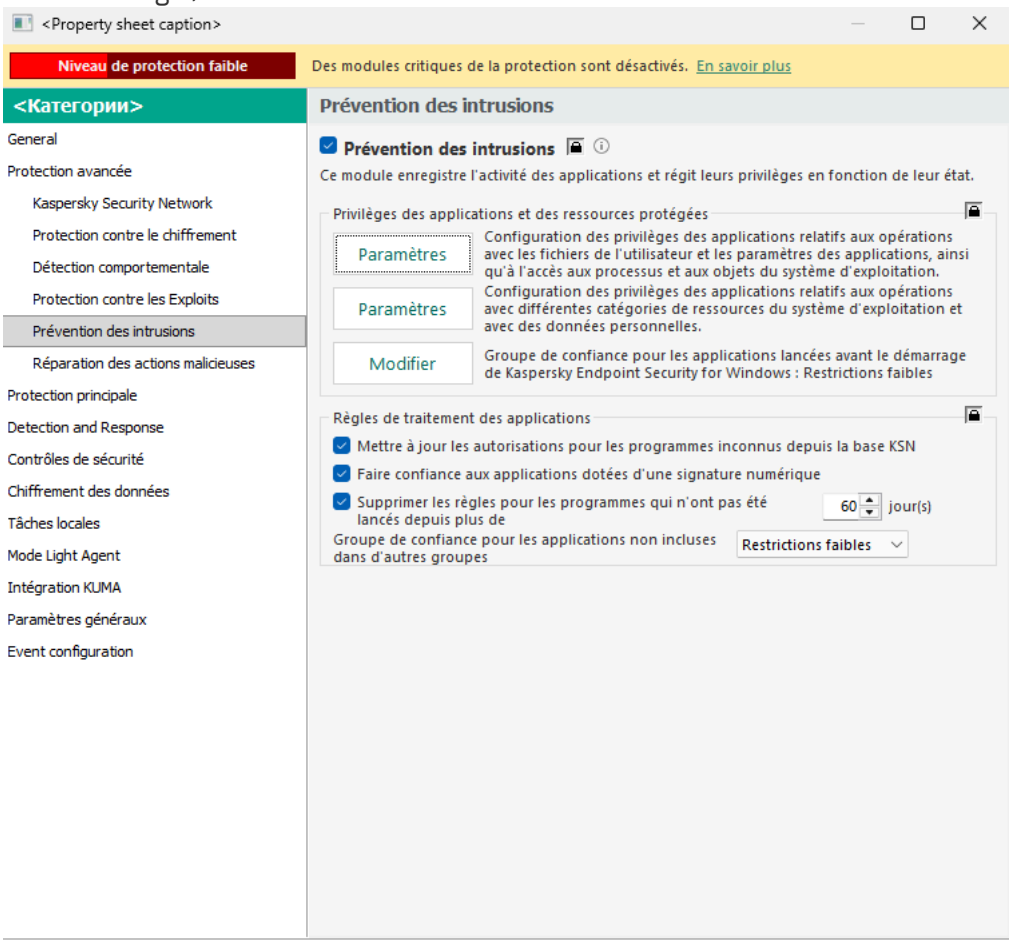
Lorsque vous lancez une application dont les informations ont été supprimées, Kaspersky Endpoint Security examine l'application comme au premier lancement.

Configuration de la suppression automatique des informations relatives aux applications non utilisées dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Prévention des intrusions**.



Paramètres de la prévention des intrusions

4. 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 règles pour les programmes qui n'ont pas été lancés depuis plus de X jour(s)** et indiquez le nombre de jours.

     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 de données, décochez la case **Supprimer les règles pour les programmes qui n'ont pas été lancés depuis plus de X jour(s)**.

  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.

5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration de la suppression automatique des informations relatives aux applications non utilisées dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **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 règles pour les programmes qui n'ont pas été lancés depuis plus de (jours, de 1 à 90)** et indiquez le nombre de jours.

     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 de données, décochez la case **Supprimer les règles pour les programmes qui n'ont pas été lancés depuis plus de (jours, de 1 à 90)**.

     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. Dans la fenêtre principale de l'application, cliquez sur le bouton .

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 règles pour les programmes qui n'ont pas été lancés depuis plus de X jours (de 1 à 90)** et indiquez le nombre de jours.

  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 de données, décochez la case **Supprimer les règles pour les programmes qui n'ont pas été lancés depuis plus de X jours (de 1 à 90)**.

  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 fonctionnalités de protection du signal audio et d'accès à la webcam ne sont pas prises en charge sur les ordinateurs équipés d'un processeur ARM.

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 autorise la réception des flux audio et vidéo uniquement pour les applications en provenance du groupe *De confiance*. Les applications des groupes *Restrictions faibles*, *Restrictions élevées* et *Douteuses* ne sont pas autorisées 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 *Douteuses* 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'images (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.

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 un ordinateur et que le système d'exploitation le reconnait 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 correctement saisi, l'application enregistre les paramètres d'identification, à savoir le VID/PID du clavier et le numéro du port auquel il est connecté, 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. Vous pouvez configurer le nombre de tentatives de saisie du code numérique. En cas de plusieurs saisies erronées du code numérique ou si la fenêtre d'autorisation de clavier (cf. Illustration ci-dessous) est fermée, l'application bloque la saisie depuis ce clavier. Si la durée de blocage de l'appareil USB arrive à échéance 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.

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.

Comment activer ou désactiver le module Protection BadUSB dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection BadUSB**.
4. Utilisez la case **Protection BadUSB** pour activer ou désactiver le module.
5. Dans le groupe **Autorisation de l'appareil USB lors de la connexion**, réglez les paramètres de sécurité pour saisir le code d'autorisation :
   - **Nombre maximal de tentatives d'autorisation des appareils USB**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.
   - **Délai d'attente lorsque le nombre maximal de tentatives est atteint (min.)**. La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le module Protection BadUSB dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection BadUSB**.
5. Utilisez le commutateur **Protection BadUSB ACTIVÉE** pour activer ou désactiver le module.
6. Dans le groupe **Autorisation des appareils USB**, réglez les paramètres de sécurité pour saisir le code d'autorisation :

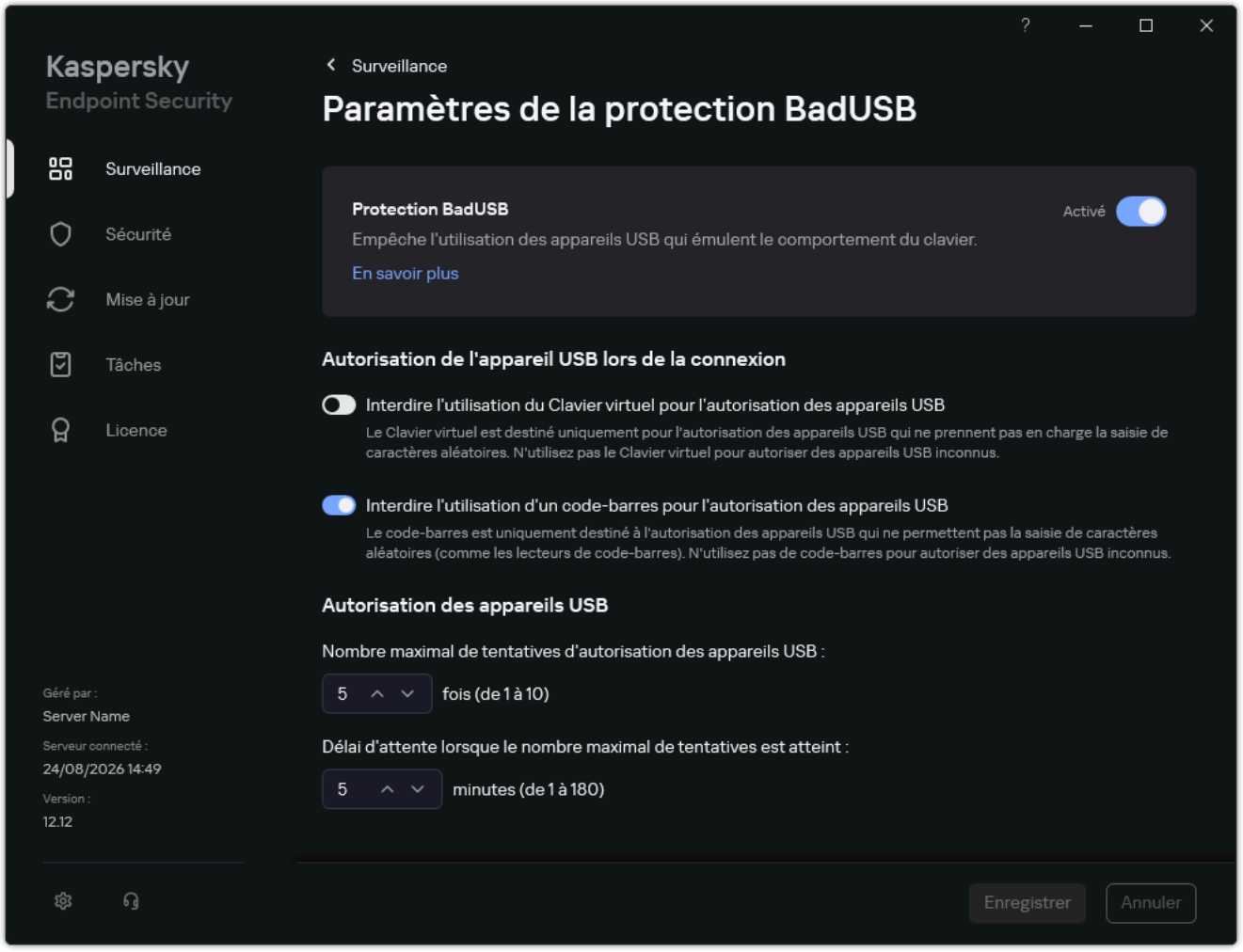
   - **Nombre maximal de tentatives d'autorisation des appareils USB**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.

   - **Délai d'attente lorsque le nombre maximal de tentatives est atteint (minutes)**. La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).
7. Enregistrez vos modifications.

Comment activer ou désactiver le module Protection BadUSB 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 **Protection principale** → **Protection BadUSB**.



Paramètres du module Protection BadUSB

3. Utilisez le commutateur **Protection BadUSB** pour activer ou désactiver le module.

4. Dans le groupe **Autorisation de l'appareil USB lors de la connexion**, réglez les paramètres de sécurité pour saisir le code d'autorisation :

   - **Nombre maximal de tentatives d'autorisation des appareils USB**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.

   - **Délai d'attente lorsque le nombre maximal de tentatives est atteint**. La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).

5. 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.

Comment autoriser ou interdire l'utilisation du clavier virtuel pour l'autorisation dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection BadUSB**.
4. 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.
5. Enregistrez vos modifications.

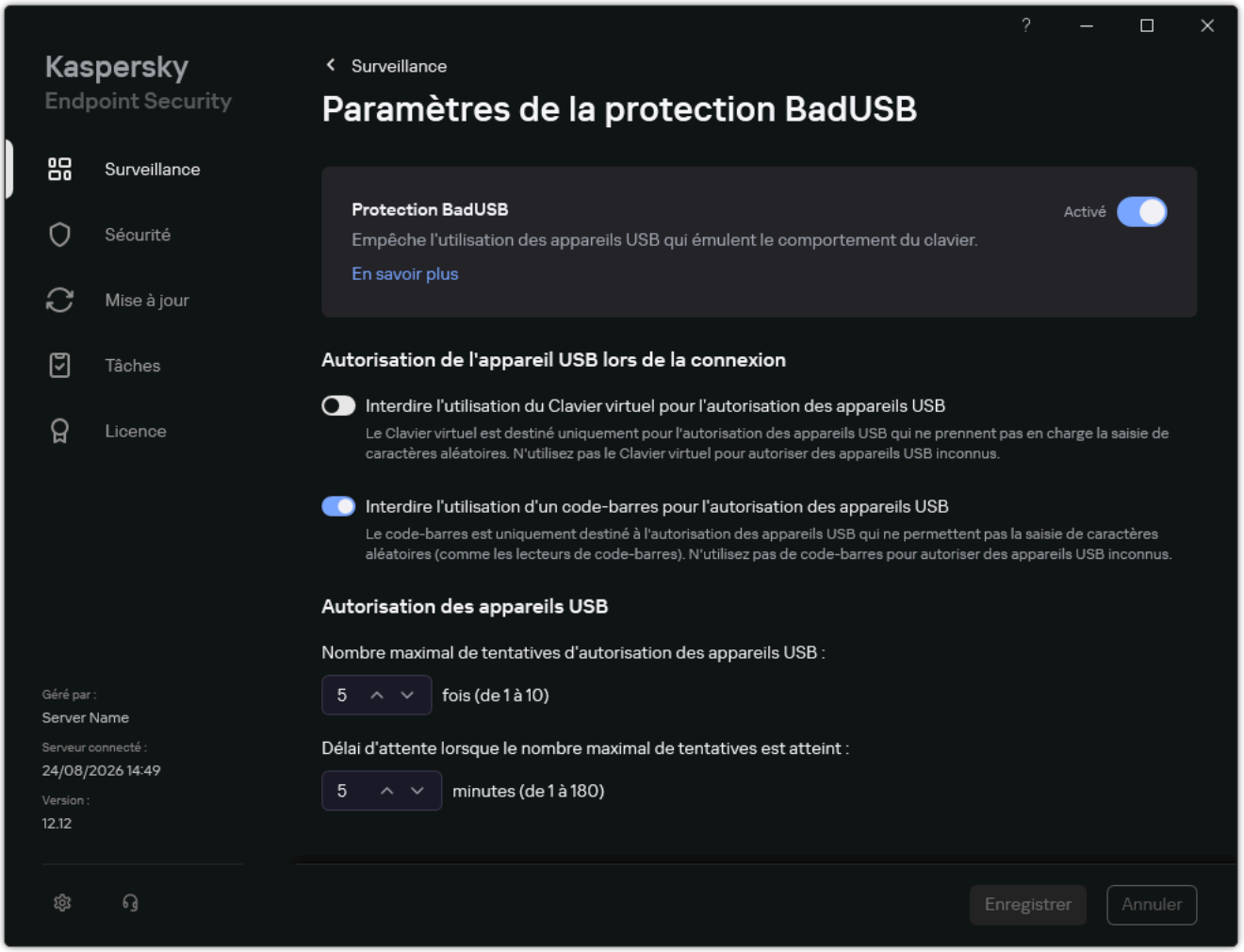
Comment autoriser ou interdire l'utilisation du clavier virtuel pour l'autorisation dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection BadUSB**.
5. Utilisez le commutateur **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.
6. Enregistrez vos modifications.

Autoriser ou interdire l'utilisation du clavier virtuel pour l'autorisation dans l'interface de l'application

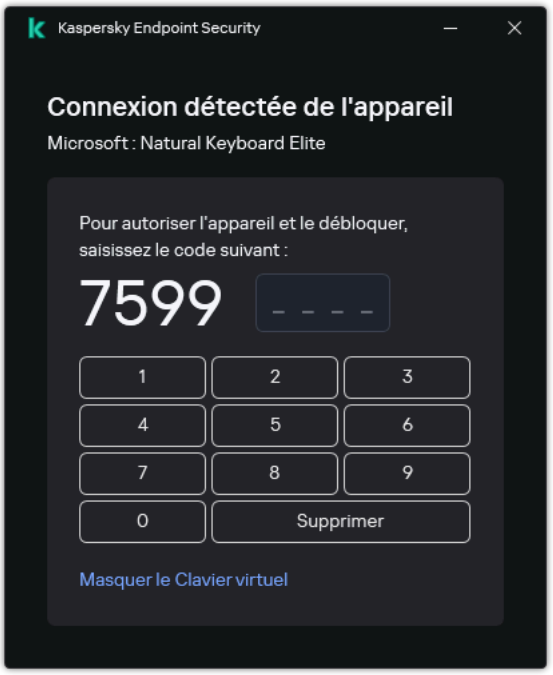
1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection BadUSB**.



Paramètres du module Protection BadUSB

3. Utilisez le commutateur **Interdire l'utilisation du Clavier virtuel pour l'autorisation des appareils USB** pour interdire ou autoriser l'utilisation du clavier virtuel pour l'autorisation.

4. Enregistrez vos modifications.



Autorisation des appareils USB

Autorisation d'utilisation du lecteur de code-barres

Lors de la connexion d'un lecteur de code-barres à l'ordinateur, le module Protection BadUSB identifie cet appareil comme un appareil d'entrée et vous invite à procéder à une autorisation. Pour autoriser le lecteur de code-barres, il faut scanner un code-barres affiché à l'écran. L'application génère un code-barres au format Code39 pris en charge par la plupart des lecteurs de code-barres et de codes QR.

Kaspersky Endpoint Security prend également en charge un autre mode d'autorisation pour le lecteur de code-barres. Si vous utilisez des appareils à écran tactile, vous pouvez utiliser le clavier virtuel pour saisir un code. Pour ce faire, vous devez autoriser le clavier virtuel. Cette méthode est pratique, par exemple, dans le cas de lecteurs de code-barres fixes intégrés dans les caisses enregistreuses. Les autres modes d'autorisation de lecteurs de code-barres sont interdits.

Par défaut, l'application n'utilise pas de code-barres pour l'autorisation des appareils USB.

Comment activer l'autorisation des appareils USB par code-barres dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection BadUSB**.

5. Utilisez la case **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB** pour interdire ou autoriser l'utilisation de code-barres pour l'autorisation.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'autorisation des appareils USB par code-barres dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection BadUSB**.

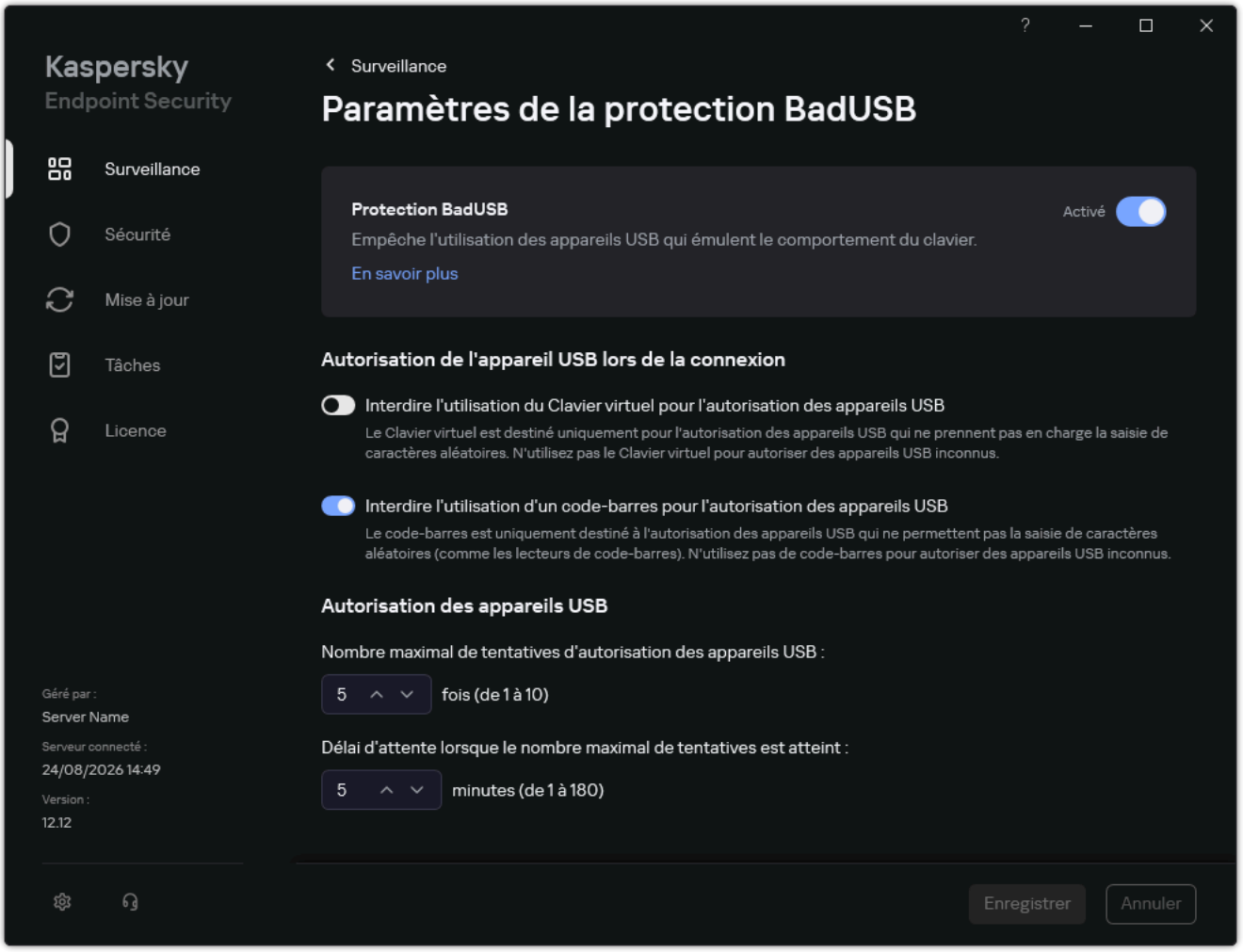
5. Utilisez le commutateur **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB** pour interdire ou autoriser l'utilisation de code-barres pour l'autorisation.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'autorisation des appareils USB par code-barres dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .

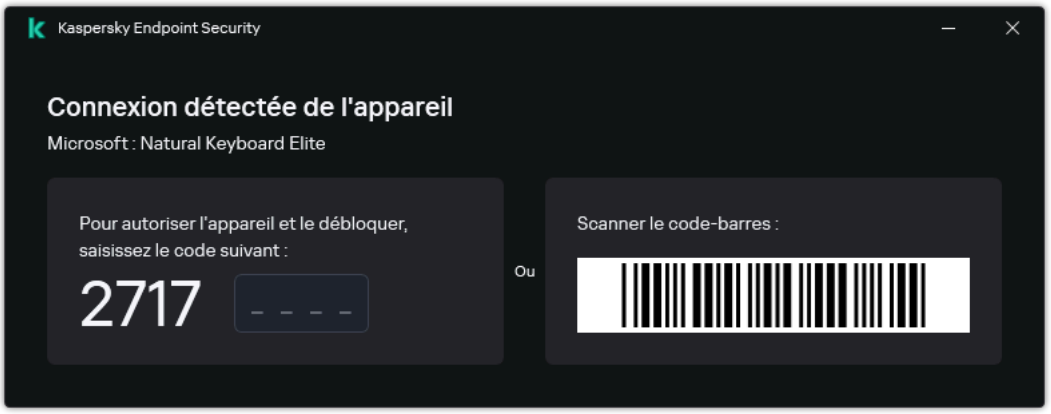
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection BadUSB**.



Paramètres du module Protection BadUSB

3. Utilisez le commutateur **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB** pour interdire ou autoriser l'utilisation de code-barres pour l'autorisation.

4. Enregistrez vos modifications.

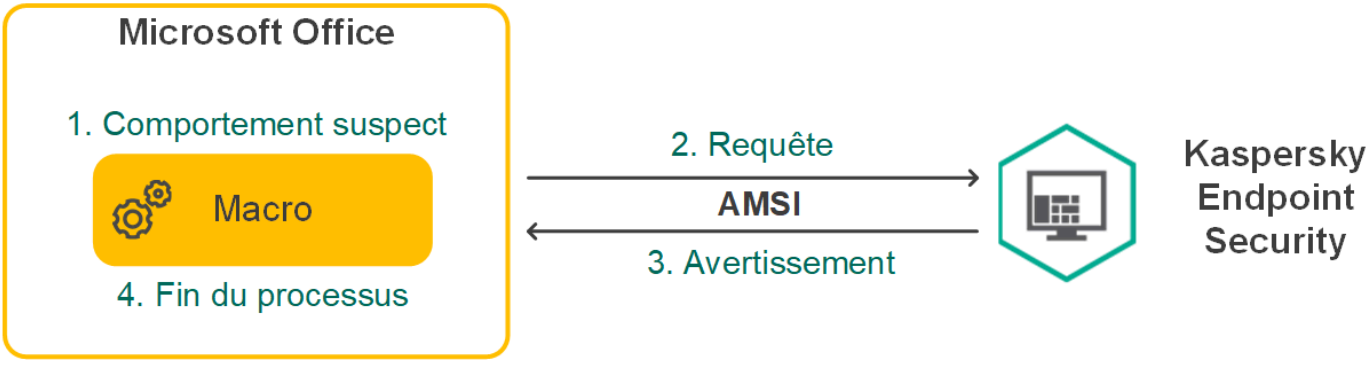


Autorisation d'utilisation du lecteur de code-barres

Protection AMSI

Le module Protection AMSI est destiné à prendre en charge 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, veuillez consulter 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, une application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt l'action).



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 protection AMSI ne refuse pas les demandes provenant d'applications tierces pour lesquelles l'intégration continue avec le module de protection AMSI est activée.

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/Enterprise multi-session
- Windows 11 Home/Pro/Pro for Workstations/Education/Enterprise/Enterprise multi-session
- Windows Server 2016 Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2019 Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (y compris le mode Server Core) ;
- Serveur Windows 2025 Standard/Datacenter.

Activation et désactivation de la protection AMSI

Par défaut, la Protection AMSI est activée et fonctionne dans le mode recommandé par Kaspersky (cf. tableau ci-après).

Comment activer ou désactiver la Protection AMSI dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Scanner AMSI**.
4. Utilisez la case **Scanner AMSI** pour activer ou désactiver le module.
5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

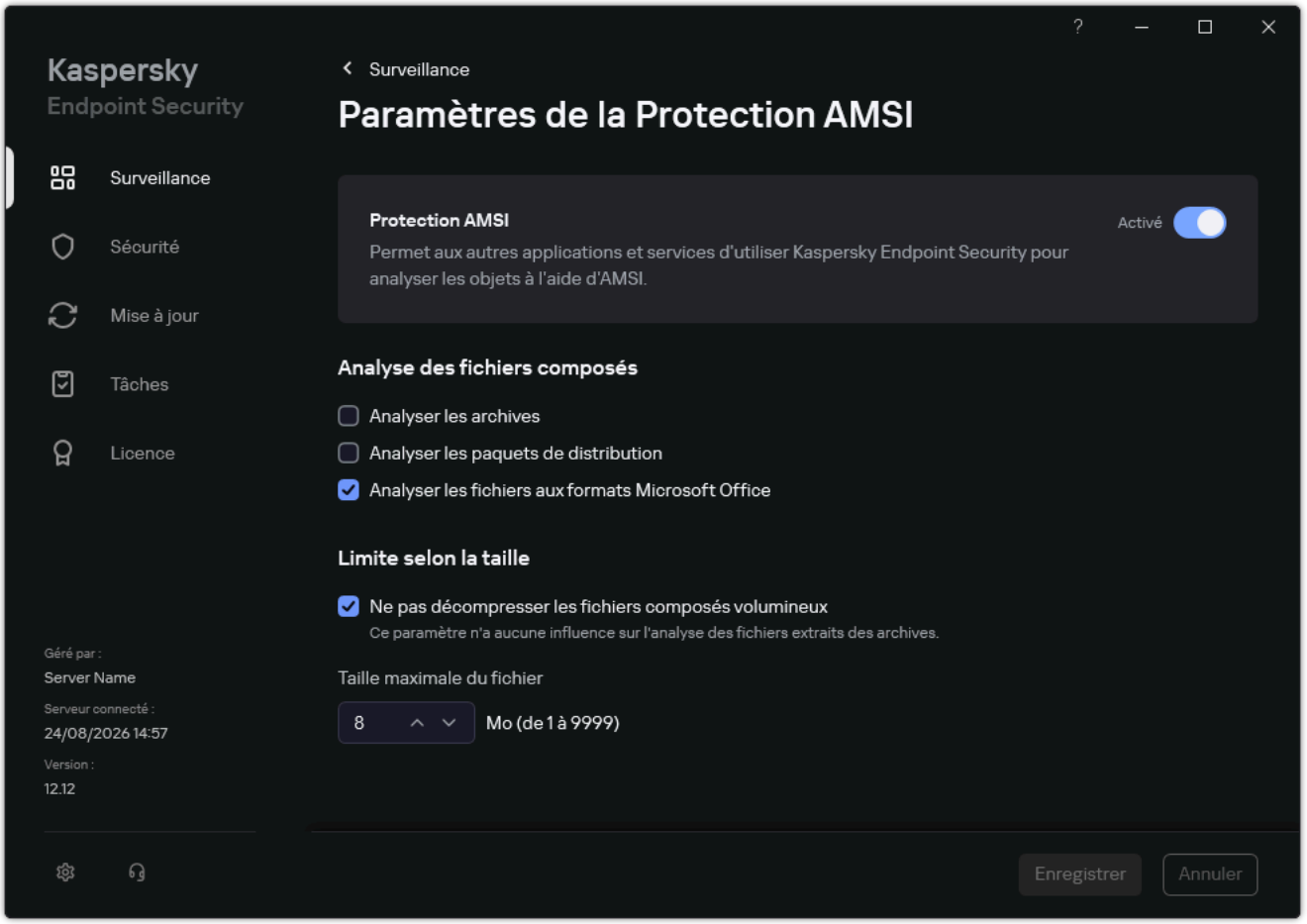
Comment activer ou désactiver la Protection AMSI dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection AMSI**.
5. Utilisez le commutateur **Protection AMSI ACTIVÉE** pour activer ou désactiver le module.
6. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer ou désactiver la Protection AMSI 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 **Protection principale** → **Protection AMSI**.



Paramètres de protection AMSI

3. Utilisez le commutateur **Protection AMSI** pour activer ou désactiver le module.

4. Enregistrez vos modifications.

Paramètres de la protection AMSI recommandés par les experts de Kaspersky

Paramètre	Valeur	Description
Analyser les archives	**Désactivé**	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les paquets de distribution	**Désactivé**	Analyse des paquets de distribution des applications tierces.
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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Ne pas décompresser les fichiers composés volumineux	**Taille maximale du fichier 8 Mo**	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.

Optimisation de l'analyse des fichiers par la Protection AMSI

Vous pouvez optimiser l'analyse des fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Vous pouvez sélectionner les fichiers composés qui doivent être analysés : archives, paquets de distribution ou fichiers au format Office. Vous pouvez également limiter la taille des fichiers composés à analyser. Le module de la protection AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.

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 les types de fichiers composés à analyser pour accélérer l'analyse.

Comment activer l'analyse des connexions chiffrées dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Scanner AMSI**.
4. 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.
5. 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 volumineux** et indiquez la valeur requise. 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 volumineux**.

   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 volumineux** soit cochée ou non.

6. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas 🔒.

Comment activer l'analyse des connexions chiffrées dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Protection AMSI**.

5. 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.

6. Dans le groupe **Optimisation de l'analyse**, 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 **Limites de taille autorisées** et indiquez la valeur requise. 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 **Limites de taille autorisées**.

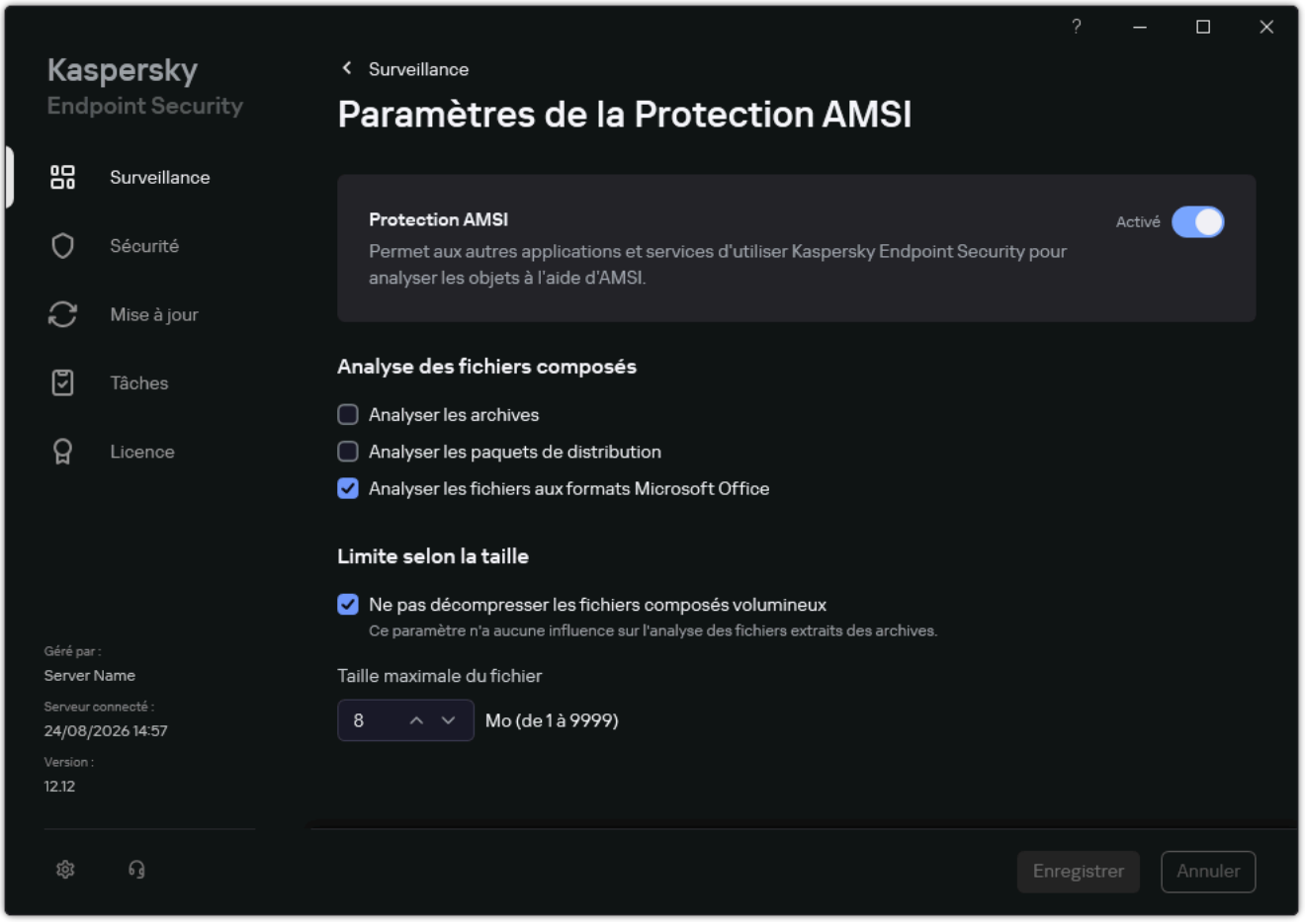
   Le module de la protection AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Limites de taille autorisées** soit cochée ou non.

7. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas 🔒.

Comment activer l'analyse des connexions chiffrées 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 **Protection principale** → **Protection AMSI**.



Paramètres de 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 volumineux** et indiquez la valeur requise. 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 volumineux**.

   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 volumineux** soit cochée ou non.

5. Enregistrez vos modifications.

Protection contre les menaces Internet

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants depuis Internet et 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.

Pour utiliser la Protection contre les menaces Internet, vous devez procéder à la configuration initiale de l'application :

- Pour contrôler le trafic HTTPS, activez l'analyse des connexions sécurisées (activé par défaut).

- Sélectionnez les ports que Kaspersky Endpoint Security doit surveiller (par défaut, l'application surveille tous les ports).

- Sélectionnez les applications dont vous souhaitez que Kaspersky Endpoint Security contrôle le trafic. La plupart des navigateurs sont déjà présents dans la liste des applications recommandées par Kaspersky. Si votre navigateur ne figure pas dans la liste, ajoutez-le manuellement.

- Nous vous recommandons d'injecter un script d'interaction avec les pages Internet dans le trafic Internet (par défaut, l'injection de script est désactivée). Ce script permet d'enregistrer les événements de la Protection contre les menaces Internet pour le journal des événements de l'application, le journal des événements du système d'exploitation et les rapports.

Lorsqu'un utilisateur tente d'ouvrir un site Internet malveillant ou de phishing, Kaspersky Endpoint Security bloque l'accès et affiche un avertissement.

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. L'application peut appliquer différents groupes de paramètres pour le module Protection contre les menaces Internet. Ces groupes de paramètres stockés dans l'application sont appelés *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres **Recommandé** 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.

Vous pouvez sélectionner ou configurer le niveau de sécurité uniquement dans la Console d'administration (MMC) ou dans l'interface locale de l'application. Vous ne pouvez pas sélectionner ni configurer le niveau de sécurité dans Web Console ni dans Cloud Console.

Procédure d'activation ou de désactivation du module Protection contre les menaces Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.
4. Utilisez la case **Protection contre les menaces Internet** pour activer ou désactiver le module.
5. Si vous avez activé le module, réalisez l'une des opérations suivantes dans le groupe **Niveau de sécurité** :
   - 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 un 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 l'application 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** et définissez vos propres paramètres du module (voir le tableau ci-dessous).

     Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Par défaut**.

6. 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 :

   - **Bloquer**. 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.

   - **Informer**. 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.

7. Enregistrez vos modifications.

Comment activer ou désactiver le module Protection contre les menaces Internet dans la Web Console

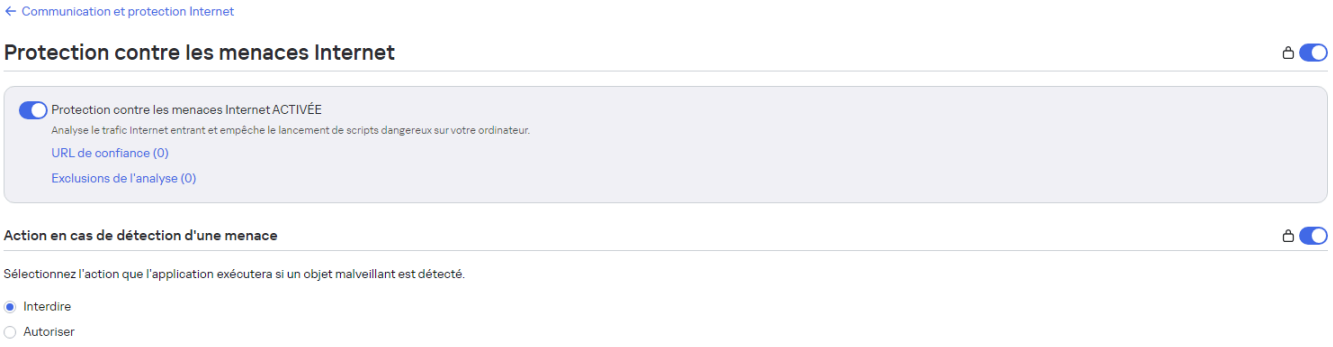
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces Internet**.



Paramètres du module Protection contre les menaces Internet

5. Utilisez le commutateur **Protection contre les menaces Internet ACTIVÉE** pour activer ou désactiver le module.

6. 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**. 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.

   - **Autoriser, informer ou demander une action (selon le système d'exploitation)**. 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.

7. Si nécessaire, dressez une liste d'adresses Internet de confiance.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Procédure d'activation ou de désactivation du module Protection contre les menaces Internet

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 le groupe **Niveau de sécurité** :

   - 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 un 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 l'application 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 (voir le tableau ci-dessous).

     Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut**.

5. 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 :

   - **Bloquer**. 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.

   - **Informer**. 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.

6. 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 l'adresse Internet par rapport à la base de données des adresses Internet malveillantes	**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.
Vérifier l'adresse Internet par rapport à la base de données des adresses Internet 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)	**Moyenne**	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 cas de détection d'une menace	**Bloquer**	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.

Configuration des méthodes de détection des adresses Internet malveillantes

La Protection contre les menaces Internet détecte les adresses Internet malveillantes à l'aide de bases de données antivirus, du service dans le Cloud Kaspersky Security Network ainsi que de l'analyse heuristique.

Vous pouvez sélectionner les méthodes de détection des adresses Internet malveillantes uniquement dans la Console d'administration (MMC) ou dans l'interface locale de l'application. Vous ne pouvez pas sélectionner les méthodes de détection des adresses Internet malveillantes dans Web Console ni Cloud Console. L'option par défaut consiste à vérifier les adresses Internet par rapport à la base de données des adresses malveillantes à l'aide de l'analyse heuristique (analyse standard).

Analyse à l'aide de la base de données des adresses 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 Security 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 l'analyse des connexions chiffrées est désactivée, 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.

Comment activer ou désactiver la vérification des adresses Internet par rapport à la base de données des adresses Internet malveillantes à l'aide de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Méthodes d'analyse**, cochez ou décochez la case **Vérifier l'adresse Internet par rapport à la base de données des adresses Internet malveillantes** pour activer ou désactiver la vérification des adresses par rapport à la base de données des adresses Internet malveillantes.
6. Enregistrez vos modifications.

Comment activer ou désactiver la vérification des adresses par rapport à la base de données des adresses malveillantes 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 **Protection principale** → **Protection contre les menaces Internet**.
3. Cliquez sur **Paramètres avancés**.
4. Dans le groupe **Méthodes d'analyse**, cochez ou décochez la case **Vérifier l'adresse Internet par rapport à la base de données des adresses Internet malveillantes** pour activer ou désactiver la vérification des adresses par rapport à la base de données des adresses Internet malveillantes.
5. Enregistrez vos modifications.

Analyse heuristique

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.

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.

Comment activer ou désactiver l'utilisation de l'analyse heuristique dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.
5. Dans la fenêtre qui s'ouvre, 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.
6. Définissez le niveau de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.

   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.
7. Enregistrez vos modifications.

Comment activer ou désactiver l'utilisation de l'analyse heuristique 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 **Protection principale** → **Protection contre les menaces Internet**.

3. Cliquez sur **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.

   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.

5. Enregistrez vos modifications.

Anti-phishing

La Protection contre les menaces Internet vérifie les liens pour vérifier s'ils appartiennent à des adresses Internet de phishing. Cette mesure 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 d'autres sources, comme des messageries, 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.

Vous pouvez configurer l'Anti-phishing uniquement dans la Console d'administration (MMC) ou dans l'interface locale de l'application. Vous ne pouvez pas configurer l'Anti-phishing dans Web Console ni Cloud Console. Par défaut, l'Anti-Phishing avec analyse heuristique est activé.

Comment activer ou désactiver l'Anti-phishing dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.

5. Dans la fenêtre qui s'ouvre, dans le groupe **Paramètres de l'Anti-Phishing**, cochez ou décochez la case **Vérifier l'adresse Internet par rapport à la base de données des adresses Internet de phishing** pour activer ou désactiver l'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.

6. 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.

   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 analyser les liens, outre la base de données antivirus et l'analyse heuristique, vous pouvez utiliser les bases de données de réputation de Kaspersky Security Network.

7. Enregistrez vos modifications.

Comment activer ou désactiver l'Anti-phishing 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 **Protection principale** → **Protection contre les menaces Internet**.

3. Cliquez sur **Paramètres avancés**.

4. 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 **Vérifier l'adresse Internet par rapport à la base de données des adresses Internet 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.

5. 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.

   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 analyser les liens, outre la base de données antivirus et l'analyse heuristique, vous pouvez utiliser les bases de données de réputation de Kaspersky Security Network.

6. Enregistrez vos modifications.

Constitution d'une liste des URL de confiance

Outre les sites Internet malveillants et de phishing, la Protection contre les menaces Internet peut bloquer d'autres sites Internet. Par exemple, la Protection contre les menaces Internet bloque le trafic HTTP qui ne répond pas aux normes RFC. 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.

Comment ajouter une URL de confiance à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.
6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **URL de confiance**.
7. Cochez la case **Ne pas analyser le trafic Internet en provenance des adresses URL de confiance**.

   Si cette option est sélectionnée, 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.
8. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable.

   Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

   Vous pouvez également importer une liste d'URL de confiance à partir d'un fichier XML.
9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter une URL de confiance dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Adresses Internet**.

   Une fenêtre contenant une liste d'URL de confiance s'ouvre.

6. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable.

   Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

   Vous pouvez également importer une liste d'URL de confiance à partir d'un fichier XML.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter une URL de confiance 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 **Protection principale** → **Protection contre les menaces Internet**.

3. Cliquez sur **Paramètres avancés**.

4. Cochez la case **Ne pas analyser le trafic Internet à partir des adresses Internet de confiance**.

   Si cette option est sélectionnée, 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.

   Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

   Vous pouvez également importer une liste d'URL de confiance à partir d'un fichier XML.

6. Enregistrez vos modifications.

Par conséquent, la Protection contre les menaces Internet n'analyse pas le trafic des URL de confiance. L'utilisateur peut toujours ouvrir un site Internet de confiance et télécharger un fichier à partir de ce site. Si vous ne parvenez pas à accéder au site Internet, vérifiez les paramètres des modules Analyse des connexions chiffrées, Contrôle Internet et Contrôle des ports réseau. Si Kaspersky Endpoint Security détecte un fichier téléchargé à partir d'un site Internet de confiance comme étant malveillant, vous pouvez ajouter ce fichier aux exclusions.

Vous pouvez également créer une liste générale d'exclusions pour les connexions chiffrées. Dans ce cas, Kaspersky Endpoint Security n'analyse pas le trafic HTTPS des URL de confiance lorsque les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet fonctionnent.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces Internet**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **URL de confiance**.
6. 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste complète des adresses Internet de confiance dans un fichier XML.
7. 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. Ouvrez le fichier.

      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.
8. Enregistrez vos modifications.

Comment exporter et importer une liste d'adresses Internet de confiance dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces Internet**.

5. Pour exporter la liste des exclusions dans le groupe **Liste des règles**, procédez comme suit :

   a. Sélectionnez les adresses Internet de confiance que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des URL de confiance dans un fichier JSON dans le dossier des téléchargements par défaut.

6. Pour importer la liste d'exclusions dans le groupe **Liste des règles**, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des adresses de confiance.

   b. Ouvrez le fichier.

      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 JSON.

7. Enregistrez vos modifications.

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 protège l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et d'une analyse heuristique.

La Protection contre les menaces par emails peut analyser les messages entrants et sortants. L'application prend en charge les protocoles POP3, SMTP, IMAP et NNTP dans les clients de messagerie suivants :

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pour analyser le trafic dans les clients de messagerie Mozilla Thunderbird, MyOffice Mail et R7-Office Organizer, vous devez ajouter le certificat Kaspersky à la liste de certificats et sélectionner la propre liste de certificats.

La Protection contre les menaces par emails ne prend pas en charge d'autres protocoles et clients de messagerie.

La Protection contre les menaces par emails peut ne pas toujours être en mesure d'accéder aux messages *au niveau du protocole* (par exemple, lors de l'utilisation de la solution Microsoft Exchange). Pour cette raison, la Protection contre les menaces par emails inclut une extension pour Microsoft Office Outlook. L'extension permet d'analyser les messages *au niveau du client de messagerie*. L'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2010, 2013, 2016, 2019, 2021, 2024 et 365. Sur les ordinateurs équipés d'un processeur ARM, l'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2016, Outlook 2021, Outlook 2024 et Outlook 365 pour ARM64.

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 ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

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. L'application 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 *niveaux de sécurité* : **Élevé**, **Recommandé**, **Faible**. Les paramètres **Recommandé** 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.

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.

Procédure d'activation ou de désactivation du module Protection contre les menaces par emails dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.
4. Utilisez la case **Protection contre les menaces par emails** pour activer ou désactiver le module.

5. Si vous avez activé le module, réalisez l'une des opérations suivantes dans le groupe **Niveau de sécurité** :

   - 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. Le niveau de sécurité Élevé pour la protection de la messagerie 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 l'application et la sécurité de la messagerie. 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 de la messagerie est recommandé pour un travail en environnement bien protégé. 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** et définissez vos propres paramètres du module (voir le tableau ci-dessous).

     Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Par défaut**.

6. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

   - **Désinfecter ; supprimer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant ou sortant, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant, l'application 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, l'application ajoute un avertissement à l'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, l'application tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

   - **Bloquer**. Si un objet infecté est détecté dans un message entrant, l'application ajoute un avertissement à l'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, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le module Protection contre les menaces par emails dans la Web Console

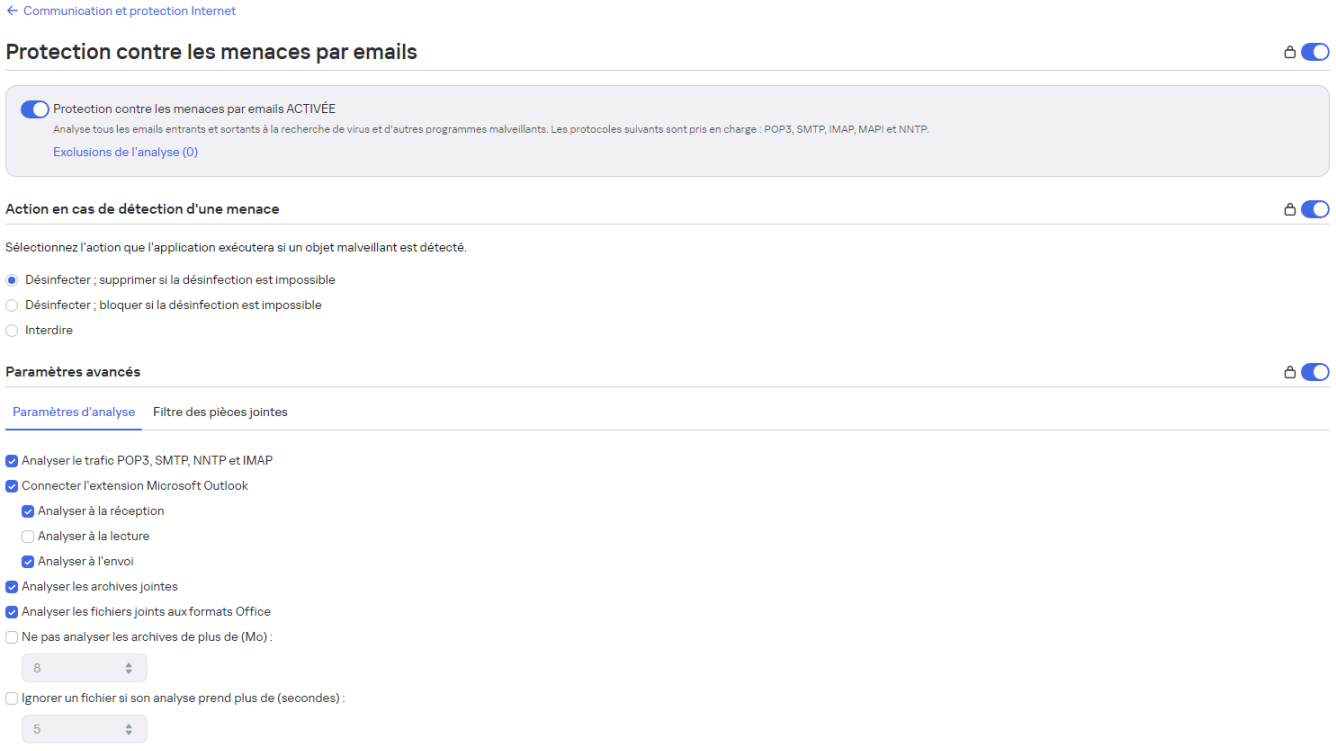
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces par emails**.



Paramètres du module Protection contre les menaces par emails

5. Utilisez le commutateur **Protection contre les menaces par emails ACTIVÉE** pour activer ou désactiver le module.

6. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

   - **Désinfecter ; supprimer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant ou sortant, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant, l'application 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, l'application ajoute un avertissement à l'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, l'application tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

   - **Interdire**. Si un objet infecté est détecté dans un message entrant, l'application ajoute un avertissement à l'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, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

7. Si nécessaire, modifiez les paramètres avancés de la Protection contre les menaces par emails.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le module Protection contre les menaces par emails 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 **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 le groupe **Niveau de sécurité** :

- 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. Le niveau de sécurité Élevé pour la protection de la messagerie 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 l'application et la sécurité de la messagerie. 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 de la messagerie est recommandé pour un travail en environnement bien protégé. 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 (voir le tableau ci-dessous).

  Vous pouvez rétablir les valeurs des niveaux de sécurité prédéfinis en cliquant sur le bouton **Restaurer le niveau de protection par défaut**.

5. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants :

- **Désinfecter ; supprimer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant ou sortant, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

- **Désinfecter ; bloquer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant, l'application 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, l'application ajoute un avertissement à l'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, l'application tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

- **Interdire**. Si un objet infecté est détecté dans un message entrant, l'application ajoute un avertissement à l'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, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

6. 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	**Messages entrants et sortants**	La *Zone d'analyse* 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 des emails à l'aide d'une extension pour Microsoft Outlook, il est recommandé d'utiliser 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 des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les fichiers joints 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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Filtre des pièces jointes	**Renommer les pièces jointes de types 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	**Moyenne**	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.
Action en cas de détection d'une menace	**Désinfecter ; supprimer si la désinfection est impossible**	Si un objet infecté est détecté dans un message entrant ou sortant, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **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, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

   - **Désinfecter ; bloquer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant, l'application 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, l'application ajoute un avertissement à l'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, l'application tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.

   - **Interdire**. Si un objet infecté est détecté dans un message entrant, l'application ajoute un avertissement à l'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, l'application 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Zone de protection**, sélectionnez les messages à analyser :

   - **Messages entrants et sortants**.

   - **Analyser uniquement les emails 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 dans le système d'exploitation**, procédez comme suit :

- Cochez la case **Analyser le trafic POP3, SMTP, NNTP et 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 et 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 client de messagerie autre que Microsoft Office Outlook, le module Protection contre les menaces par emails n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP ni IMAP quand la case **Analyser le trafic POP3, SMTP, NNTP et IMAP** est décochée.

- 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Analyse des fichiers composés**, configurez les paramètres d'analyse :

   - **Analyser les fichiers joints 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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.

   - **Analyser les archives jointes**. Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).

     > Si pendant l'analyse, l'application 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 (de 1 à 9999)**. 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 de vérification des archives à X sec (de 1 à 9999)**. 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 aux emails

> Le filtre des pièces jointes ne s'applique pas aux emails 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.

3. Cliquez sur **Paramètres avancés**.

4. Dans le groupe **Filtre des pièces jointes**, exécutez une des actions suivantes :

   - **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.

   - **Renommer les pièces jointes de types 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.

   - **Supprimer les pièces jointes de types indiqués**. Si cette option est sélectionnée, le module Protection contre les menaces par emails supprime les fichiers joints des types de messages électroniques indiqués.

5. Si à l'étape précédente des instructions vous avez choisi l'option **Renommer les pièces jointes de types indiqués** ou l'option **Supprimer les pièces jointes de types 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. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **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. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste complète des extensions dans un fichier XML.

6. Pour importer la 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. Ouvrez le fichier.

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.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.

5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Filtre des pièces jointes**.

6. 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. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste complète des extensions dans un fichier XML.

7. 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. Ouvrez le fichier.

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.

8. 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. L'extension permet d'analyser les messages au niveau d'un client de messagerie plutôt qu'au niveau du protocole. En plus des messages, l'extension vous permet d'analyser les objets reçus via l'interface MAPI à partir des stockages Microsoft Exchange (par exemple, les objets du calendrier). Cette analyse a lieu dans le client de messagerie.

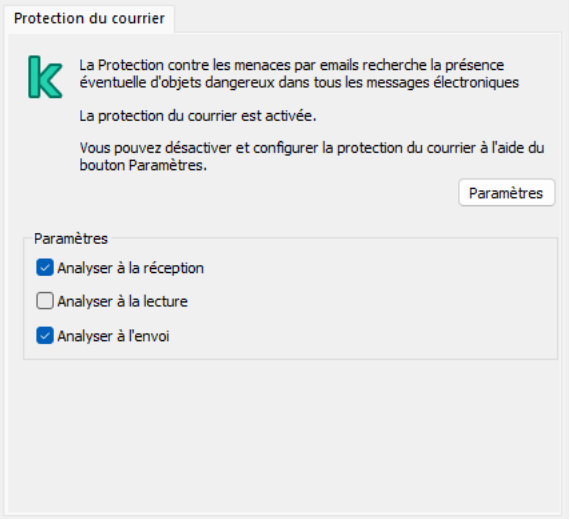
Vous pouvez passer à la configuration des paramètres du module Protection contre les menaces par emails depuis l'application Outlook et indiquer le moment auquel il convient de rechercher parmi les messages électroniques la présence de virus et d'autres applications présentant une menace.

L'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2010, 2013, 2016, 2019, 2021, 2024 et 365.

Sur les ordinateurs équipés d'un processeur ARM, l'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2016, Outlook 2021, Outlook 2024 et Outlook 365 pour ARM64.

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 (voir la figure ci-dessous).



Paramètres du module Protection contre les menaces par emails dans Outlook

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.

Lors de l'analyse des emails avec l'extension Protection contre les menaces par emails pour Outlook, nous vous recommandons 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.

Comment configurer le mode de fonctionnement de l'extension du module Protection contre les menaces par emails pour Outlook dans la Console d'administration (MMC)

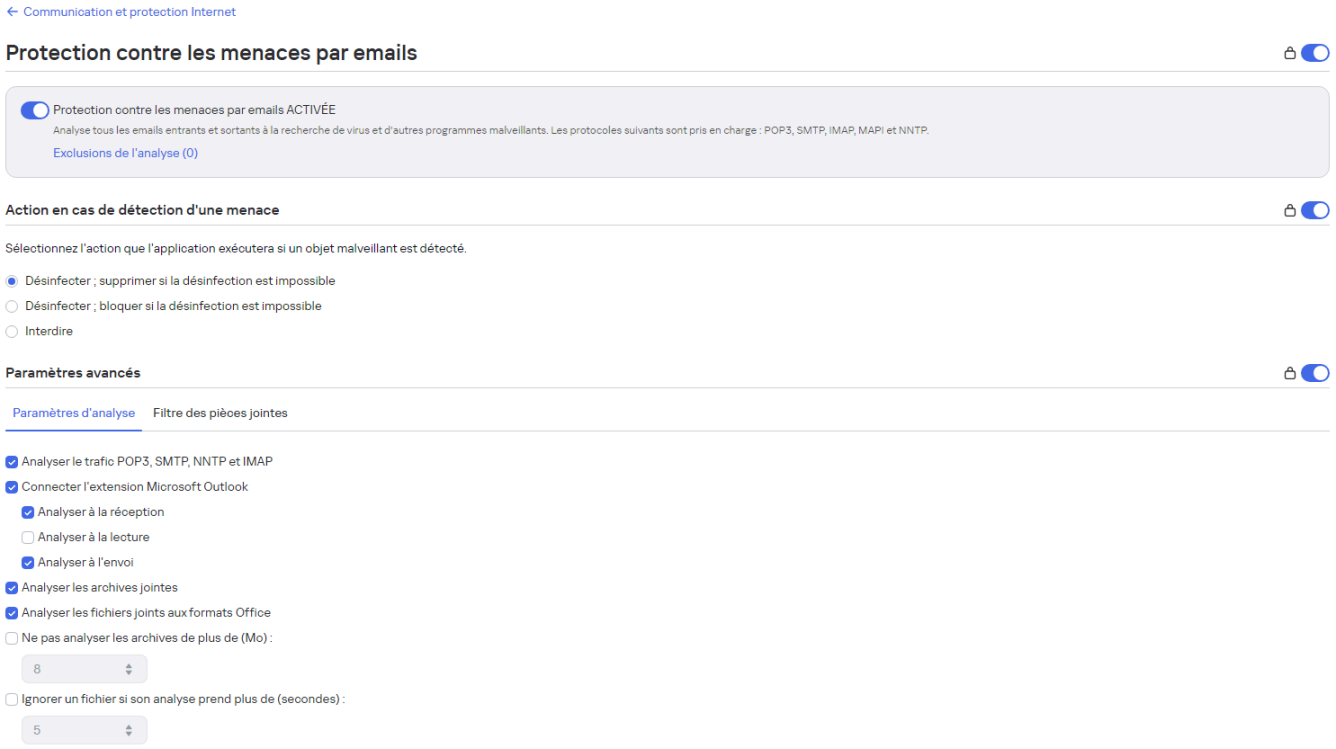
1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces par emails**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Niveau de sécurité**.
6. Dans la fenêtre qui s'ouvre, dans le groupe **Intégration au système**, cochez la case **Connecter l'extension Microsoft Outlook**.
7. Cliquez sur **Paramètres**.
8. Dans la fenêtre **Protection du courrier**, réalisez une des opérations suivantes :
   - 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. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer le mode de fonctionnement de l'extension du module Protection contre les menaces par emails pour Outlook dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces par emails**.



Paramètres du module Protection contre les menaces par emails

5. Sous les **Paramètres avancés**, sélectionnez l'onglet **Paramètres d'analyse**.

6. Cochez la case **Connecter l'extension Microsoft Outlook**.

7. Configurez le mode de l'extension :

- 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.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Analyse des emails dans Thunderbird, MyOffice et R7-Office

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. Pour les clients de messagerie Mozilla Thunderbird, MyOffice Mail et R7-Office Organizer, l'application n'a accès aux messages qu'au *niveau du protocole* (POP3, SMTP, IMAP, NNTP).

Pour analyser le trafic dans les clients de messagerie Mozilla Thunderbird, MyOffice Mail et R7-Office Organizer, vous devez ajouter le certificat Kaspersky à la liste de certificats et sélectionner la propre liste de certificats.

Le module Protection contre les menaces par emails n'analyse pas les messages si le client de messagerie est ouvert dans un navigateur.

Protection en temps réel contre les menaces par emails

La Protection contre les menaces par emails peut analyser les messages entrants et sortants. 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. Lorsqu'un fichier malveillant est détecté dans une pièce jointe, Kaspersky Endpoint Security ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

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.

Recherche de programmes malveillants dans les bases de messagerie

La Protection contre les menaces par emails empêche l'infection de l'ordinateur au niveau du protocole, mais si l'ordinateur a été infecté avant l'installation de Kaspersky Endpoint Security, l'application peut détecter la menace dans les bases de données de messagerie à l'aide de la tâche *Analyse des logiciels malveillants*. L'application ne désinfecte ni ne supprime les fichiers infectés dans les bases de données de messagerie, quels que soient les paramètres de la tâche. Cela est dû au fait que Kaspersky Endpoint Security ne décompose pas les messages de Thunderbird, MyOffice et P7-Office en différents éléments (en-tête, corps, pièces jointes) de la même manière que les messages de Microsoft Office Outlook. L'application ajoute uniquement les informations relatives aux objets détectés à la liste des menaces actives.

Pour éliminer les menaces actives, procédez comme suit :

1. Recherchez et supprimez manuellement le message contenant l'objet détecté dans l'interface du client de messagerie.

   L'application affiche des informations sur l'objet détecté dans la liste des menaces actives.

Exemple de carte d'objet détecté :

!	**HEUR:Trojan.PDF.Phish.gen** Objet : `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox//` `[From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Exécutez l'opération de compression de la base de données.

   Lorsqu'un message est supprimé dans l'interface utilisateur, le client de messagerie ajoute uniquement une marque de suppression. Le client de messagerie ne supprime réellement le message qu'après une compression de la base de données. Pour en savoir plus sur la compression d'une base de données, consultez l'aide de votre client de messagerie (par exemple, Mozilla Thunderbird).

3. Exécutez de nouveau la tâche *Analyse des logiciels malveillants* et assurez-vous que la menace a disparu.

Si la suppression des messages contenant des fichiers infectés n'est pas disponible pour le moment, quelle qu'en soit la raison, vous pouvez traiter ces menaces dans l'interface utilisateur de Kaspersky Endpoint Security. Pour les fichiers des clients de messagerie, deux options permettent de traiter une menace : **Ignorer** et **Ajouter aux exclusions**. Pour empêcher l'application d'ajouter ces objets à la liste des menaces actives lors d'une nouvelle analyse, ajoutez-les à la liste des exclusions de l'analyse.

Protection contre les menaces réseau

Le module *Protection contre les menaces réseau* (également appelé Intrusion Detection System, IDS) surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, l'application 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 l'application. 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. Kaspersky Endpoint Security surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau et bloque les attaques.

Comment activer ou désactiver la Protection contre les menaces réseau dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces réseau**.

4. Utilisez la case **Protection contre les menaces réseau** pour activer ou désactiver le module.

5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le module Protection contre les menaces réseau dans la Web Console

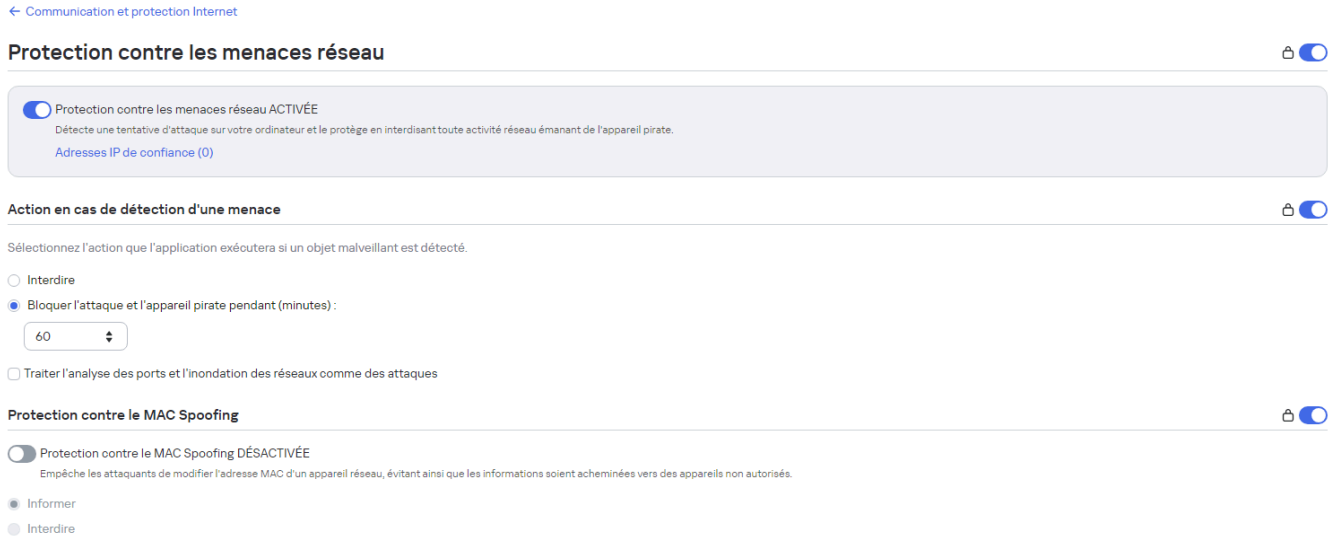
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces réseau**.



Paramètres de la Protection contre les menaces réseau

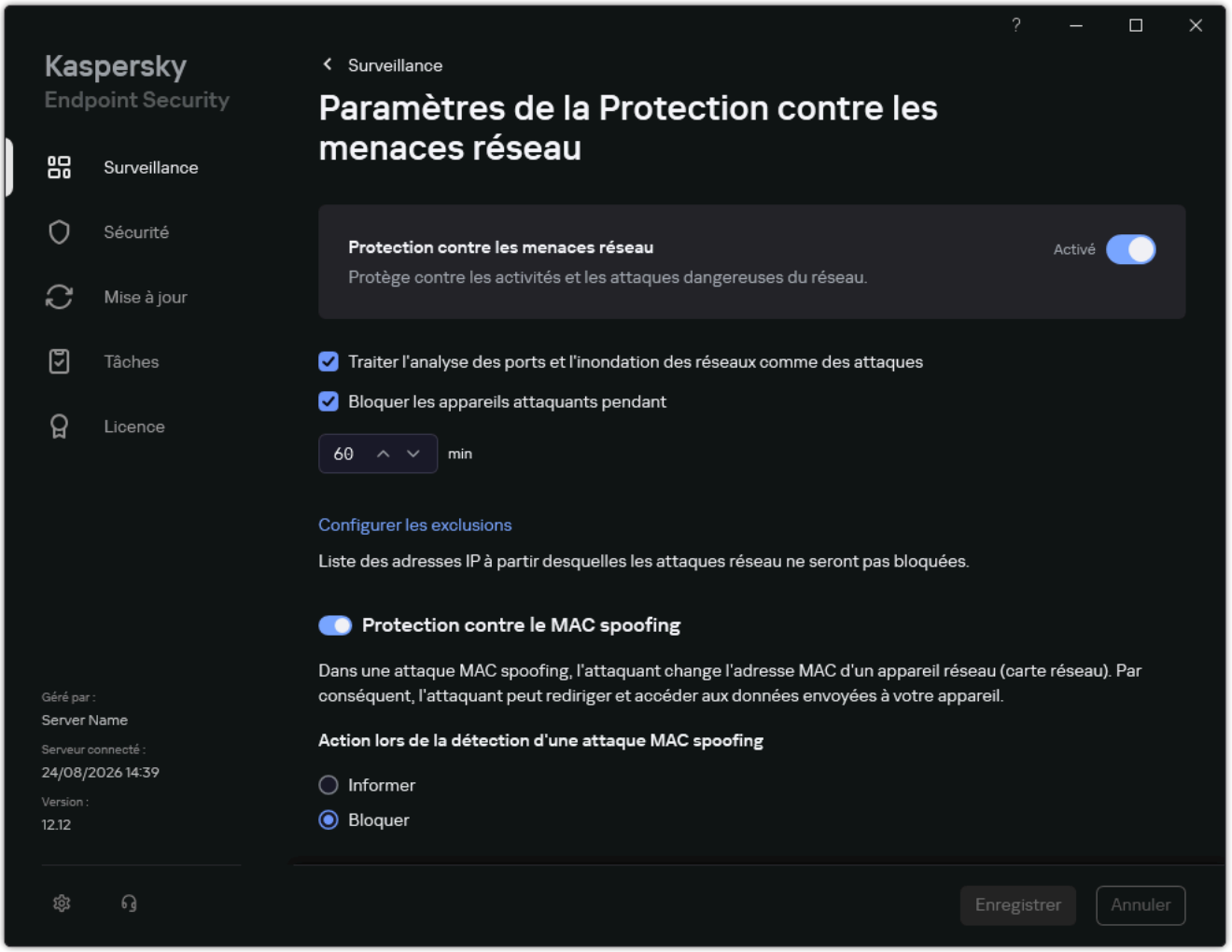
5. Utilisez le commutateur **Protection contre les menaces réseau ACTIVÉE** pour activer ou désactiver le module.

6. Enregistrez vos modifications.

Comment activer ou désactiver la Protection contre les menaces réseau 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 **Protection principale** → **Protection contre les menaces réseau**.



Paramètres de la Protection contre les menaces réseau

3. Utilisez le commutateur **Protection contre les menaces réseau** pour activer ou désactiver le module.

4. Enregistrez vos modifications.

Blocage d'un ordinateur attaquant

Si le module Protection contre les menaces réseau est activé, Kaspersky Endpoint Security bloque automatiquement les menaces réseau. De plus, l'application peut bloquer l'ordinateur attaquant et restreindre l'envoi de paquets réseau pendant un certain temps. Par défaut, Kaspersky Endpoint Security bloque l'ordinateur pendant une heure.

Comment bloquer un ordinateur attaquant dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces réseau**.

4. Sous **Paramètres de la Protection contre les menaces réseau**, cochez la case **Bloquer les appareils attaquants pendant N min**.

   Si cette option est activée, le module Protection contre les menaces réseau 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. Le temps minimum qu'un ordinateur attaquant doit passer dans la liste du groupe est d'une minute. La durée maximale est de 999 minutes.

5. Définissez une durée de blocage différente pour un ordinateur attaquant dans le champ situé à droite de la case **Bloquer les appareils attaquants pendant X min**.

6. Enregistrez vos modifications.

Comment bloquer un ordinateur attaquant dans Web Console

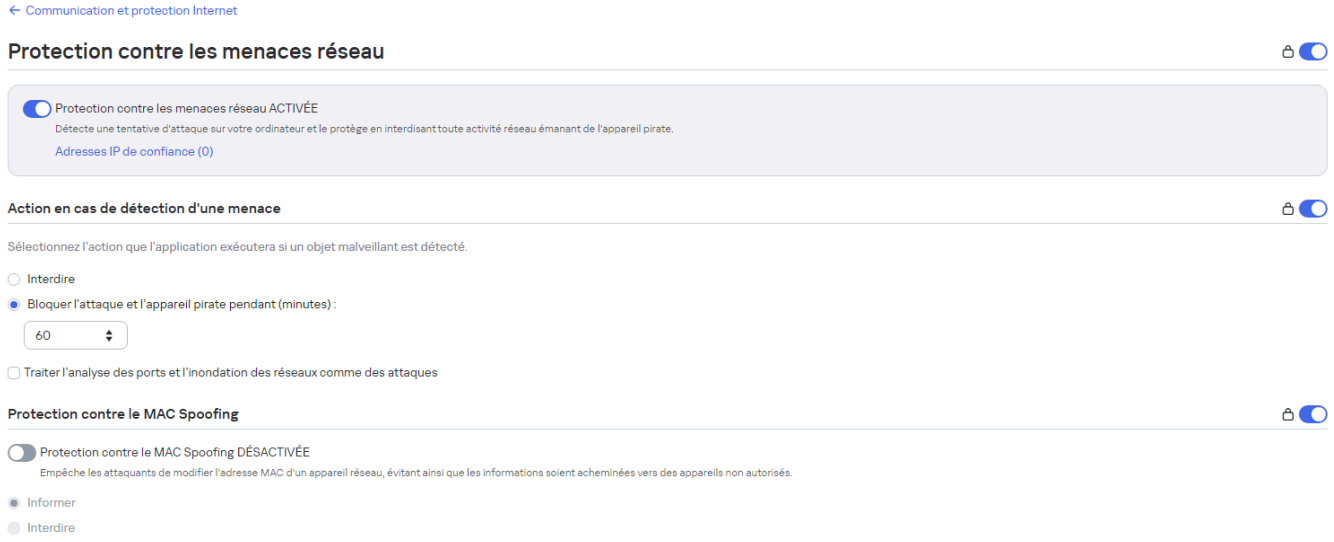
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces réseau**.



Paramètres de la Protection contre les menaces réseau

5. Dans le groupe **Action en cas de détection d'une menace**, cochez la case **Bloquer l'attaque et l'appareil pirate pendant (minutes)**.

   Si cette option est activée, le module Protection contre les menaces réseau 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. Le temps minimum qu'un ordinateur attaquant doit passer dans la liste du groupe est d'une minute. La durée maximale est de 999 minutes.

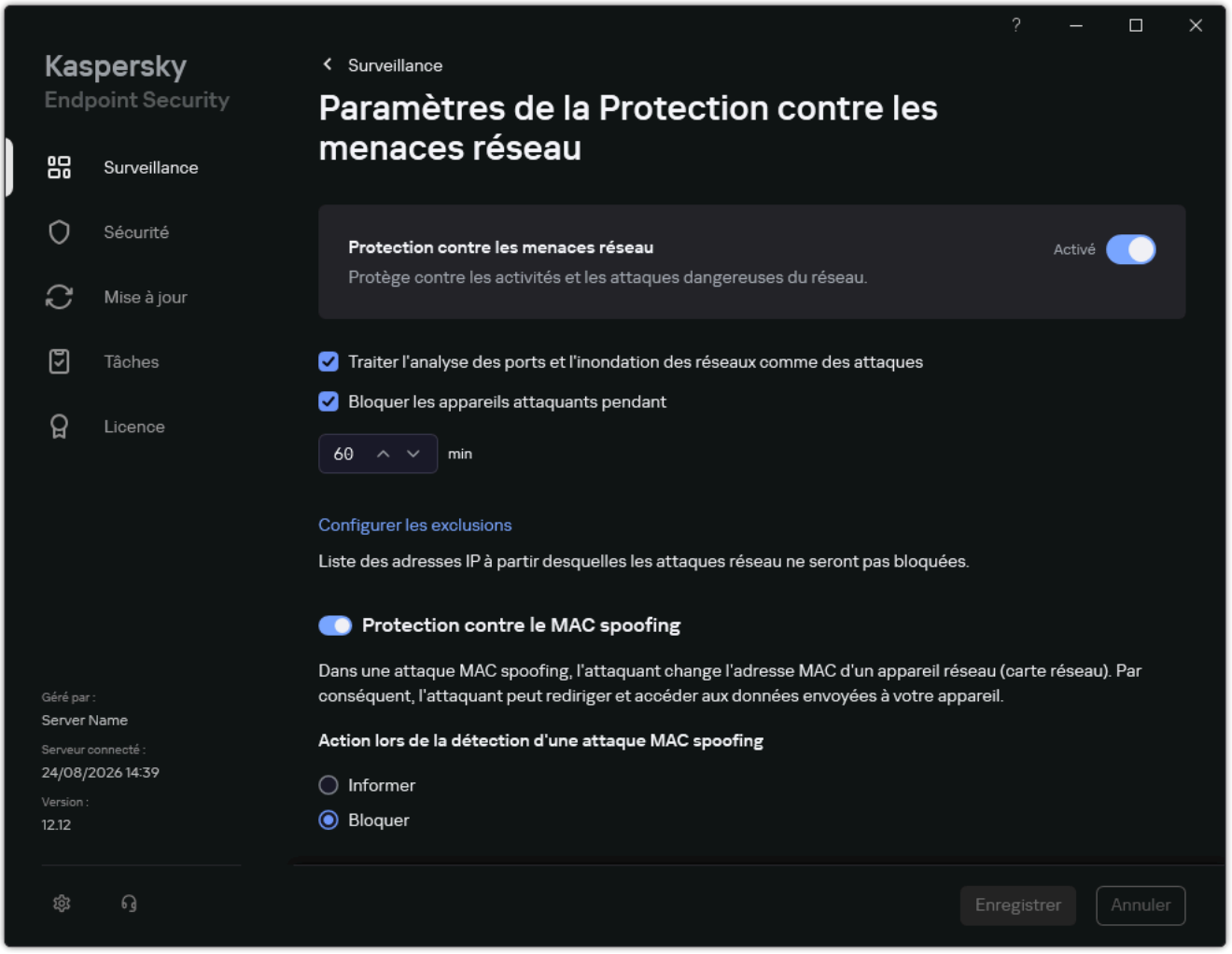
6. Modifier la durée de blocage de l'ordinateur attaquant.

7. Enregistrez vos modifications.

Comment bloquer un ordinateur attaquant dans l'interface utilisateur 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 **Protection principale** → **Protection contre les menaces réseau**.



Paramètres de la Protection contre les menaces réseau

3. Activez le commutateur **Bloquer les appareils attaquants pendant N min**.

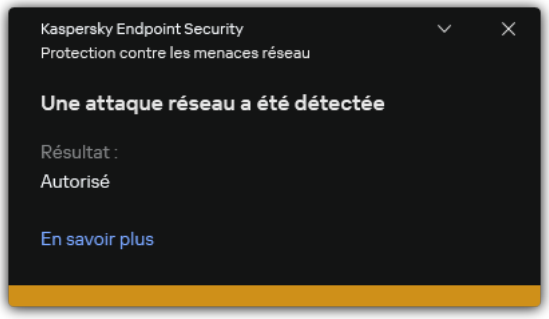
   Si cette option est activée, le module Protection contre les menaces réseau ajoute l'ordinateur à l'origine de l'attaque à la liste des ordinateurs à bloquer. Cela signifie que le module Protection contre les menaces réseau bloque la connexion réseau avec l'ordinateur attaquant après la première tentative 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. Le temps minimum qu'un ordinateur attaquant doit passer dans la liste du groupe est d'une minute. La durée maximale est de 999 minutes.

4. Définissez une durée de blocage différente pour un ordinateur attaquant dans le champ sous l'interrupteur à bascule **Bloquer les appareils attaquants pendant X min**.

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. Kaspersky Endpoint Security crée l'événement *Une attaque réseau a été détectée*. L'événement contient des informations à propos de l'ordinateur attaquant : adresses IP et MAC.

Vous pouvez consulter l'adresse MAC de l'ordinateur attaquant dans l'interface utilisateur de l'application ou dans la console de Kaspersky Security Center de version 15.1 ou ultérieure.



Notification concernant la détection d'une attaque réseau

Kaspersky Endpoint Security débloque l'ordinateur à l'expiration du délai spécifié. La console Kaspersky Security Center ne fournit pas d'outils de surveillance des ordinateurs bloqués autres que les événements *Une attaque réseau a été détectée* dans le rapport. Vous pouvez afficher une liste des ordinateurs bloqués uniquement dans l'interface de l'application. Cette fonctionnalité est fournie par l'outil *Surveillance du réseau*. Vous pouvez également utiliser l'outil Surveillance du réseau pour débloquer un ordinateur.

Pour débloquer un ordinateur :

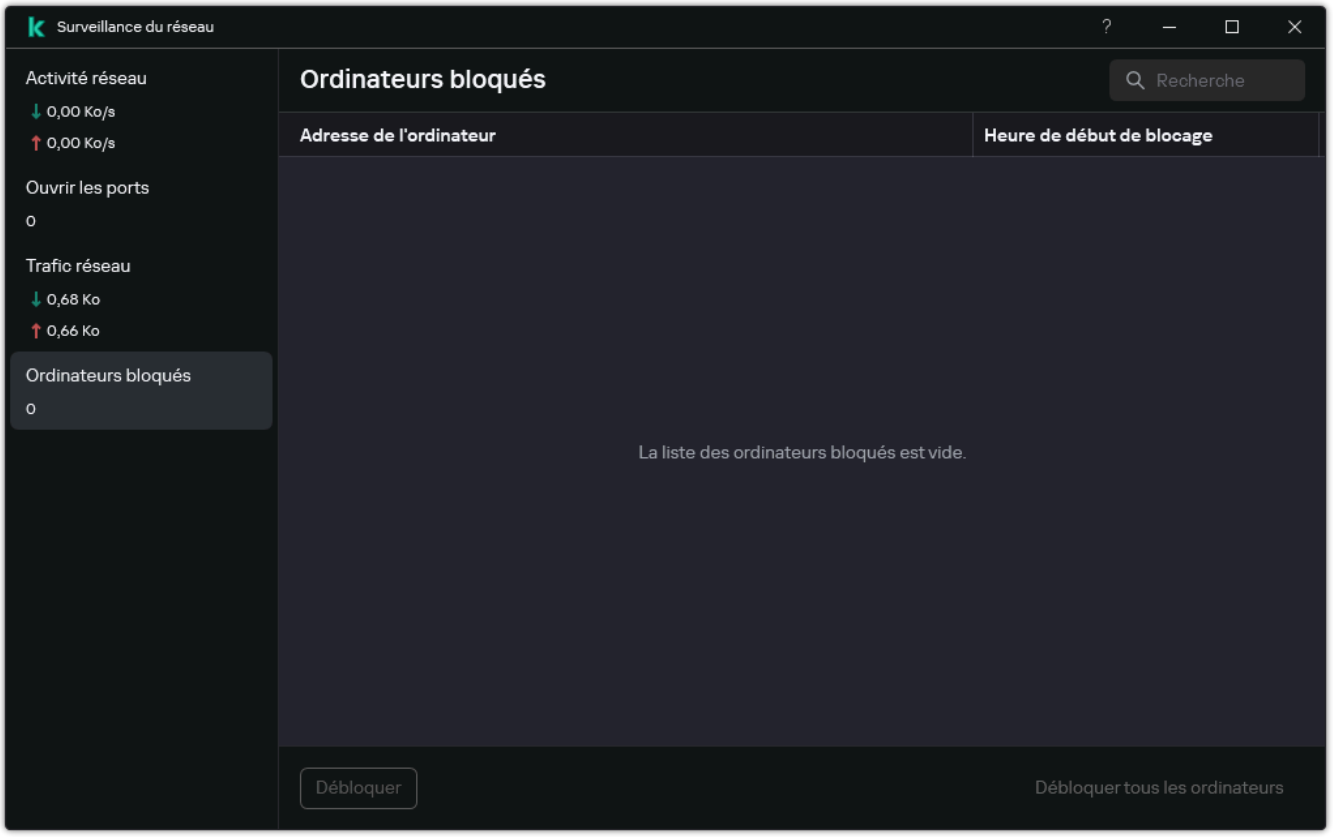
1. Dans la fenêtre principale de l'application, dans la section **Surveillance**, cliquez sur la mosaïque **Surveillance du réseau**.

2. Rendez-vous dans l'onglet **Ordinateurs bloqués**.

   Cela ouvre une liste d'ordinateurs bloqués (voir figure ci-dessous).

   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.

3. Sélectionnez l'ordinateur que vous souhaitez débloquer et cliquez sur **Débloquer**.



Liste des ordinateurs bloqués

Configuration des adresses des exclusions du blocage

Kaspersky Endpoint Security peut reconnaitre 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. Vous pouvez également sélectionner le protocole et le port utilisés pour la communication et autoriser des activités réseau spécifiques.

Comment configurer les adresses des exclusions du blocage dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces réseau**.
5. Cliquez sur le bouton **Exclusions** dans le groupe **Paramètres de la Protection contre les menaces réseau**.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
7. Saisissez l'adresse IP de l'ordinateur à l'origine des attaques réseaux qui ne devront pas être bloquées.

   Si nécessaire, sélectionnez le protocole et les ports via lesquels les données sont transmises.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

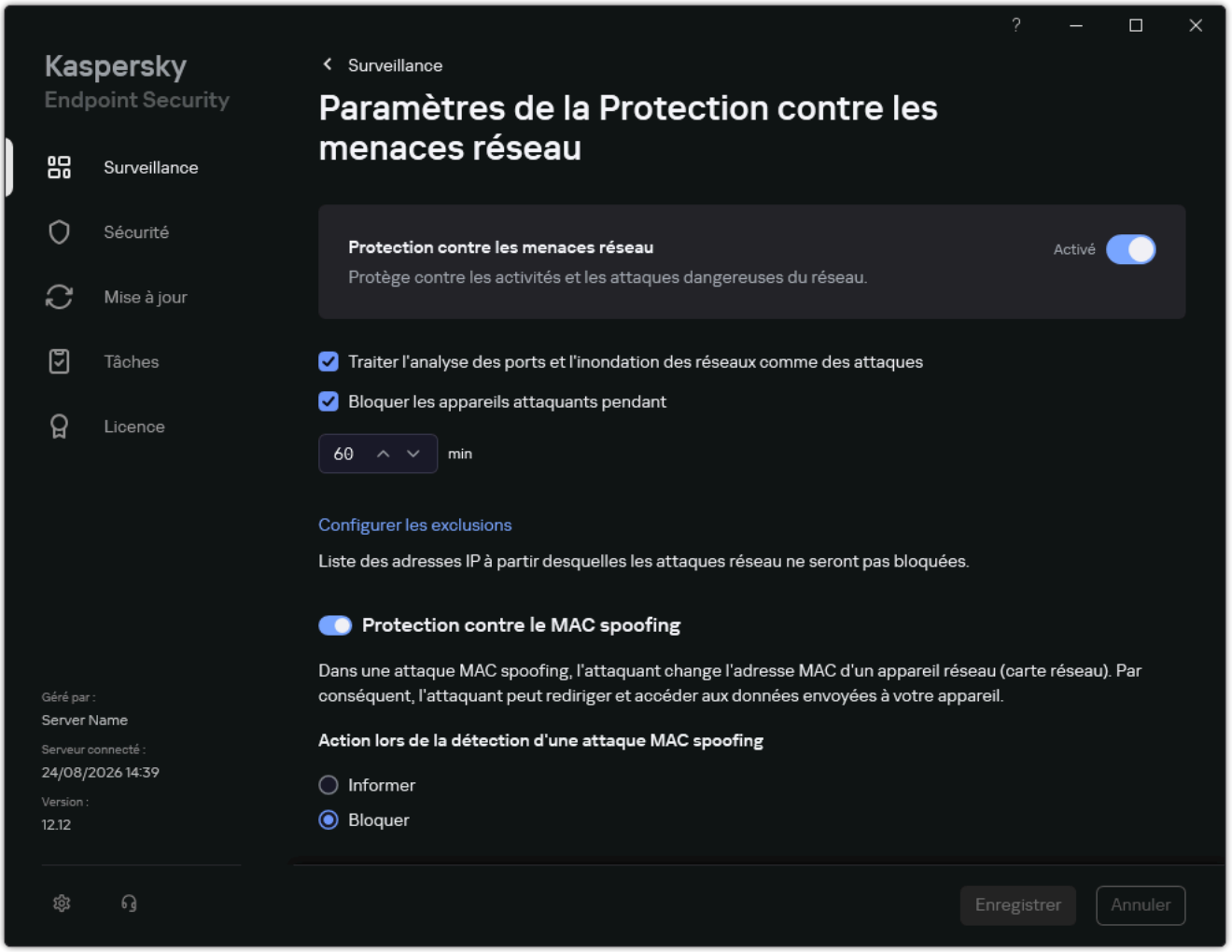
Configuration des adresses exclues du blocage dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Adresses IP**.
   Une fenêtre reprenant la liste des adresses IP de confiance s'ouvre.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
7. Saisissez l'adresse IP de l'ordinateur à l'origine des attaques réseaux qui ne devront pas être bloquées.
   Le cas échéant, indiquez le sous-réseau.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment configurer les adresses des exclusions du blocage dans l'interface utilisateur 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 **Protection principale** → **Protection contre les menaces réseau**.



Paramètres de la 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.

   Si nécessaire, sélectionnez le protocole et les ports via lesquels les données sont transmises.

6. Enregistrez vos modifications.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces réseau**.
4. Cliquez sur le bouton **Exclusions** dans le groupe **Paramètres de la Protection contre les menaces réseau**.
5. 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. Appuyez 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.
6. Pour importer la liste des exclusions, procédez comme suit :
   a. Appuyez 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. Ouvrez le fichier.

      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.

Comment exporter et importer une liste d'exclusions dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces réseau**.
5. Dans la partie supérieure de la fenêtre, cliquez sur le lien **Adresses IP de confiance**.

   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. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des exclusions dans un fichier JSON dans le dossier des téléchargements par défaut.

7. Pour importer la liste des exclusions, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des exclusions.

   b. Ouvrez le fichier.

      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 JSON.

8. Enregistrez vos modifications.

Configuration de la Protection contre les menaces 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.

Vous ne pouvez pas configurer d'exclusions distinctes pour ces types d'attaques. Cela signifie que même si des adresses IP individuelles sont ajoutées à la zone de confiance, Kaspersky Endpoint Security bloque l'ordinateur attaquant si une telle attaque est détectée. Vous pouvez activer ou désactiver la détection de telles attaques.

Il est déconseillé d'activer la protection contre l'usurpation d'adresse MAC sur les machines virtuelles dans l'infrastructure Microsoft Hyper-V. En raison des particularités de la plateforme Microsoft Hyper-V, Kaspersky Industrial CyberSecurity for Nodes peut bloquer l'hyperviseur en raison de résultats faussement positifs.

Comment configurer la Protection contre les menaces réseau par type dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection principale** → **Protection contre les menaces réseau**.
4. Utilisez la case **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection de ces attaques.

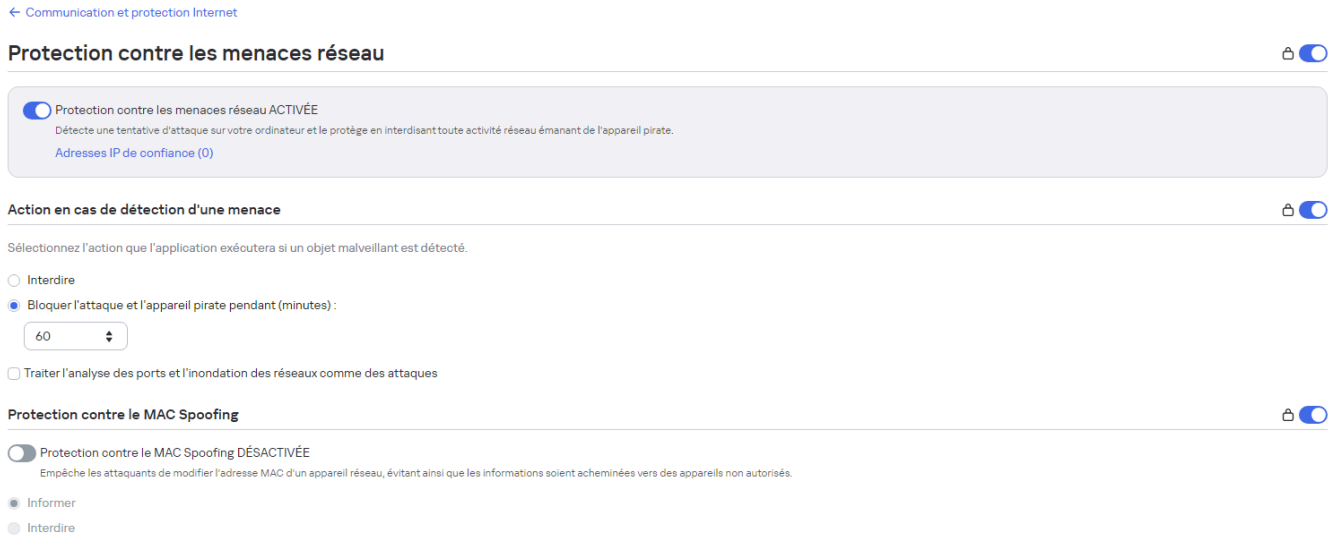
   Si cette fonctionnalité est activée, Kaspersky Endpoint Security surveille le trafic réseau à la recherche de pratiques de balayage des ports et d'inondation des réseaux. Si un tel comportement est détecté, l'application en informe l'utilisateur et envoie l'événement correspondant à Kaspersky Security Center. L'application fournit des informations sur l'ordinateur qui effectue les requêtes. Ces informations sont nécessaires pour assurer une réponse rapide. Toutefois, Kaspersky Endpoint Security ne bloque pas l'ordinateur qui effectue les requêtes, car il se peut que ce type de trafic soit normal sur le réseau de l'entreprise.
5. Dans le groupe **Mode de protection contre le MAC spoofing**, sélectionnez l'une des options suivantes :
   - **Ne pas suivre le MAC spoofing**.
   - **Informer**.
   - **Bloquer**.
6. Enregistrez vos modifications.

Comment configurer la Protection contre les menaces réseau par type dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Protection contre les menaces réseau**.



Paramètres de la Protection contre les menaces réseau

5. Utilisez la case **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection de ces attaques.

   Si cette fonctionnalité est activée, Kaspersky Endpoint Security surveille le trafic réseau à la recherche de pratiques de balayage des ports et d'inondation des réseaux. Si un tel comportement est détecté, l'application en informe l'utilisateur et envoie l'événement correspondant à Kaspersky Security Center. L'application fournit des informations sur l'ordinateur qui effectue les requêtes. Ces informations sont nécessaires pour assurer une réponse rapide. Toutefois, Kaspersky Endpoint Security ne bloque pas l'ordinateur qui effectue les requêtes, car il se peut que ce type de trafic soit normal sur le réseau de l'entreprise.

6. Sous **Protection contre le MAC Spoofing**, configurez la détection des attaques de MAC spoofing :

   a. Utilisez le commutateur **Protection contre le MAC Spoofing ACTIVÉE** pour activer ou désactiver la détection de ces attaques.

   b. Sélectionnez l'action à exécuter lorsqu'une attaque de MAC spoofing est détectée :

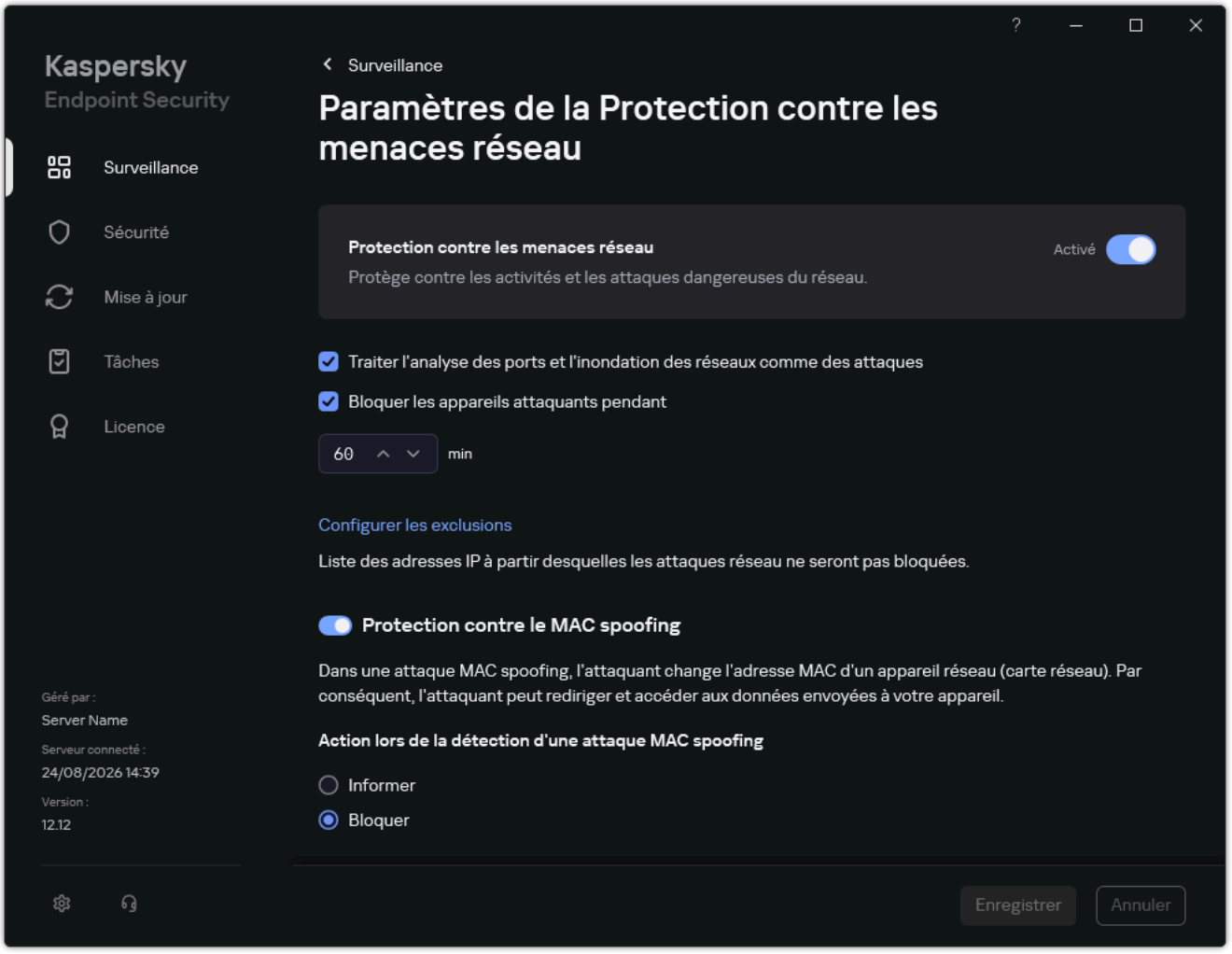
      - **Informer**.
      - **Interdire**.

7. Enregistrez vos modifications.

Comment configurer la Protection contre les menaces réseau par type 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 **Protection principale** → **Protection contre les menaces réseau**.



Paramètres de la 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.

   Si cette fonctionnalité est activée, Kaspersky Endpoint Security surveille le trafic réseau à la recherche de pratiques de balayage des ports et d'inondation des réseaux. Si un tel comportement est détecté, l'application en informe l'utilisateur et envoie l'événement correspondant à Kaspersky Security Center. L'application fournit des informations sur l'ordinateur qui effectue les requêtes. Ces informations sont nécessaires pour assurer une réponse rapide. Toutefois, Kaspersky Endpoint Security ne bloque pas l'ordinateur qui effectue les requêtes, car il se peut que ce type de trafic soit normal sur le réseau de l'entreprise.

4. Utilisez le commutateur **Protection contre le MAC spoofing** pour activer ou désactiver la détection de ces attaques.

5. Dans le groupe **Action lors de la détection d'une attaque MAC spoofing**, sélectionnez l'une des options suivantes :

   - **Informer**.
   - **Bloquer**.

6. Enregistrez vos modifications.

Pare-feu

Le module Pare-feu bloque les connexions non autorisées à un 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 l'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. 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 de réseau pour les applications fonctionnent d'une manière particulière. La règle de réseau pour les applications inclut des règles d'accès basées sur l'état du réseau : *Réseau public*, *Réseau local*, *Réseau de confiance*. 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.

Types de connexions réseau

Le Pare-feu permet de surveiller l'activité du réseau en fonction du type de connexion réseau. Kaspersky Endpoint Security obtient le type de connexion réseau via le système d'exploitation de l'ordinateur. Le type de connexion réseau dans le système d'exploitation est défini par l'utilisateur lors de la configuration de la connexion. Vous pouvez modifier le type de connexion réseau dans les paramètres de Kaspersky Endpoint Security. Le Pare-feu contrôle l'activité réseau en fonction du type de réseau spécifié dans les paramètres de Kaspersky Endpoint Security, et non pas du système d'exploitation.

Les types de connexion réseau suivants sont disponibles :

- **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 le type *Réseau public* au réseau Internet. Vous ne pouvez pas modifier le type de 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 un 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.

Compatibilité avec le Pare-feu Windows Defender

Le système d'exploitation possède son propre pare-feu intégré, le *Pare-feu Windows Defender*. Le comportement de l'application varie en fonction du type de système d'exploitation :

- **Poste de travail**. L'utilisation du Pare-feu Kaspersky en parallèle avec le Pare-feu Windows Defender peut entraîner un dysfonctionnement du système d'exploitation. Par conséquent, Kaspersky Endpoint Security dispose d'un mécanisme qui empêche l'utilisation simultanée des deux pare-feu. Lorsque vous activez le Pare-feu Kaspersky, le système d'exploitation désactive automatiquement le Pare-feu Windows Defender. Lorsque vous désactivez le Pare-feu Kaspersky, le système d'exploitation réactive automatiquement le Pare-feu Windows Defender afin que l'ordinateur reste protégé.

- **Serveur**. Le Pare-feu Kaspersky et le Pare-feu Windows Defender sont incompatibles. Le programme d'installation de Kaspersky Endpoint Security supprime automatiquement le Pare-feu Windows Defender lors de l'installation de l'application.

Activation et désactivation du Pare-feu

Par défaut, le Pare-feu est activé et fonctionne en mode optimal.

Comment activer ou désactiver le Pare-feu dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.
4. Utilisez la case **Pare-feu** pour activer ou désactiver le module.
5. Enregistrez vos modifications.

Comment activer ou désactiver le Pare-feu dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.
5. Utilisez le commutateur **Pare-feu ACTIVÉ** pour activer ou désactiver le module.
6. Enregistrez vos modifications.

Comment activer ou désactiver le Pare-feu 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 **Protection principale** → **Pare-feu**.
3. Utilisez le commutateur **Pare-feu** pour activer ou désactiver le module.
4. Enregistrez vos modifications.

Par conséquent, si le Pare-feu est activé, Kaspersky Endpoint Security contrôle l'activité du réseau et bloque les connexions réseau non autorisées à votre ordinateur, ainsi que l'activité réseau non autorisée des applications sur votre ordinateur. L'activité du réseau est également contrôlée par le module Protection contre les menaces réseau. Le module Protection contre les menaces réseau (également appelé Intrusion Detection System, IDS) surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau.

> Kaspersky Endpoint Security enregistre les événements d'attaque réseau dans ses rapports, quels que soient les paramètres du Pare-feu. Même si le Pare-feu bloque la connexion réseau à l'aide des règles et empêche ainsi une attaque réseau, le module Protection contre les menaces réseau enregistre les événements d'attaque réseau. Il est nécessaire pour générer des informations statistiques sur les attaques réseau sur les ordinateurs de votre organisation.

Modification du type de connexion réseau

Par défaut, le Pare-feu attribue le type *Réseau public* au réseau Internet. Vous ne pouvez pas modifier le type de réseau Internet.

Pour modifier le type de connexion réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.
3. Cliquez sur **Réseaux disponibles**.
4. Sélectionnez la connexion réseau dont vous souhaitez modifier le type.
5. Dans la colonne **Type de réseau**, sélectionnez le type de 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 un 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

Le pare-feu filtre l'ensemble de l'activité réseau sur l'ordinateur conformément aux règles pour les paquets réseau. Les règles pour les paquets réseau contiennent des conditions (par exemple, direction, protocole) que le pare-feu applique pour contrôler les connexions réseau de l'ordinateur. Les règles pour les paquets réseau spécifient également l'action que le pare-feu effectue avec la connexion qui correspond à la règle (autoriser ou interdire la connexion).

Recommandations pour la création de règles pour les paquets réseau

Vous pouvez définir une adresse IP ou une plage d'adresses IP pour filtrer l'activité réseau. Vous pouvez également indiquer un nom DNS.

Si un nom DNS est utilisé dans une règle, Kaspersky Endpoint Security résout ce nom DNS en adresse IP, puis traite la règle comme si cette adresse IP y était indiquée.

Kaspersky Endpoint Security peut résoudre les noms DNS dans les cas suivants :

- Lancement de l'application

- Modification des paramètres du Pare-feu

Lorsque l'application résout les noms DNS depuis l'ordinateur sur lequel elle est installée, un grand nombre de requêtes peuvent être envoyées au serveur DNS. Pour éviter cela, nous vous recommandons d'utiliser des adresses IP plutôt que des noms DNS lors de la création de règles.

Dans certains cas, l'utilisation de noms DNS dans les noms de paquets réseau peut présenter des risques, car le propriétaire du serveur DNS peut modifier les paramètres de l'enregistrement DNS. Un acteur malveillant peut aussi usurper les messages DNS et contourner les règles du pare-feu.

Vous pouvez contrôler les connexions réseau en fonction des noms DNS à l'aide des règles du Contrôle Internet. Si vous devez définir un nom DNS dans les règles de pare-feu :

- Assurez la sécurité du réseau local de l'entreprise.
- Assurez la sécurité de la mise en cache et des serveurs DNS faisant autorité.
- Activez la protection de l'enregistrement DNS contre toute modification.

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.

Méthodes de création de règles 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.

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, dans la section **Surveillance**, cliquez sur la mosaïque **Surveillance du réseau**.
2. Rendez-vous dans 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 réseau**.

   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 **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

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **Règles pour les paquets**.

   Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.

4. Dans la liste déroulante **Ajouter**, sélectionnez l'emplacement de la règle dans la liste : en haut de la liste, en bas de la liste ou à côté de la règle sélectionnée.

   La position de la règle dans la liste détermine la priorité de la règle. La règle située en haut de la liste a la priorité la plus élevée.

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 **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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres du Pare-feu**.

   Cette action ouvre la liste des règles pour les paquets réseau et la liste des règles réseau des applications.

5. Rendez-vous dans 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.

6. Dans la liste déroulante **Ajouter**, sélectionnez l'emplacement de la règle dans la liste : en haut de la liste, en bas de la liste ou à côté de la règle sélectionnée.

   La position de la règle dans la liste détermine la priorité de la règle. La règle située en haut de la liste a la priorité la plus élevée.

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 bouton . 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. Sauvegardez la nouvelle règle de réseau.

11. Utilisez les boutons **En haut**/**En 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. Pour ce faire, décochez la case à côté de l'objet.

Comment créer une règle pour les paquets réseau dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.

5. 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.

6. Cliquez sur **Ajouter**.

   Cette action ouvre le formulaire permettant de créer une règle réseau.

7. Saisissez manuellement le nom du service réseau dans le champ **Nom de la règle**.

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 un modèle de règle**. 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.

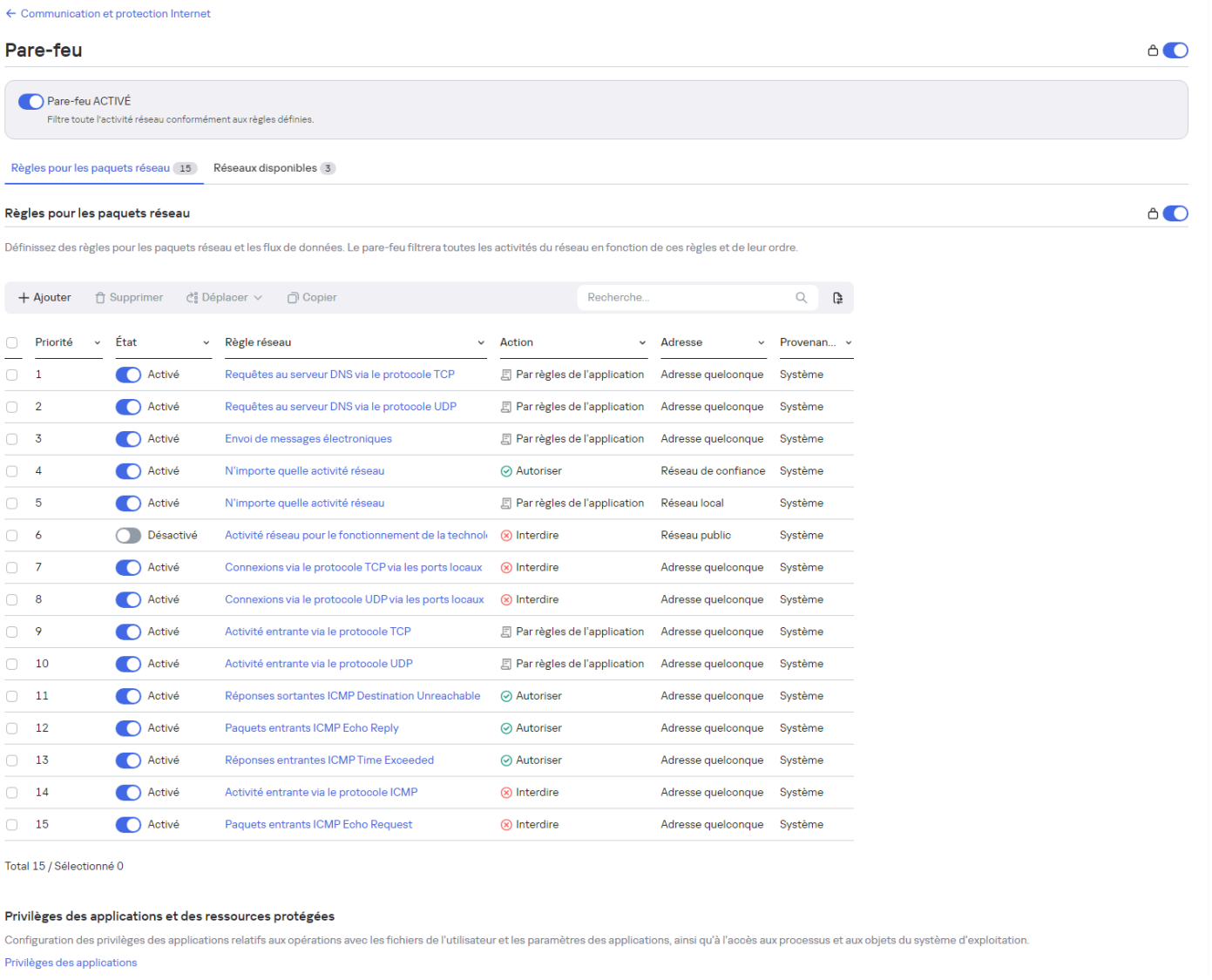
10. Enregistrez la règle de réseau.

    La nouvelle règle réseau sera ajoutée à la liste.

11. Utilisez le bouton **Déplacer** 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.



Règles pour les paquets du Pare-feu

Paramètres des règles pour les paquets réseau

Paramètre	Description
Action	**Autoriser**. **Bloquer**. **Par règles de l'application**. Si cette option est sélectionnée, le pare-feu applique les règles réseau des applications à la connexion réseau.

Paramètre	Description
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 de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée. Plage de valeurs possibles pour les numéros de port : 0–65535. Dans chaque champ, vous pouvez saisir plusieurs valeurs séparées par une virgule (`,`) ou définissez une plage de valeurs à l'aide du signe « `-` ». Par exemple : • `100,101` • `100-130` • `100,110-130`
Direction	**Entrant (paquet)**. Le pare-feu applique la règle réseau à tous les paquets réseau entrants. **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. **Entrant/Sortant**. Le pare-feu applique la règle réseau à tous les paquets réseau entrants et sortants. **Sortant (paquet)**. Le pare-feu applique la règle réseau à tous les paquets réseau sortants. **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.
Adaptateurs réseau	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.
Durée de vie (TTL)	Limitation du contrôle des paquets réseau en fonction de leur durée de vie (Time to Live, TTL).
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). Vous pouvez également indiquer le nom DNS d'un ordinateur au lieu de son adresse IP. Vous devez utiliser les noms DNS uniquement pour les ordinateurs du réseau local ou les services internes. L'interaction avec les services cloud (comme Microsoft Azure) et les autres ressources Internet doit être administrée par le module Contrôle Internet. Si, dans la règle de paquet réseau, vous avez ajouté un nom DNS dont l'adresse IP n'a pas pu être déterminée, Kaspersky Endpoint Security affichera un avertissement. Dans la liste des règles de paquets réseau de Web Console, une colonne est ajoutée avec une description de l'erreur. Dans la Console d'administration (MMC), la description de l'erreur n'est pas disponible. Ces règles de paquet sont mises en évidence en couleur.
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. L'application stocke les adresses locales uniquement si une liste d'adresses distantes est définie. C'est-à-dire que la valeur **Adresses de la liste** a été sélectionnée pour **Adresses distantes** et qu'au moins une adresse a été ajoutée. Les applications ne peuvent pas toujours obtenir une adresse locale. Si c'est le cas, ce paramètre est ignoré.

Activation et désactivation de la règle pour les paquets réseau

Pour activer ou désactiver la règle pour les paquets réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.
3. Cliquez sur **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **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**. Si cette option est sélectionnée, le pare-feu applique les règles réseau des applications à la connexion réseau.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **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. Utilisez les boutons **Haut**/**Bas** pour configurer la priorité de la règle 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres du Pare-feu**.

   Cette action ouvre la liste des règles pour les paquets réseau et la liste des règles réseau des applications.

5. Rendez-vous dans l'onglet **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. 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. Enregistrez le fichier.

      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. Ouvrez le fichier.

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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.

5. Pour exporter la liste des règles dans le groupe **Règles pour les paquets réseau**, procédez comme suit :

   a. Sélectionnez les règles que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

   Kaspersky Endpoint Security exporte la liste des règles dans un fichier JSON dans le dossier des téléchargements par défaut.

6. Pour importer la liste des règles dans le groupe **Règles pour les paquets réseau**, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

   Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des règles.

   b. Ouvrez le fichier.

   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 JSON.

7. Enregistrez vos modifications.

Définition de règles pour les paquets réseau au format XML

Le pare-feu autorise l'exportation des règles pour les paquets réseau au format XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre de règles du même type.

Le fichier XML contient deux nœuds principaux : `Rules` et `Resources`. Le nœud `Rules` présente la liste des règles pour les paquets réseau. Ce nœud contient des règles configurées par défaut (*règles prédéfinies*) ainsi que des règles ajoutées par l'utilisateur (*règles personnalisées*).

Marquage des règles pour les paquets réseau

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
```

```
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Paramètres des règles pour les paquets réseau au format XML

Paramètre	Description	Valeur
`<key name="0000">`	Priorité de la règle. Plus la valeur est basse, plus la priorité est élevée.	Entier La valeur de priorité doit être composée de 4 chiffres. Les nœuds du fichier XML doivent être classés par valeur de priorité, en commençant par `0000`.
`RuleId`	Identifiant de la règle.	**Règles prédéfinies** `100` – **Requêtes au serveur DNS via le protocole TCP**. `101` – **Requêtes au serveur DNS via le protocole UDP**. `102` – **Envoi de messages électroniques**. `110` – **N'importe quelle activité réseau** (Réseaux de confiance). `125` – **N'importe quelle activité réseau** (Réseaux locaux). `130` – **Activité réseau pour le fonctionnement de la technologie du bureau à distance**. `131` – **Connexions via le protocole TCP via les ports locaux**. `132` – **Connexions via le protocole UDP via les ports locaux**. `133` – **Activité entrante via le protocole TCP**. `134` – **Activité entrante via le protocole UDP**. `137` – **Réponses sortantes ICMP Destination Unreachable**. `138` – **Paquets entrants ICMP Echo Reply**. `140` – **Réponses entrantes ICMP Time Exceeded**. `142` – **Activité entrante via le protocole ICMP**. `266` – **Paquets entrants ICMPv6 Echo Request**.
`RuleState`	État de la règle.	`0` – la règle prédéfinie est désactivée `1` – la règle prédéfinie est activée `2` – la règle personnalisée est désactivée `3` – la règle personnalisée est activée
`RuleTypeId`	Identifiant du type de règle.	`4` – règle pour les paquets réseau.
`AppIdEx`	Identifiant de l'application à laquelle appartient la règle pour les paquets réseau.	Si la règle n'appartient à aucune application, la valeur est `0`.
`ResIdEx`	Identifiant principal de la ressource avec des paramètres de règles. Vous pouvez utiliser cet identifiant pour localiser un groupe avec des paramètres de règles dans le nœud `Resources`.	Entier
`ResIdEx2`	Identifiant du type de réseau.	`0` – **Adresse quelconque**. `50` – **Réseaux de confiance**. `51` – **Réseaux locaux**. `52` – **Réseaux publics**. `<Network Identifier>` – **Adresses de la liste** (les adresses sont définies manuellement).
`AccessFlag`	Valeur du paramètre **Action**.	`0` – **Autoriser**. `2` – **Par règles de l'application**. `3` – **Bloquer**. `4` – **Autoriser** et **Consigner dans le rapport**. `6` – **Par règles de l'application** et **Consigner dans le rapport**. `7` – **Bloquer** et **Consigner dans le rapport**.
`</key>`		

Le nœud `Resources` contient les paramètres des règles pour les paquets réseau. Les paramètres personnalisés de règles pour les paquets réseau figurent dans le groupe `<key name="0004">`.

Marquage personnalisé des règles pour les paquets réseau

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Paramètres personnalisés des règles pour les paquets réseau

Paramètre	Description	Valeur
`<key name="Data">`	Identifiant du bloc de paramètres.	Entier
`RemotePorts`	Valeur du paramètre **Ports distants**.	Liste des plages de ports distants.
`LocalPorts`	Valeur du paramètre **Ports locaux**.	Liste des plages de ports locaux.

Paramètre	Description	Valeur
`AdapterBindings`	Valeur du paramètre **Adaptateurs réseau**.	`IpAddresses` – valeur du paramètre **Adresses IP**. `MacAddresses` – valeur du paramètre **Adresses MAC**. `AdapterName` – nom de l'adaptateur réseau. `InterfaceType` – valeur du paramètre **Type d'interface** : • `0` – **Autre**. • `1` – **LoopBack**. • `2` – **Réseau filaire (Ethernet)**. • `3` – **Réseau sans fil (Wi-Fi)**. • `4` – **Tunnel**. • `5` – **Connexion PPP**. • `6` – **Connexion PPPoE**. • `7` – **Connexion VPN**. • `8` – **Connexion modem**.
`unique`	Identifiant interne de la structure.	Entier Il est recommandé de laisser ce paramètre inchangé.
`Proto`	Valeur du paramètre **Protocole**.	`0` – désactivé. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Valeur du paramètre **Direction**.	`1` – **Entrant (paquet)**. `2` – **Sortant (paquet)**. `3` – **Entrant/Sortant**. `4` – **Entrant**. `5` – **Sortant**.

Paramètre	Description	Valeur
`IcmpType`	Valeur du paramètre **Type ICMP**.	**Protocole ICMP** `0` – **Echo Reply** (ICMP) ou désactivé. `3` – **Destination Unreachable** (ICMP). `4` – **Source Quench**. `5` – **Redirect**. `6` – **Alternate Host Address**. `8` – **Echo Request**. `9` – **Router Advertisement**. `10` – **Router Solicitation**. `11` – **Time Exceeded**. `12` – **Parameter Problem**. `13` – **Timestamp**. `14` – **Timestamp Reply**. `15` – **Information Request**. `16` – **Information Reply**. `17` – **Address Mask Request**. `18` – **Address Mask Reply**. `30` – **Traceroute**. `31` – **Datagram Conversion Error**. `32` – **Mobile Host Redirect**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Mobile Registration Request**. `36` – **Mobile Registration Reply**. `37` – **Domain Name Request**. `38` – **Domain Name Reply**. `40` – **Photuris**. **Protocole ICMPv6** `1` – **Destination Unreachable**. `2` – **Packet Too Big**. `3` – **Time Exceeded**. `4` – **Parameter Problem**. `128` – **Echo Request**. `129` – **Echo Reply**. `130` – **Multicast Listener Query**. `131` – **Multicast Listener Report**. `132` – **Multicast Listener Done**. `133` – **Router Solicitation**. `134` – **Router Advertisement**. `135` – **Neighbor Solicitation**. `136` – **Neighbor Advertisement**. `137` – **Redirect Message**. `138` – **Router Renumbering**. `139` – **ICMP Node Information Query**. `141` – **Inverse Neighbor Discovery Solicitation Message**. `142` – **Inverse Neighbor Discovery Advertisement Message**. `143` – **Version 2 Multicast Listener Report**.

Paramètre	Description	Valeur
		`144` – **Home Agent Address Discovery Request Message**. `145` – **Home Agent Address Discovery Reply Message**. `146` – **Mobile Prefix Solicitation**. `147` – **Mobile Prefix Advertisement**. `148` – **Certification Path Solicitation Message**. `149` – **Certification Path Advertisement Message**. `151` – **Multicast Router Advertisement**. `152` – **Multicast Router Solicitation**. `153` – **Multicast Router Termination**.
`IcmpCode`	Valeur du paramètre **Code ICMP**.	`0` – **Code 0** ou désactivé. `1` – **Code 1**. `2` – **Code 2**.
`Flags`	Pointeur d'attribut de structure.	Entier Il est recommandé de laisser ce paramètre inchangé.
`TTL`	Valeur du paramètre **Durée de vie (TTL)**.	Valeur en secondes. Si le paramètre est désactivé, la valeur est `0`.
`</key>`		
`Id`	Identifiant principal de la ressource (voir le nœud `Rules`).	Entier
`ParentID`	Identifiant du groupe parent.	Entier Il est recommandé de laisser ce paramètre inchangé.
`Flags`	État de la règle.	`6` – la règle est désactivée. `38` – la règle est activée.
`Name`	Nom de la règle pour les paquets réseau.	Chaîne

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, dans la section **Surveillance**, cliquez sur la mosaïque **Surveillance du réseau**.

2. Rendez-vous dans 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 **Ouvrir les ports** 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 réseau de 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 **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 **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **Règles pour les applications**.

   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 **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 **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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez la section **Protection principale** → **Pare-feu**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres du Pare-feu**.

   Cette action ouvre la liste des règles pour les paquets réseau et la liste des règles réseau des applications.

5. Rendez-vous dans l'onglet **Règles réseau des applications**.

6. Cliquez sur **Ajouter**.

7. Dans la fenêtre qui s'ouvre, 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.

8. Cliquez sur **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.

9. Sélectionnez l'application requise.

10. Dans la liste déroulante **Ajoutez l'application sélectionnée au groupe de confiance**, sélectionnez **Groupes par défaut**, puis cliquez sur **OK**.

    L'application sera ajoutée au groupe par défaut.

11. 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.

12. Sélectionnez l'onglet **Règles réseau**.

    Cette action permet d'ouvrir la liste des règles réseau que le pare-feu a définies par défaut.

13. Cliquez sur **Ajouter**.

    Cette action permet d'ouvrir les propriétés des règles réseau.

14. Saisissez manuellement le nom du service réseau dans le champ **Nom**.

15. 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.

16. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le rapport.

17. Sauvegardez la nouvelle règle de réseau.

18. Utilisez les boutons **En haut**/**En bas** pour configurer la priorité de la règle réseau.

19. 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Communication et protection Internet** → **Pare-feu**.

5. Dans le groupe **Privilèges des applications et des ressources protégées**, cliquez sur le lien **Privilèges des applications**.

   Cette action ouvre la fenêtre de configuration des privilèges de l'application et la liste des ressources protégées.

6. Rendez-vous dans 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** dans le groupe **Applications**.

   Cette action lance l'Assistant pour ajouter une application à un groupe de confiance.

8. Sélectionnez le groupe de confiance pertinent pour l'application.

9. Sélectionnez le type **Application**. Passez à l'étape suivante.

   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.

    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 **Ajouter**.

    Cette action permet d'ouvrir les propriétés des règles d'application.

15. Saisissez manuellement le nom du service réseau dans le champ **Nom de la règle**.

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 un modèle de règle**. 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. Enregistrez la règle de réseau.

    La nouvelle règle réseau sera ajoutée à la liste.

19. Utilisez le bouton **Déplacer** 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 de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée. Plage de valeurs possibles pour les numéros de port : 0–65535. Dans chaque champ, vous pouvez saisir plusieurs valeurs séparées par une virgule (`,`) ou définissez une plage de valeurs à l'aide du signe « `-` ». Par exemple : • `100,101` • `100-130` • `100,110-130`
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). Vous pouvez également indiquer le nom DNS d'un ordinateur au lieu de son adresse IP. Vous devez utiliser les noms DNS uniquement pour les ordinateurs du réseau local ou les services internes. L'interaction avec les services cloud (comme Microsoft Azure) et les autres ressources Internet doit être administrée par le module Contrôle Internet. Si, dans la règle de paquet réseau, vous avez ajouté un nom DNS dont l'adresse IP n'a pas pu être déterminée, Kaspersky Endpoint Security affichera un avertissement. Dans la liste des règles de paquets réseau de Web Console, une colonne est ajoutée avec une description de l'erreur. Dans la Console d'administration (MMC), la description de l'erreur n'est pas disponible. Ces règles de paquet sont mises en évidence en couleur.
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. L'application stocke les adresses locales uniquement si une liste d'adresses distantes est définie. C'est-à-dire que la valeur **Adresses de la liste** a été sélectionnée pour **Adresses distantes** et qu'au moins une adresse a été ajoutée. Les applications ne peuvent pas toujours obtenir une adresse locale. Si c'est le cas, ce paramètre est ignoré.

Activation et désactivation de la règle réseau des applications

Pour activer ou désactiver la règle réseau des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.
3. Cliquez sur **Règles pour les applications**.

   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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **Règles pour les applications**.

   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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **Règles pour les applications**.

   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**.
   - **Interdire**.
   - **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Protection principale** → **Pare-feu**.

3. Cliquez sur **Règles pour les applications**.

   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. Utilisez les boutons **Haut**/**Bas** pour configurer la priorité de la règle 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, dans la section **Surveillance**, cliquez sur la mosaïque **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 **Ouvrir les ports** 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 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.

Le module Protection contre les Exploits surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus.

Activation et désactivation de la Protection contre les Exploits

Par défaut, la Protection contre les Exploits est activée et fonctionne en mode optimal. Kaspersky Endpoint Security surveille les fichiers exécutables exécutés par les 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).

Comment activer ou désactiver la Protection contre les Exploits dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre les Exploits**.
4. Utilisez la case **Protection contre les Exploits** pour activer ou désactiver le module.
5. Sélectionnez l'action appropriée dans le groupe **En cas de détection d'un exploit** :
   - **Bloquer**. 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.
   - **Informer**. 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.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver la Protection contre les Exploits dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre les Exploits**.
5. Utilisez le commutateur **Protection contre les Exploits** pour activer ou désactiver le module.

6. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

- **Interdire**. 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.

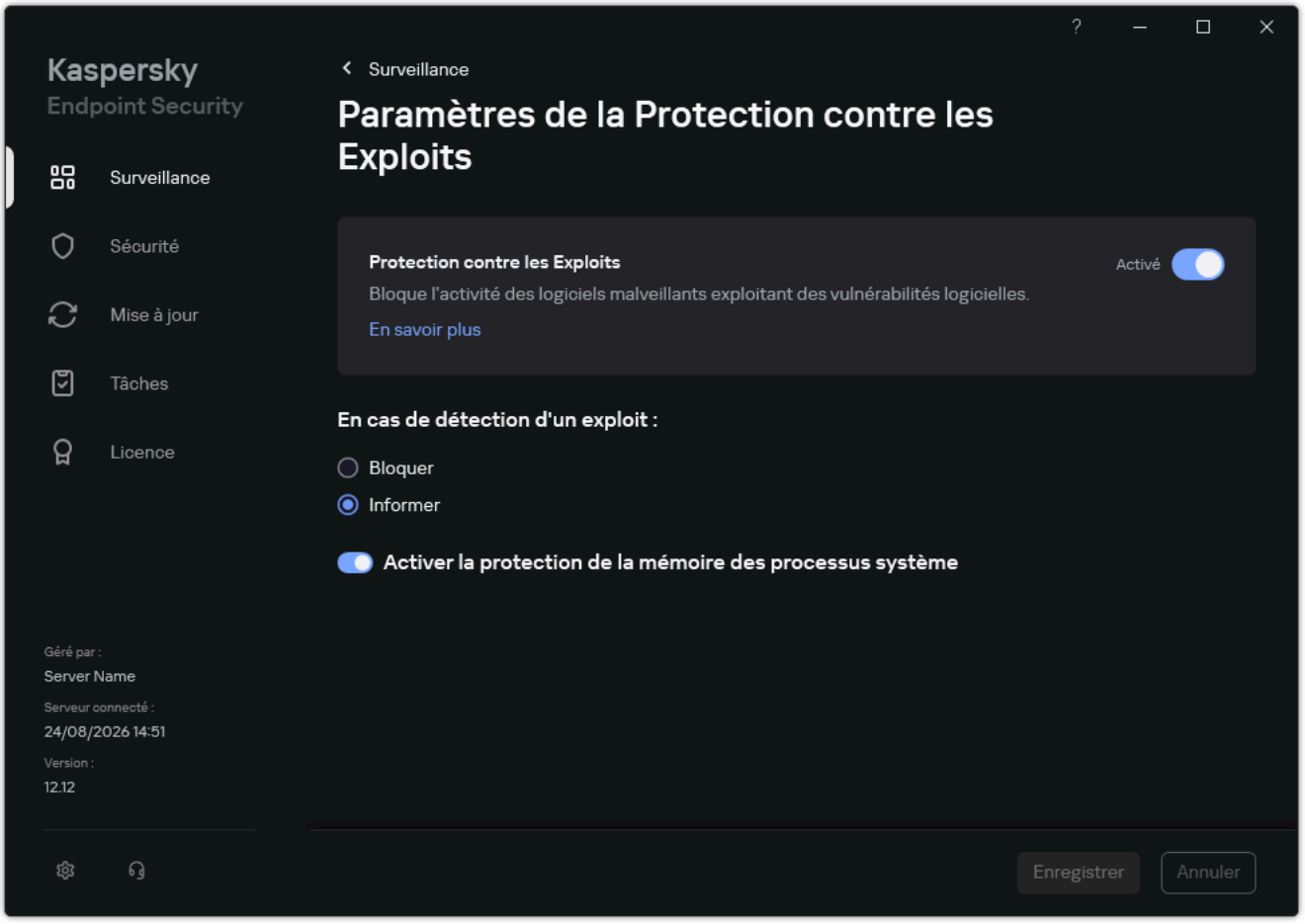
- **Informer**. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert un exploit, crée une entrée dans le journal qui reprend les informations relatives à l'exploit et ajoute les informations relatives à l'exploit dans la liste des menaces actives.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment activer ou désactiver la Protection contre les Exploits 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 **Protection avancée** → **Protection contre les Exploits**.



Paramètres de protection contre les exploits

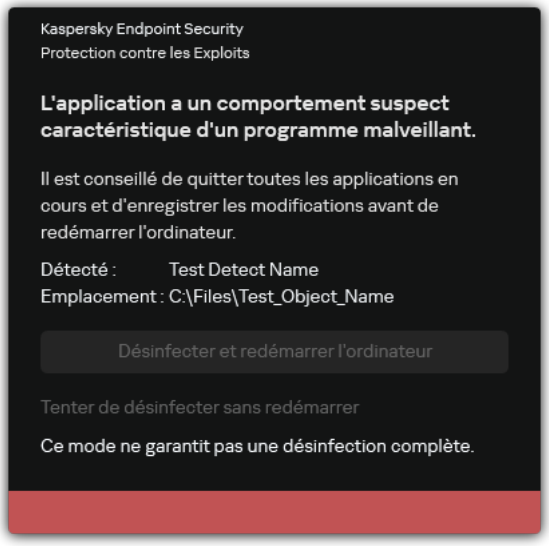
3. Utilisez le commutateur **Protection contre les Exploits** pour activer ou désactiver le module.

4. Sélectionnez l'action appropriée dans le groupe **En cas de détection d'un exploit** :

   - **Bloquer**. 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.

   - **Informer**. 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.

5. Enregistrez vos modifications.



Notification concernant une menace active

Protection de la mémoire des processus système

La protection de la mémoire des processus système est activée par défaut. Kaspersky Endpoint Security bloque les processus externes qui tentent d'accéder aux processus du système.

Comment activer ou désactiver la protection de la mémoire des processus système dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre les Exploits**.

4. Utilisez la case **Activer la protection de la mémoire des processus système** pour activer ou désactiver l'option.

5. Enregistrez vos modifications.

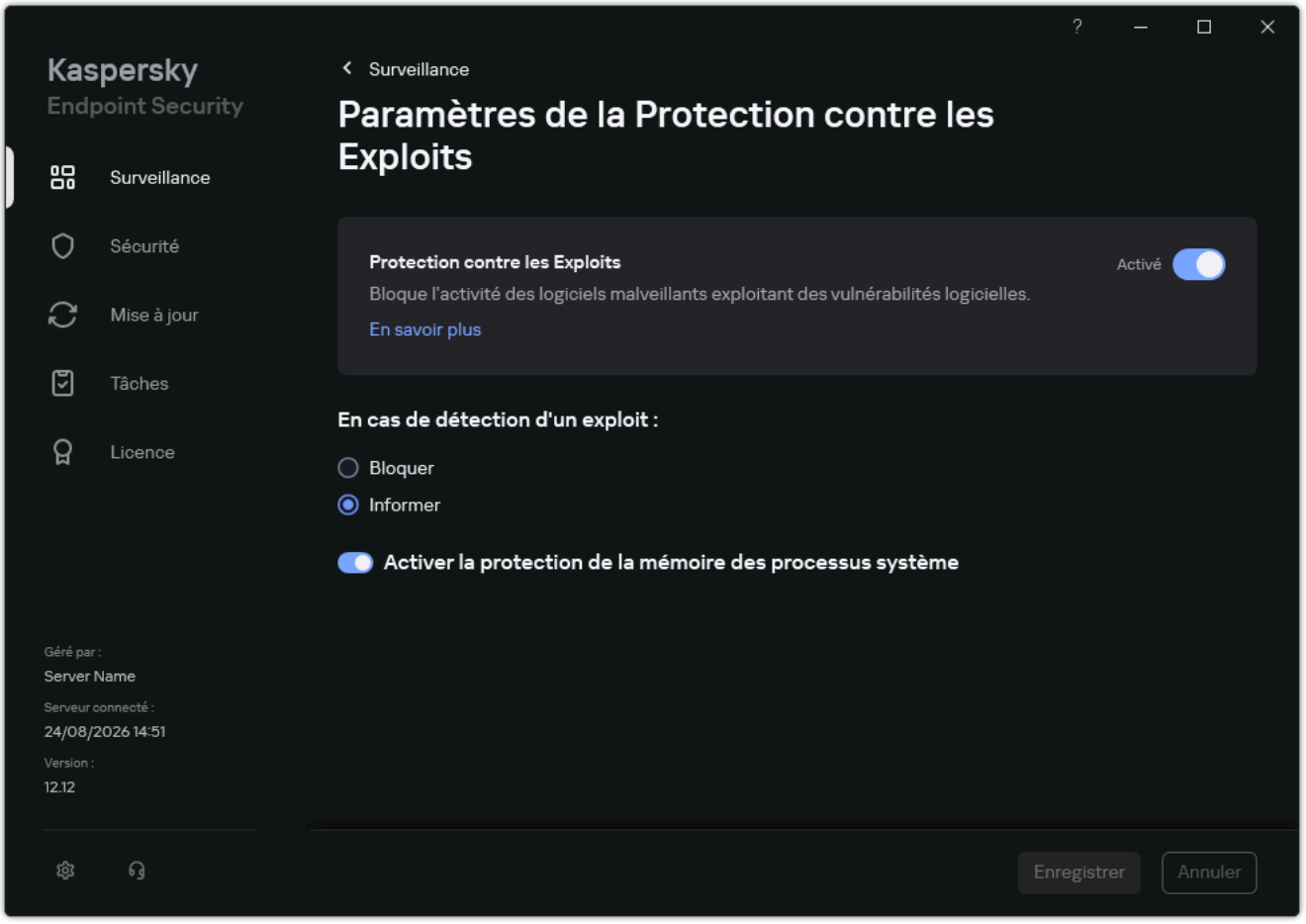
Comment activer ou désactiver la protection de la mémoire des processus système dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre les Exploits**.
5. Utilisez le commutateur **Protection de la mémoire des processus système ACTIVÉE** pour activer ou désactiver cette fonctionnalité.
6. Enregistrez vos modifications.

Comment activer ou désactiver la protection de la mémoire des processus système 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 **Protection avancée** → **Protection contre les Exploits**.



Paramètres de 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.

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 repose sur les modèles de comportement dangereux et garantit la protection proactive de l'ordinateur.

Le module Détection comportementale surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus.

Par défaut, la Détection comportementale est activée et fonctionne dans le mode recommandé par les experts de Kaspersky. En cas de détection d'une activité malveillante, Kaspersky Endpoint Security supprime le fichier exécutable de l'application malveillante.

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.

Comment activer ou désactiver la Détection comportementale dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Détection comportementale**.

5. Utilisez la case **Détection comportementale** pour activer ou désactiver le module.

6. Sélectionnez l'action appropriée dans le groupe **Action exécutée lors de la détection d'une activité malveillante** :

   - **Supprimer**. 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.

   - **Bloquer**. Si cet élément est sélectionné, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.

   - **Informer**. 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.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver la Détection comportementale dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Détection comportementale**

5. Utilisez le commutateur **Détection comportementale ACTIVÉE** pour activer ou désactiver le module.

6. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

   - **Supprimer**. 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.

   - **Interdire**. Si cet élément est sélectionné, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.

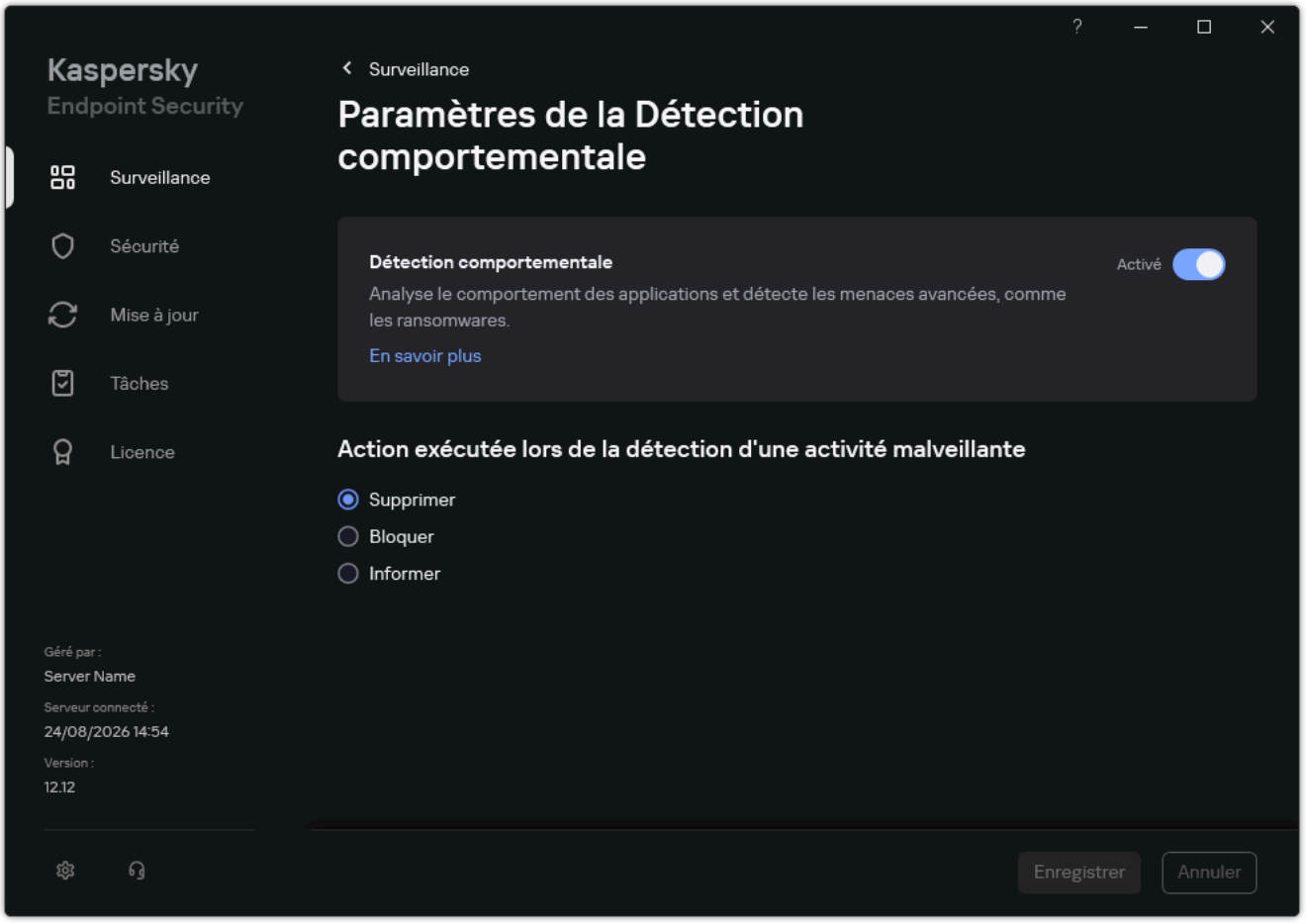
   - **Informer**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver la Détection comportementale 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 **Protection avancée** → **Détection comportementale**.



Paramètres de la Détection comportementale

3. Utilisez le commutateur **Détection comportementale** pour activer ou désactiver le module.

4. Sélectionnez l'action appropriée dans le groupe **Action exécutée lors de la détection d'une activité malveillante** :

   - **Supprimer**. 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.

   - **Bloquer**. Si cet élément est sélectionné, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.

   - **Informer**. 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.

5. 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.

Protection contre le chiffrement

À partir de Kaspersky Endpoint Security 12.12 for Windows, la protection des dossiers partagés contre le chiffrement externe, qui faisait auparavant partie du module Détection comportementale, est désormais un module distinct, appelé Protection contre le chiffrement.

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.

Le module Protection contre le chiffrement 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.

Pour que le module Protection contre le chiffrement fonctionne, il faut activer le module Détection comportementale.

Kaspersky Endpoint Security réalise les opérations suivantes en cas de détection d'une tentative de modification de fichiers dans des dossiers partagés :

- Bloque l'accès à la modification de fichiers pour la session à l'origine de l'activité malveillante (le fichier sera en lecture seule) ;
- Crée des copies de sauvegarde des fichiers modifiés ;
- Ajoute une entrée aux rapports locaux de l'interface de l'application et envoie des informations à Kaspersky Security Center sur l'activité malveillante détectée.
- Si le module Réparation des actions malicieuses est activé, l'application restaure les fichiers modifiés au départ des copies de sauvegarde.

Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe

Par défaut, la protection des dossiers partagés contre le chiffrement externe est activée et fonctionne conformément aux recommandations des experts de Kaspersky. Pour configurer cette fonctionnalité, vous pouvez créer une zone de protection et configurer des exclusions, si nécessaire. Par défaut, l'application identifie automatiquement les dossiers partagés et surveille l'activité des fichiers dans tous les dossiers. En cas de détection d'une tentative de chiffrement externe des fichiers dans les dossiers partagés, Kaspersky Endpoint Security bloque la session de l'utilisateur distant pendant une heure (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.

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre le chiffrement**.

4. Utilisez la case **Protection contre le chiffrement** pour activer ou désactiver la détection d'une activité caractéristique du chiffrement externe.

5. Sélectionnez l'action pertinente que l'application entreprendra en cas de détection d'une tentative de modification des fichiers dans les dossiers partagés :

   - **Bloquer la connexion pendant N min**. Si cette option est sélectionnée, lorsque Kaspersky Endpoint Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, lors de la détection d'une tentative de modification des fichiers dans les dossiers partagés, Kaspersky Endpoint Security ajoute des informations sur cette tentative à la liste des menaces actives, ajoute une entrée aux rapports locaux de l'interface de l'application et envoie des informations à Kaspersky Security Center sur l'activité malveillante détectée.

6. Si nécessaire, modifiez une zone de protection et définissez des exclusions.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.

5. Utilisez le commutateur **Protection contre le chiffrement ACTIVÉE** pour activer ou désactiver la détection d'une activité caractéristique du chiffrement externe.

6. Sélectionnez l'action pertinente que l'application entreprendra en cas de détection d'une tentative de modification des fichiers dans les dossiers partagés :

   - **Bloquer la connexion pendant (minutes) N min**. Si cette option est sélectionnée, lorsque Kaspersky Endpoint Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant (minutes) X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, lors de la détection d'une tentative de modification des fichiers dans les dossiers partagés, Kaspersky Endpoint Security ajoute des informations sur cette tentative à la liste des menaces actives, ajoute une entrée aux rapports locaux de l'interface de l'application et envoie des informations à Kaspersky Security Center sur l'activité malveillante détectée.

7. Si nécessaire, modifiez une zone de protection et définissez des exclusions.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe 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 **Protection avancée** → **Protection contre le chiffrement**.

3. Utilisez la case **Protection des dossiers partagés contre le chiffrement externe** pour activer ou désactiver la détection d'une activité caractéristique du chiffrement externe.

4. Utilisez la case **Protection des dossiers partagés contre le chiffrement externe** pour activer ou désactiver la détection d'une activité caractéristique du chiffrement externe.

5. Sélectionnez l'action pertinente que l'application entreprendra en cas de détection d'une tentative de modification des fichiers dans les dossiers partagés :

   - **Bloquer la connexion pendant (min) N min**. Si cette option est sélectionnée, lorsque Kaspersky Endpoint Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant (min) X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, lors de la détection d'une tentative de modification des fichiers dans les dossiers partagés, Kaspersky Endpoint Security ajoute des informations sur cette tentative à la liste des menaces actives, ajoute une entrée aux rapports locaux de l'interface de l'application et envoie des informations à Kaspersky Security Center sur l'activité malveillante détectée.

6. Si nécessaire, modifiez une zone de protection et définissez des exclusions.

7. Enregistrez vos modifications.

Configuration de la période de blocage d'un ordinateur non fiable

Un *ordinateur non fiable* est un ordinateur distant qui mène des activités malveillantes ou qui chiffre des données. Par défaut, Kaspersky Endpoint Security bloque la session de l'utilisateur distant pendant une heure. À l'expiration de la période de blocage, Kaspersky Endpoint Security supprime l'ordinateur de la liste de blocages et rétablit l'accès au dossier partagé.

Comment configurer la période de blocage d'un ordinateur non fiable dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre le chiffrement**.

4. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez **Bloquer la connexion pendant N minutes**.

5. Configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.

6. Enregistrez vos modifications.

Comment configurer la période de blocage d'un ordinateur non fiable dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.

5. Sous **Action en cas de détection d'une menace**, configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.

6. Enregistrez vos modifications.

Comment configurer la période de blocage d'un ordinateur non fiable 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 **Protection avancée** → **Protection contre le chiffrement**.

3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'option **Bloquer la connexion pendant (min)**.

4. Configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.

5. Enregistrez vos modifications.

En conséquence, l'ordinateur distant sera verrouillé. Pour déverrouiller l'ordinateur distant, vous pouvez redémarrer Kaspersky Endpoint Security.

Modification de la zone de protection

La *zone de protection* est une liste de chemins d'accès aux dossiers partagés, dans laquelle Kaspersky Endpoint Security surveille l'activité des fichiers. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Par défaut, l'application identifie automatiquement les dossiers partagés et surveille l'activité des fichiers dans tous les dossiers.

L'exclusion d'un dossier de la zone de protection 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.

> Vous pouvez également exclure les ordinateurs à partir des lesquels les tentatives de chiffrement externe ne doivent pas être traitées.

Comment modifier une zone de protection dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre le chiffrement**.

4. Dans le groupe **Zone de protection**, sélectionnez l'option **Seuls les dossiers partagés indiqués**.

5. Dans la liste des dossiers, cliquez sur **Ajouter**.

6. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

   > Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.

7. Cliquez sur **OK**.

8. Si nécessaire, définissez les exclusions de la zone de protection :

   a. Cliquez sur le bouton **Selon le masque** dans le groupe **Exclusions de l'analyse**.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

c. Dans la fenêtre qui s'affiche, indiquez l'extension du fichier dans le champ `*.<file extension>` ou le chemin d'un dossier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

L'application ne prend pas en charge certaines extensions des fichiers d'exclusion. Ainsi, vous pouvez indiquer une exclusion comme `*.docx` ou `**\Folder\**`.

Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

9. Enregistrez vos modifications.

Comment modifier une zone de protection dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.

5. Dans le groupe **Zone de protection**, sélectionnez l'option **Uniquement les dossiers partagés indiqués**.

6. Dans la liste des dossiers, cliquez sur **Ajouter**.

7. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

   Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.

8. Cliquez sur **OK**.

9. Si nécessaire, définissez les exclusions de la zone de protection :

   a. Dans la partie supérieure de la fenêtre, cliquez sur le lien **Exclusions de l'analyse**.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   c. Dans la fenêtre qui s'affiche, indiquez l'extension du fichier dans le champ `*.<file extension>` ou le chemin d'un dossier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

   L'application ne prend pas en charge certaines extensions des fichiers d'exclusion. Ainsi, vous pouvez indiquer une exclusion comme `*.docx` ou `**\Folder\**`.

   Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

10. Enregistrez vos modifications.

Comment modifier une zone de protection 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 **Protection avancée** → **Protection contre le chiffrement**.

3. Dans le groupe **Zone de protection**, sélectionnez l'option **Seuls les dossiers partagés indiqués**.

4. Dans la liste des dossiers, cliquez sur **Ajouter**.

5. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

   > Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.

6. Cliquez sur **OK**.

7. Si nécessaire, définissez les exclusions de la zone de protection :

   a. Dans la partie supérieure de la fenêtre, cliquez sur le lien **Exclusions selon un masque**.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   c. Dans la fenêtre qui s'affiche, indiquez l'extension du fichier dans le champ `*.<file extension>` ou le chemin d'un dossier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

      L'application ne prend pas en charge certaines extensions des fichiers d'exclusion. Ainsi, vous pouvez indiquer une exclusion comme `*.docx` ou `**\Folder\**`.

   Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

8. Enregistrez vos modifications.

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

4. Cliquez sur **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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

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 **Commentaire**.

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.

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zone de confiance**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exclusions de l'analyse des logiciels malveillants**.

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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des exclusions d'analyse dans l'interface utilisateur de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

9. Sélectionnez la manière dont vous souhaitez ajouter l'exclusion : **Chemin d'accès au fichier ou au dossier**.

10. Saisissez le chemin d'accès au 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

    Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `C:\Users\*\Folder\`.

11. Dans le groupe **Appliquer l'exclusion à**, 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 **Ajouter aux exclusions** pour l'exclusion.

    Vous pouvez utiliser le commutateur pour mettre fin à une exclusion à tout moment.

14. Enregistrez vos modifications.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Exclusions de l'analyse et applications de confiance** → **Exclusions de l'analyse**.

   Une fenêtre reprenant la liste des exclusions s'ouvre.

5. 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.

6. 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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des exclusions d'analyse dans l'interface utilisateur de l'application.

7. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

8. Cliquez sur **Ajouter**.

9. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.

10. Le lien **Sélectionnez un fichier ou un 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**.

11. 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

12. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

13. Le lien **Description de l'exclusion de l'analyse (cliquez sur les éléments soulignés pour les modifier)** bloque l'ouverture de la fenêtre **Modules de la protection**.

14. Cochez la case située à côté du module **Détection comportementale**.

15. Enregistrez vos modifications.

Ajout d'ordinateurs de confiance pour le chiffrement externe des données

Si votre organisation utilise le chiffrement externe des données dans son flux de travail d'échange de fichiers, vous devez créer une liste d'ordinateurs de confiance. Kaspersky Endpoint Security ne surveille pas le chiffrement des données par les ordinateurs de confiance.

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.

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre le chiffrement**.
5. Cliquez sur le bouton **Par nom ou adresse IP** dans le groupe **Exclusions de l'analyse**.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Par nom ou adresse IP**.
7. Saisissez les adresses IP, la plage d'adresses IP ou les noms des ordinateurs à partir desquels les tentatives de chiffrement externe ne doivent pas être traitées.

   Exemples :

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.
5. Dans la partie droite de la fenêtre, cliquez sur le lien **Exclusions de la Protection contre le chiffrement**.
6. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
7. Saisissez les adresses IP, la plage d'adresses IP ou les noms des ordinateurs à partir desquels les tentatives de chiffrement externe ne doivent pas être traitées.

   Exemples :

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données 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 **Protection avancée** → **Protection contre le chiffrement**.
3. Dans la partie supérieure de la fenêtre, cliquez sur le lien **Exclusions par nom ou par adresse IP**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
5. Saisissez les adresses IP, la plage d'adresses IP ou les noms des ordinateurs à partir desquels les tentatives de chiffrement externe ne doivent pas être traitées.

   Exemples :

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Protection contre le chiffrement**.
4. Cliquez sur le bouton **Par nom ou adresse IP** dans le groupe **Exclusions de l'analyse**.

5. 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. Appuyez 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.

6. Pour importer la liste des exclusions, procédez comme suit :

   a. Appuyez 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. Ouvrez le fichier.

      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.

Comment exporter et importer une liste d'exclusions dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**.

5. Cliquez sur le lien **Exclusions par nom ou par adresse IP**.

6. Pour exporter la liste des règles, procédez comme suit :

   a. Sélectionnez les exclusions que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des exclusions dans un fichier JSON dans le dossier des téléchargements par défaut.

7. Pour importer la liste des exclusions, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des exclusions.

   b. Ouvrez le fichier.

      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 JSON.

8. Enregistrez vos modifications.

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 l'analyse des logiciels malveillants.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Réparation des actions malicieuses**.
4. Utilisez la case **Réparation des actions malicieuses** pour activer ou désactiver le module.
5. 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 **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Réparation des actions malicieuses**.
5. Utilisez le commutateur **Réparation des actions malicieuses ACTIVÉE** 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **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.

La fonctionnalité KSN peut ne pas être disponible dans le logiciel aux États-Unis.

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 à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés. Pour en savoir plus sur la configuration de l'accès à KSN, consultez l'aide de Kaspersky Security Center.

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.

L'infrastructure des bases de données de réputation de Kaspersky

Kaspersky Endpoint Security prend en charge les solutions d'infrastructure suivantes pour utiliser les bases de données de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky 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.

- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

Activation et désactivation de l'utilisation de Kaspersky Security Network

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.

Comment activer ou désactiver l'utilisation de KSN dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Kaspersky Security Network**.
4. 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. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.
5. Le cas échéant, décochez la case **Activer le mode étendu de KSN**. Par défaut, le mode KSN étendu est activé.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver l'utilisation de KSN dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Kaspersky Security Network**.
5. Utilisez le commutateur **Utilisation de Kaspersky Security Network (KSN) ACTIVÉE** pour activer ou désactiver le module.

   Si vous avez activé l'utilisation de KSN, Kaspersky Endpoint Security affichera la déclaration de Kaspersky Security Network. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.
6. Si nécessaire, désactivez le commutateur **Utiliser le mode étendu de KSN**. Par défaut, le mode KSN étendu est activé.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver l'utilisation de KSN 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 **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. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.

4. Si nécessaire, désactivez le commutateur **Activer le mode étendu de KSN**. Par défaut, le mode KSN étendu est activé.

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.

Limitations de Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) 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. Kaspersky Private Security Network 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 *Douteuses* dans la base de données de réputation locale, mais a une réputation *De confiance* dans KSN/KPSN, Kaspersky Endpoint Security détectera le fichier comme *Douteuses* 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 à 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 .

- Kaspersky Endpoint Security en mode Light Agent communique avec les Serveurs KSN via un serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge.

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.

Si l'application fonctionne en mode Light Agent, le mode Cloud n'est pas disponible.

Comment activer ou désactiver le mode cloud pour les modules de protection dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Kaspersky Security Network**.
4. Utilisez la case **Activer le mode Cloud** pour activer ou désactiver le module.
5. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le mode cloud pour les modules de protection dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Kaspersky Security Network**.
5. Utilisez le commutateur **Utiliser le mode cloud** pour activer ou désactiver le module.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer ou désactiver le mode cloud pour les modules de protection 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 **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.

Paramètres du proxy KSN

Les ordinateurs des utilisateurs qui sont administrés par le Serveur d'administration de Kaspersky Security Center peuvent interagir avec KSN soit directement, soit via le service KSN Proxy.

> Si l'application s'exécute en mode Light Agent, la communication directe avec KSN n'est pas prise en charge. Kaspersky Endpoint Security communique avec les serveurs KSN via un serveur proxy KSN.

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.

Par défaut, une fois que KSN est activé et que la Déclaration KSN est acceptée, l'application utilise un serveur proxy pour se connecter à Kaspersky Security Network. Le serveur proxy utilisé par l'application est le Serveur d'administration de Kaspersky Security Center via le port TCP 13111. Par conséquent, si KSN Proxy n'est pas disponible, vous devez vérifier les points suivants :

- Le service `ksnproxy` est exécuté sur le Serveur d'administration.
- Le Pare-feu de l'ordinateur ne bloque pas le port 13111.

Vous pouvez configurer l'utilisation du KSN Proxy comme suit : activer ou désactiver le KSN Proxy, et configurer le port pour la connexion. Pour ce faire, vous devez ouvrir les propriétés du Serveur d'administration. Pour plus de détails sur la configuration de KSN Proxy, consultez l'aide de Kaspersky Security Center. Vous pouvez également activer ou désactiver le KSN Proxy pour des ordinateurs individuels dans la stratégie de Kaspersky Endpoint Security.

Comment activer ou désactiver le proxy KSN dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Protection avancée** → **Kaspersky Security Network**.
4. Dans le groupe **Paramètres de KSN Proxy**, utilisez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver KSN Proxy.
5. Le cas échéant, cochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Si la case est cochée, Kaspersky Endpoint Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).
6. Enregistrez vos modifications.

Comment activer ou désactiver le proxy KSN dans Web Console ?

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Kaspersky Security Network**.
5. Utilisez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver KSN Proxy.
6. Le cas échéant, cochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Si la case est cochée, Kaspersky Endpoint Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé). Par défaut, la case est décochée.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

L'adresse du KSN Proxy correspond à l'adresse du Serveur d'administration. Lorsque le nom de domaine du Serveur d'administration est modifié, vous devez mettre à jour manuellement l'adresse du KSN Proxy.

Pour configurer l'adresse du proxy KSN, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.
3. Dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez **Propriétés**.

4. Dans l'onglet **Général** de la fenêtre qui s'ouvre, indiquez la nouvelle adresse du serveur proxy KSN.

5. Enregistrez vos modifications.

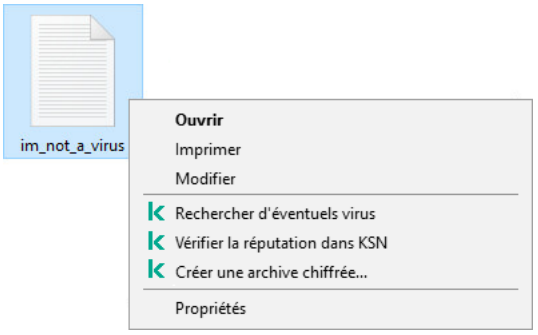
Vérification de la réputation d'un fichier dans Kaspersky Security Network

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 **Vérifier la réputation dans KSN** (cf. ill. ci-dessous).



Menu contextuel du fichier

Kaspersky Endpoint Security affiche la réputation du fichier :

De confiance (Kaspersky Security Network). L'application considère qu'un fichier est fiable si au moins une des conditions suivantes est remplie :

- le fichier porte la signature numérique d'un fournisseur de confiance ;
- le fichier a une réputation de confiance auprès de Kaspersky Security Network ;
- l'utilisateur a placé le fichier dans le groupe De confiance.

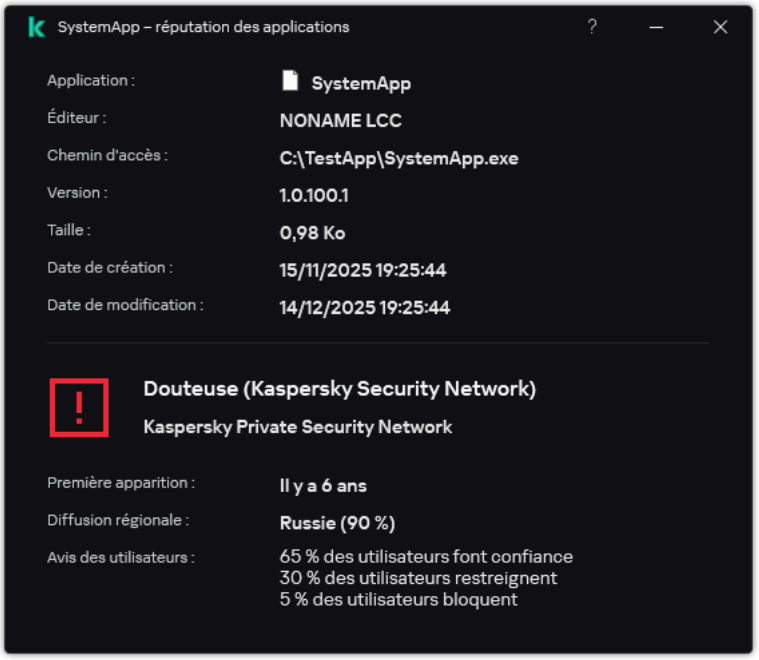
Programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être exploitées par des individus malintentionnés. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données personnelles 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.

Douteuse (Kaspersky Security Network). Un virus ou un autre programme présentant une menace.

Inconnue (Kaspersky Security Network). 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 : *Kaspersky Security Network* ou *Kaspersky Private Security Network*.

Kaspersky Endpoint Security affiche également des informations supplémentaires sur le fichier (cf. ill. ci-dessous).



Réputation d'un fichier dans Kaspersky Security Network

Analyse des connexions chiffrées

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 utilise ce certificat pour analyser les connexions chiffrées. 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, Protection contre les menaces Internet, Détection comportementale et Protection contre les Exploits 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.

Activation de l'analyse des connexions chiffrées

Par défaut, Kaspersky Endpoint Security n'analyse pas toujours les connexions chiffrées, mais uniquement à la demande des modules de protection.

Comment activer l'analyse des connexions chiffrées dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
5. Dans le groupe **Analyse des connexions chiffrées**, sélectionnez le mode d'analyse des connexions chiffrées :
   - **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 menaces Internet, 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.

6. Si nécessaire, ajoutez des exclusions à l'analyse : adresses et applications de confiance.
7. Configurez les paramètres d'analyse des connexions chiffrées (cf. tableau ci-après).
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'analyse des connexions chiffrées dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Sous **Analyse des connexions chiffrées**, désactivez le commutateur **Analyse des connexions chiffrées ACTIVÉE**.

   Si le commutateur est désactivé, Kaspersky Endpoint Security n'aura pas accès au contenu des sites Internet dont l'adresse commence par `https://`.

6. Cliquez sur **Paramètres** et sélectionnez le mode d'analyse des connexions chiffrées :

- **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 menaces Internet, 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.

7. Si nécessaire, ajoutez des exclusions à l'analyse : adresses et applications de confiance.

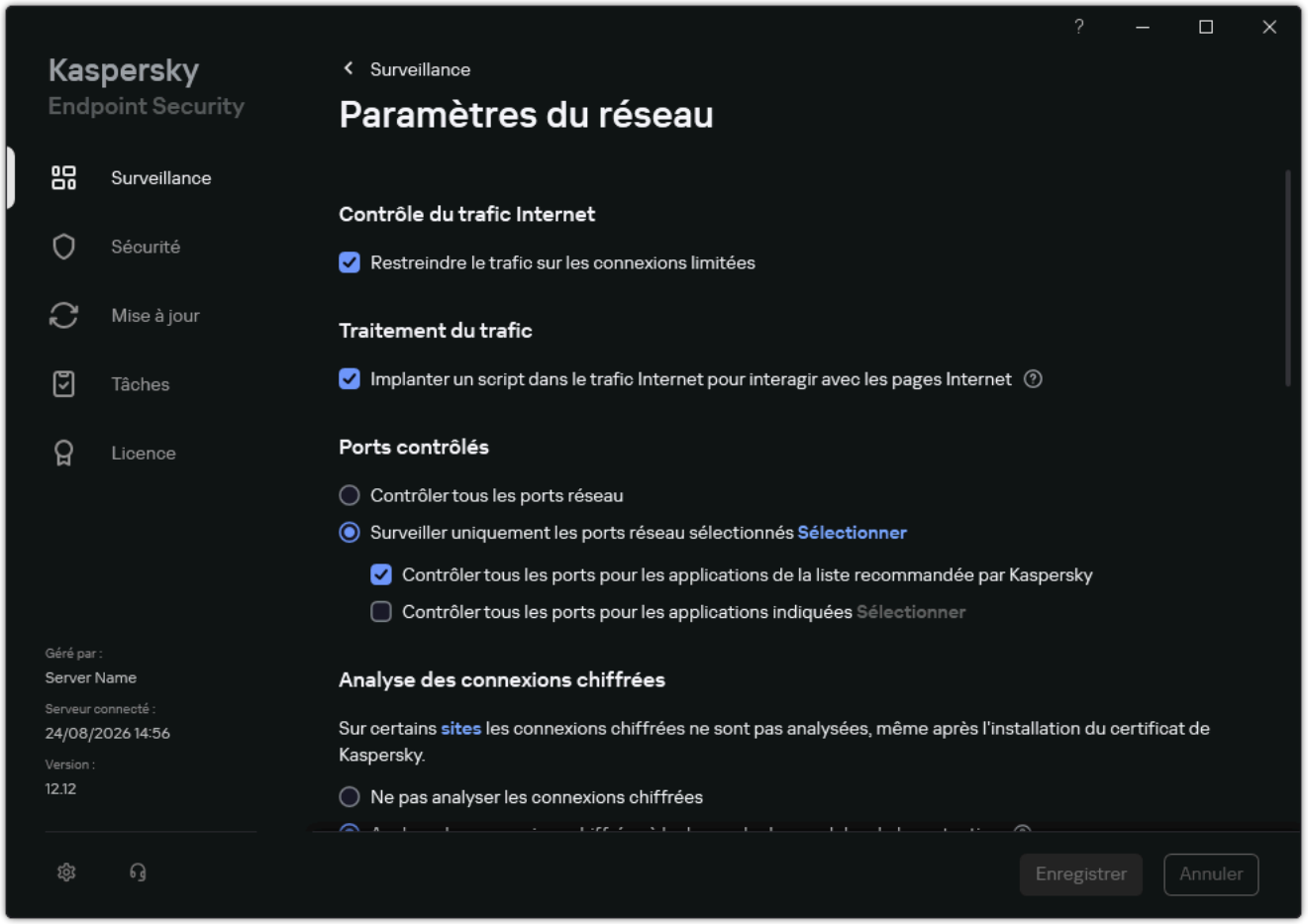
8. Configurez les paramètres d'analyse des connexions chiffrées (cf. tableau ci-après).

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'analyse des connexions chiffrées 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** → **Paramètres du réseau**.



Paramètres d'analyse des connexions chiffrées

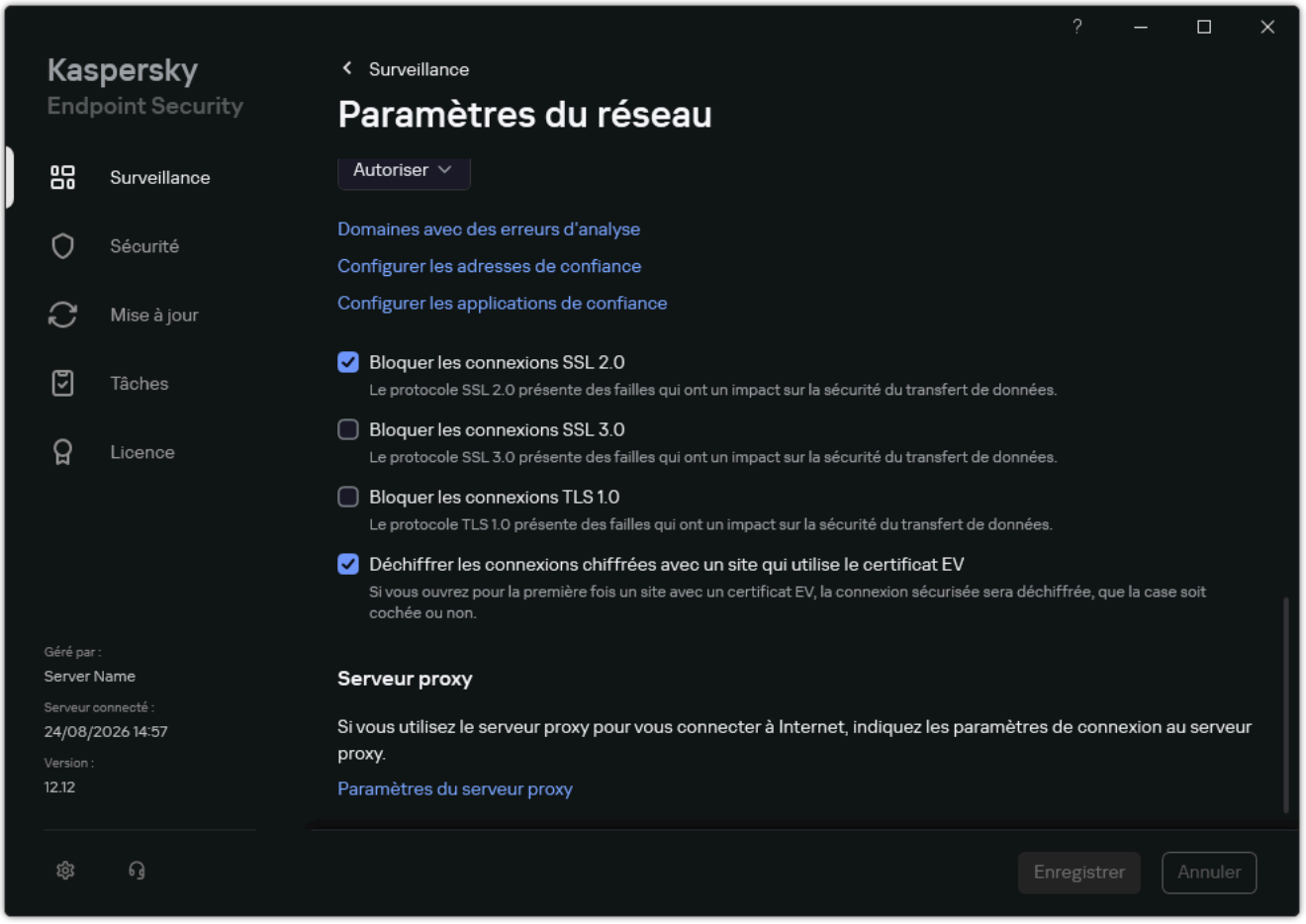
3. Dans le groupe **Analyse des connexions chiffrées**, sélectionnez le mode d'analyse des connexions chiffrées :

- **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 menaces Internet, 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. Configurez les paramètres d'analyse des connexions chiffrées (cf. tableau ci-après).



Paramètres supplémentaires relatifs à l'analyse des connexions chiffrées

6. Enregistrez vos modifications.

Paramètres d'analyse des connexions chiffrées

Paramètre	Description
Certificats racine de confiance	Liste des certificats racine de confiance. Kaspersky Endpoint Security vous permet d'installer des certificats racine de confiance sur les ordinateurs des utilisateurs si, par exemple, vous devez déployer un nouveau centre de certification. L'application vous permet d'ajouter un certificat à une liste de certificats spéciale de Kaspersky Endpoint Security. Dans ce cas, le certificat est considéré comme étant fiable uniquement pour l'application Kaspersky Endpoint Security. Autrement dit, l'utilisateur peut accéder à un site Internet avec le nouveau certificat dans le navigateur. Si une autre application tente d'accéder au site Internet, vous pouvez obtenir une erreur de connexion en raison d'un problème de certificat. Pour ajouter des éléments à la liste de certificats du système, vous pouvez utiliser les stratégies de groupe Active Directory.
Accès à un domaine doté d'un certificat douteux	• **Autoriser**. Kaspersky Endpoint Security autorise l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. 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. Si une application ou un service tiers établit une connexion avec un domaine présentant un certificat douteux, Kaspersky Endpoint Security crée son propre certificat pour analyser le trafic. Le nouveau certificat porte l'état *Douteuse*. Cette mesure est nécessaire pour avertir l'application tierce de la connexion douteuse, car la page HTML ne peut pas être affichée dans ce cas, et la connexion peut être établie en arrière-plan. • **Bloquer**. Kaspersky Endpoint Security bloque l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. 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.
Accès à un domaine présentant une erreur d'analyse des connexions chiffrées	• **Bloquer**. Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée. • **Autoriser et ajouter le domaine aux exclusions**. 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**. Kaspersky Endpoint Security génère également un événement pour signaler l'erreur d'analyse de la connexion chiffrée.
Bloquer les connexions SSL 2.0	Si cette case est cochée, l'application surveille et bloque les connexions réseau établies via le protocole SSL 2.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole SSL 2.0. Cependant, l'application ne contrôle pas le trafic réseau via ce protocole.
Bloquer les connexions SSL 3.0	Si cette case est cochée, l'application bloque les connexions réseau établies via le protocole SSL 3.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole SSL 3.0. L'application surveille le trafic réseau via ce protocole. Tous les modules de l'application fonctionnent sans restrictions.
Bloquer les connexions TLS 1.0	Si cette case est cochée, l'application bloque les connexions réseau établies via le protocole TLS 1.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole TLS 1.0. L'application surveille le trafic réseau via ce protocole. Tous les modules de l'application fonctionnent sans restrictions.
Déchiffrer les connexions chiffrées avec un site qui utilise le certificat EV	Les certificats EV (Extended Validation Certificate) 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. Si cette case est cochée, l'application déchiffre et surveille les connexions chiffrées avec les sites qui utilisent un certificat EV. Si la case est décochée, l'application 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, `https://bing.com`. 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.

Installation de certificats racine de confiance

Kaspersky Endpoint Security vous permet d'installer des certificats racine de confiance sur les ordinateurs des utilisateurs si, par exemple, vous devez déployer un nouveau centre de certification. L'application vous permet d'ajouter un certificat à une liste de certificats spéciale de Kaspersky Endpoint Security. Dans ce cas, le certificat est considéré comme étant fiable uniquement pour l'application Kaspersky Endpoint Security. Autrement dit, l'utilisateur peut accéder à un site Internet avec le nouveau certificat dans le navigateur. Si une autre application tente d'accéder au site Internet, vous pouvez obtenir une erreur de connexion en raison d'un problème de certificat. Pour ajouter des éléments à la liste de certificats du système, vous pouvez utiliser les stratégies de groupe Active Directory.

Comment installer des certificats racine de confiance dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
4. Cliquez sur le bouton **Ajouter** dans le groupe **Certificats racine de confiance**.
5. Une fenêtre s'ouvre. Dans cette fenêtre, sélectionnez un certificat racine de confiance.
   Kaspersky Endpoint Security prend en charge les certificats avec les extensions PEM, DER et CRT.
6. Enregistrez vos modifications.

Comment installer des certificats racine de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Cliquez sur le lien **Certificats racine de confiance**.
6. Une fenêtre s'ouvre. Dans cette fenêtre, cliquez sur **Ajouter** et sélectionnez un certificat racine de confiance.
   Kaspersky Endpoint Security prend en charge les certificats avec les extensions PEM, DER et CRT.
7. Enregistrez vos modifications.

Comment installer des certificats racine de confiance 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** → **Paramètres du réseau**.
3. Cliquez sur le bouton **Afficher les certificats** dans le groupe **Analyse des connexions chiffrées**.
4. Une fenêtre s'ouvre. Dans cette fenêtre, cliquez sur **Ajouter** et sélectionnez un certificat racine de confiance.
   Kaspersky Endpoint Security prend en charge les certificats avec les extensions PEM, DER et CRT.
5. Enregistrez vos modifications.

Par conséquent, lors de l'analyse du trafic, en plus de la liste de certificats du système, Kaspersky Endpoint Security utilise sa propre liste de certificats.

Analyse des connexions chiffrées utilisant un certificat douteux

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 utilise ce certificat pour analyser les connexions chiffrées. Lorsque vous visitez un domaine présentant un certificat douteux, vous pouvez autoriser ou refuser l'accès des utilisateurs à ce domaine (cf. instructions ci-dessous).

Si vous avez autorisé l'utilisateur à visiter des domaines présentant des certificats douteux, Kaspersky Endpoint Security effectue les actions suivantes :

- Lorsque vous visitez un domaine présentant un certificat douteux dans le *navigateur*, Kaspersky Endpoint Security utilise le certificat Kaspersky pour analyser le trafic. Kaspersky Endpoint Security affiche une page HTML avec un avertissement et des informations sur la raison pour laquelle il n'est pas recommandé de visiter le domaine concerné (cf. ill. ci-dessous). 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. Kaspersky Endpoint Security génère également un événement concernant l'établissement d'une connexion chiffrée avec un certificat douteux.

  Dans certains cas, Kaspersky Endpoint Security ne peut techniquement pas afficher une page HTML avec un avertissement dans le navigateur (cf. ill. ci-dessous). Par exemple, si une ressource Internet utilise une version obsolète d'un protocole réseau et un port non standard. Dans ces cas, Kaspersky Endpoint Security bloque l'accès à ce domaine, et le navigateur affiche la fenêtre standard `ERR_CONNECTION_RESET`. Pour accéder à une ressource Internet, vous pouvez ajouter un domaine aux exclusions ou utiliser un certificat de confiance.

- Si *une application ou un service tiers* établit une connexion avec un domaine présentant un certificat douteux, Kaspersky Endpoint Security crée son propre certificat pour analyser le trafic. Le nouveau certificat porte l'état *Douteux*. Cette mesure est nécessaire pour avertir l'application tierce de la connexion douteuse, car la page HTML ne peut pas être affichée dans ce cas, et la connexion peut être établie en arrière-plan. Par conséquent, si une application tierce dispose d'outils de vérification des certificats intégrés, la connexion peut être interrompue. Dans ce cas, vous devez contacter le propriétaire du domaine et établir une connexion de confiance. Si la configuration d'une connexion de confiance est impossible, vous pouvez ajouter cette application tierce à la liste des applications de confiance. Kaspersky Endpoint Security génère également un événement concernant l'établissement d'une connexion chiffrée avec un certificat douteux.

Comment configurer l'analyse des connexions chiffrées présentant un certificat douteux dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
4. Cliquez sur le bouton **Paramètres avancés** dans le groupe **Analyse des connexions chiffrées**.
5. Dans le groupe qui s'ouvre, sélectionnez le mode de fonctionnement de l'application lors de la visite d'un domaine avec un certificat non approuvé : **Autoriser** ou **Bloquer**.
6. Enregistrez vos modifications.

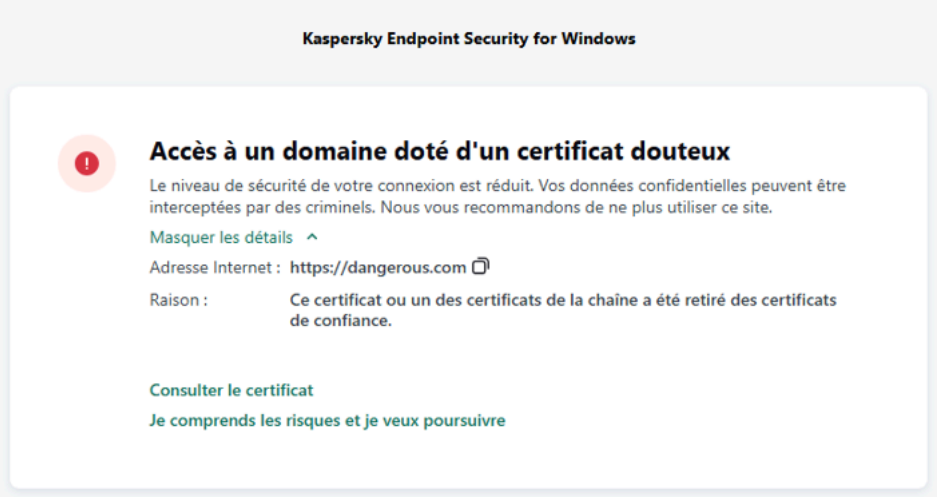
Comment configurer l'analyse des connexions chiffrées présentant un certificat douteux dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Dans le groupe **Analyse des connexions chiffrées**, cliquez sur le lien **Paramètres**.
6. Dans le groupe qui s'ouvre, sélectionnez le mode de fonctionnement de l'application lors de la visite d'un domaine avec un certificat non approuvé : **Autoriser la connexion** ou **Bloquer la connexion**.
7. Enregistrez vos modifications.

Comment configurer l'analyse des connexions chiffrées présentant un certificat douteux 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** → **Paramètres du réseau**.
3. Dans le groupe **Analyse des connexions chiffrées**, sélectionnez le mode de fonctionnement de l'application lors de la visite d'un domaine avec un certificat non approuvé : **Autoriser** ou **Bloquer**.
4. Enregistrez vos modifications.



Avertissement concernant l'accès à un domaine avec un certificat douteux

Ajout d'un certificat de Kaspersky dans la propre liste de certificats

Les navigateurs et les clients de messagerie utilisent le certificat pour vérifier la sécurité et l'authenticité des ressources Internet. Le certificat assure également le chiffrement des données entre les ressources Internet et l'utilisateur. La plupart des navigateurs et des clients de messagerie utilisent la liste de certificats de confiance (liste de certificats Windows). Par exemple, Google Chrome. Certains navigateurs et clients de messagerie utilisent par défaut leur propre liste de certificats au lieu de la liste de certificats Windows. Par exemple, 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). 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 les navigateurs et les clients de messagerie pour analyser le trafic de ces applications. Si aucune stratégie n'est appliquée à l'ordinateur, vous pouvez choisir la liste de certificats qui sera utilisée par les navigateurs et les clients de messagerie. Si vous avez sélectionné la propre liste de certificats, ajoutez manuellement le certificat Kaspersky à la liste. 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, l'application n'analyse pas le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird. L'analyse des connexions chiffrées doit également être activée pour analyser le trafic dans les clients de messagerie MyOffice Mail et R7-Office Organizer.

Avant d'ajouter un certificat au magasin de certificats du navigateur ou de l'agent de messagerie, exportez le certificat Kaspersky depuis le Panneau de configuration Windows (propriétés Internet). Pour en savoir plus sur l'ajout d'un certificat dans la liste, vous pouvez par exemple consulter 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 les navigateurs et les clients de messagerie, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
3. Dans le groupe **Analyse des connexions chiffrées**, cochez la case **Pour analyser les connexions chiffrées dans les applications disposant de leur propre liste de certificats, utilisez**.

4. Sélectionnez une liste de certificats :

   - **Liste de certificats Windows (recommandé)**. Le certificat racine de Kaspersky est ajouté à cette boutique lors de l'installation de Kaspersky Endpoint Security.

   - **Propre liste de certificats**. 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.

     Les clients de messagerie MyOffice Mail et R7-Office Organizer utilisent également leur propre liste de certificats.

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 exclusions en tant qu'*adresse de confiance*. Dans ce cas, Kaspersky Endpoint Security n'analyse pas le trafic HTTPS des URL de confiance lorsque les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet fonctionnent.

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.

Comment exclure une adresse Internet des analyses de connexion chiffrées dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.

5. Cliquez sur le bouton **Configurer les adresses de confiance** dans le groupe **Analyse des connexions chiffrées**.

6. Cliquez sur **Ajouter**.

7. 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 `*` pour saisir un masque dans le nom de domaine.

   > Kaspersky Endpoint Security ne prend pas en charge le symbole `*` pour les adresses IP. Vous pouvez sélectionner une plage d'adresses IP à l'aide d'un masque de sous-réseau (par exemple, 198.51.100.0/24).

Exemples :

- `domain.com` : l'enregistrement comprend les adresses suivantes : `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. L'enregistrement ne comprend pas les sous-domaines (par exemple, `subdomain.domain.com`).
- `subdomain.domain.com` : l'enregistrement comprend les adresses suivantes : `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.
- `*.domain.com` : l'enregistrement comprend les adresses suivantes : `https://movies.domain.com`, `https://images.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exclure une adresse Internet des analyses des connexions chiffrées dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres du réseau**.
5. Cliquez sur le bouton **Domaines de confiance** dans le groupe **Analyse des connexions chiffrées**.
6. Cliquez sur **Ajouter**.
7. 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 `*` pour saisir un masque dans le nom de domaine.

   > Kaspersky Endpoint Security ne prend pas en charge le symbole `*` pour les adresses IP. Vous pouvez sélectionner une plage d'adresses IP à l'aide d'un masque de sous-réseau (par exemple, 198.51.100.0/24).

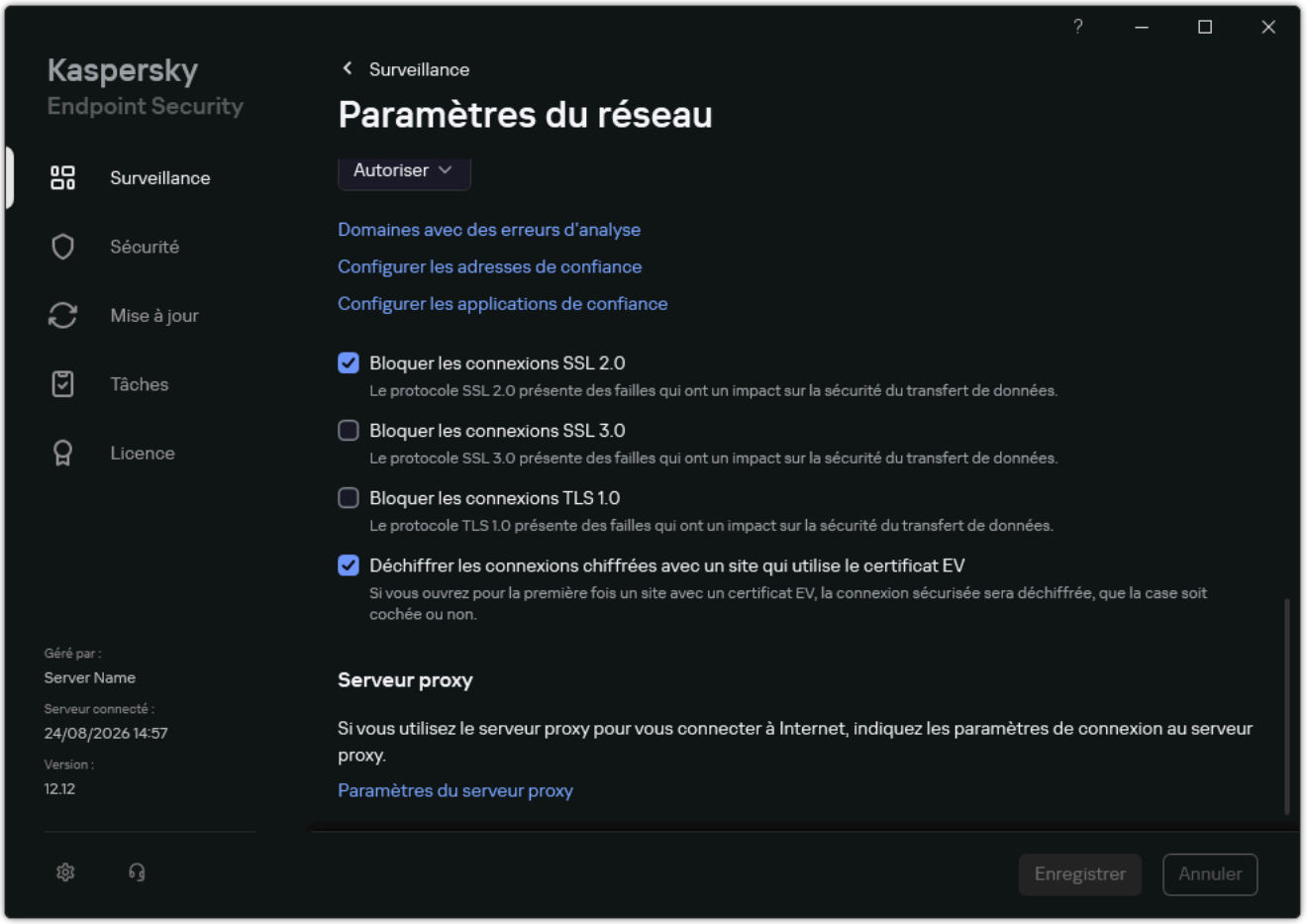
   Exemples :

   - `domain.com` : l'enregistrement comprend les adresses suivantes : `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. L'enregistrement ne comprend pas les sous-domaines (par exemple, `subdomain.domain.com`).
   - `subdomain.domain.com` : l'enregistrement comprend les adresses suivantes : `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.
   - `*.domain.com` : l'enregistrement comprend les adresses suivantes : `https://movies.domain.com`, `https://images.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exclure une adresse Internet des analyses de connexion chiffrées 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** → **Paramètres du réseau**.



Paramètres réseau des applications

3. Cliquez sur le bouton **Configurer les adresses de confiance** dans le groupe **Analyse des connexions chiffrées**.

4. Cliquez sur **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 `*` pour saisir un masque dans le nom de domaine.

   > Kaspersky Endpoint Security ne prend pas en charge le symbole `*` pour les adresses IP. Vous pouvez sélectionner une plage d'adresses IP à l'aide d'un masque de sous-réseau (par exemple, 198.51.100.0/24).

Exemples :

- `domain.com` : l'enregistrement comprend les adresses suivantes : `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. L'enregistrement ne comprend pas les sous-domaines (par exemple, `subdomain.domain.com`).

- `subdomain.domain.com` : l'enregistrement comprend les adresses suivantes : `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.

- `*.domain.com` : l'enregistrement comprend les adresses suivantes : `https://movies.domain.com`, `https://images.domain.com/page123`. L'enregistrement ne comprend pas 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.

Pour afficher une liste de domaines avec des erreurs d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.

3. Cliquez sur le bouton **Domaines avec des erreurs d'analyse** dans le groupe **Analyse des connexions chiffrées**.

   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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **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.

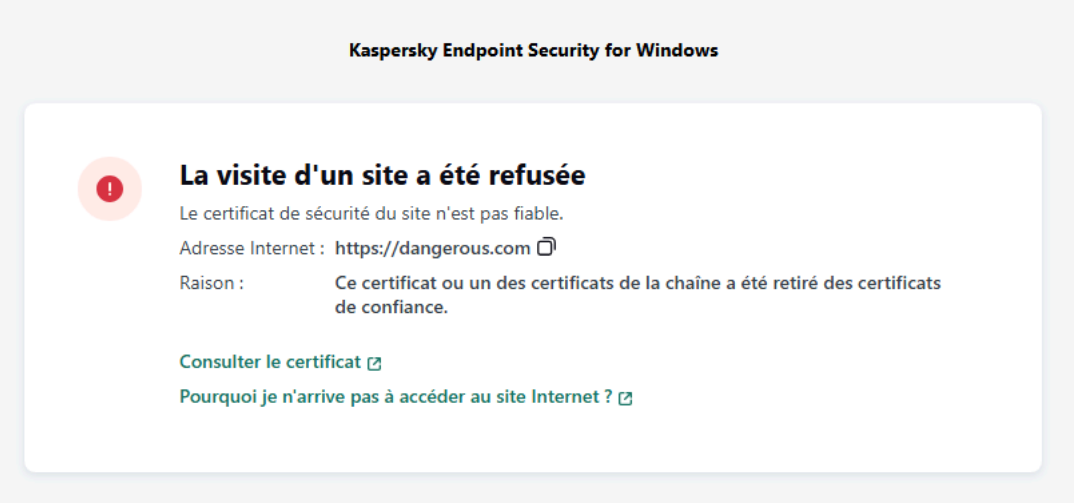
Blocage de l'accès aux domaines dotés de certificats non fiables

Dans certains cas, lors du blocage de l'accès à un domaine doté d'un certificat non fiable, Kaspersky Endpoint Security affiche dans le navigateur une page d'avertissement HTML qui ne contient pas de lien vers la ressource Internet demandée.

Cela peut se produire pour les raisons suivantes :

- L'administrateur a bloqué l'accès à un domaine doté d'un certificat non fiable.
- Le domaine possède un certificat non fiable ou non valide, et le serveur Web utilise le mécanisme HTTP Strict Transport Security (HSTS). *HSTS* est un mécanisme de sécurité qui impose l'utilisation du protocole sécurisé HTTPS pour les communications entre un client et un serveur Web. Dans ce cas, vous ne pouvez pas accéder au domaine, même si vous l'avez ajouté à la liste des adresses de confiance. Le mécanisme HSTS est décrit dans la RFC 6797.

  Dans certains cas, le site peut être ouvert directement dans un navigateur sans utiliser Kaspersky Endpoint Security. Les navigateurs ne détectent pas toujours les certificats révoqués, tandis que Kaspersky Endpoint Security vérifie en ligne la révocation des certificats lors de l'établissement d'une connexion. L'application peut ainsi détecter un problème de certificat avant le navigateur et afficher le message d'erreur correspondant.



Avertissement concernant l'accès à un domaine avec un certificat douteux

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 :

- Seul un administrateur de Kaspersky Security Center peut gérer la tâche *Suppression des données*. 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   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 **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

> 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.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la tâche **Suppression des données** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

7. Sélectionnez 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 X 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, gardez à l'esprit que les employés peuvent avoir des horaires de travail différents. Pensez également à l'horaire de travail des utilisateurs itinérants. Pour en savoir plus sur les ordinateurs déconnectés et les utilisateurs autonomes, consultez l'aide de Kaspersky Security Center.

   > Si l'ordinateur est éteint et que la connexion a été interrompue pendant une durée supérieure à celle configurée, après la mise sous tension de l'ordinateur, Kaspersky Endpoint Security ne supprime pas immédiatement les données. L'application attend la synchronisation avec Kaspersky Security Center pendant une heure. Cette mesure est nécessaire pour empêcher la suppression non autorisée de données sur les ordinateurs des utilisateurs qui ont éteint leur ordinateur, par exemple, avant de partir en vacances.

   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 "`,`".

    - **Zone prédéfinie**. 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. Enregistrez vos modifications.

12. Cochez la case en regard de la tâche.

13. Cliquez sur **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.

Contrôle de l'ordinateur

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).

Pour utiliser le Contrôle Internet, vous devez procéder à la configuration initiale de l'application :

- Pour contrôler le trafic HTTPS, activez l'analyse des connexions sécurisées (activé par défaut).
- Sélectionnez les ports que Kaspersky Endpoint Security doit surveiller (par défaut, l'application surveille tous les ports).
- Sélectionnez les applications dont vous souhaitez que Kaspersky Endpoint Security contrôle le trafic. La plupart des navigateurs sont déjà présents dans la liste des applications recommandées par Kaspersky. Si votre navigateur ne figure pas dans la liste, ajoutez-le manuellement.
- Nous vous recommandons d'injecter un script d'interaction avec les pages Internet dans le trafic Internet (par défaut, l'injection de script est désactivée). 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.

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 graphiques*.

- **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 des suites bureautiques* uniquement pour la catégorie de sites *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.

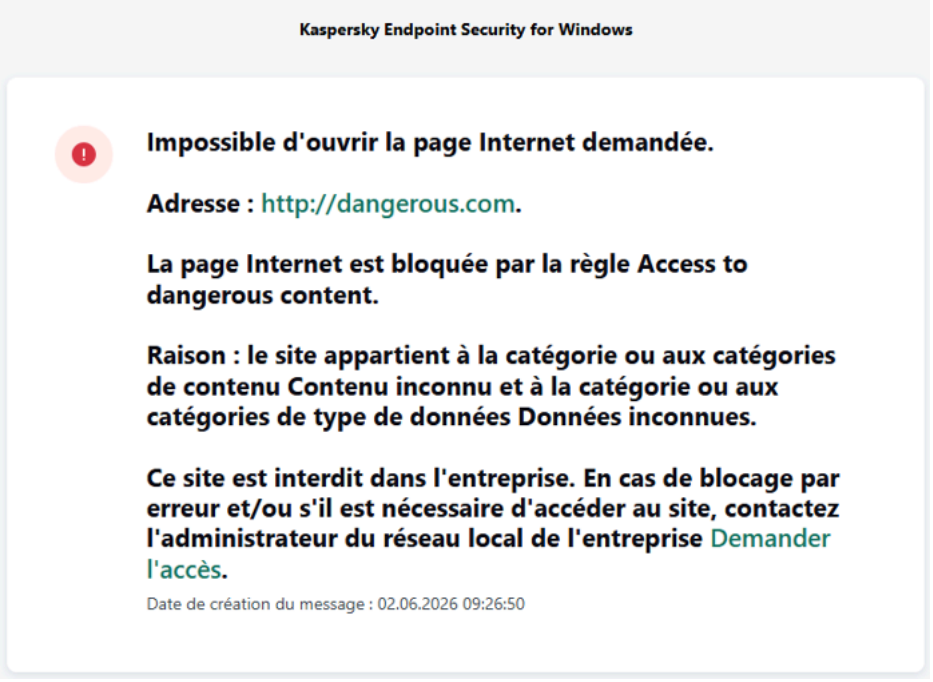
  Par exemple, vous pouvez limiter l'accès à Internet via un navigateur pour tous les utilisateurs de l'entreprise, à l'exception du service informatique.

- 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 *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.



Notifications du Contrôle Internet

Ajout d'une règle d'accès aux ressources Internet

Une *règle d'accès aux ressources Internet* est un ensemble de filtres et d'actions que Kaspersky Endpoint Security applique lorsque les utilisateurs visitent des ressources Internet. Les règles d'accès peuvent inclure une planification de règles.

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. La *Règle par défaut* est prédéfinie. 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.

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 *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.

Comment ajouter une règle d'accès aux ressources Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.

4. Cochez la case **Contrôle Internet**.

5. Cliquez sur le bouton **Ajouter** dans le groupe **Paramètres du Contrôle Internet**.

   La fenêtre **Règle d'accès aux sites** s'ouvre.

6. Configurez la règle d'accès aux ressources Internet (voir le tableau ci-dessous).

7. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

   > Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

   Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

8. Enregistrez vos modifications.

Comment ajouter une règle d'accès aux ressources Internet dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.

5. Activez le commutateur **Contrôle Internet ACTIVÉ**.

6. Cliquez sur le bouton **Ajouter** dans le groupe **Liste des règles**.

7. Configurez la règle d'accès aux ressources Internet (voir le tableau ci-dessous).

8. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

   Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

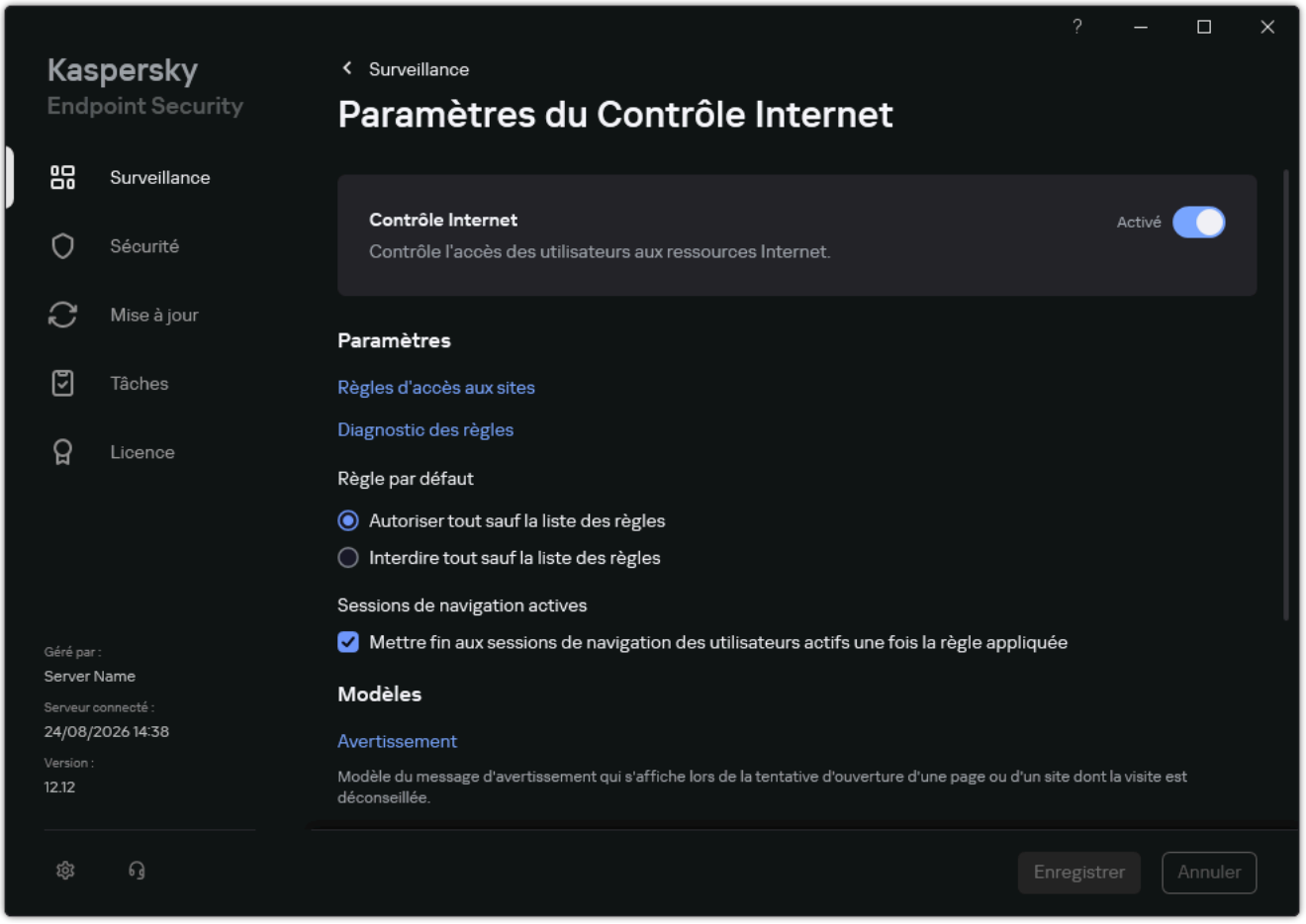
   Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

9. Enregistrez vos modifications.

Comment ajouter une règle d'accès aux ressources Internet 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 **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Activez le commutateur **Contrôle Internet**.

4. Cliquez sur le bouton **Règles d'accès aux sites** dans le groupe **Paramètres**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle d'accès aux sites** s'ouvre.

6. Configurez la règle d'accès aux ressources Internet (voir le tableau ci-dessous).

7. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

   > Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

   Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

8. Enregistrez vos modifications.

En conséquence, la nouvelle règle du Contrôle Internet est ajoutée à la liste. Si nécessaire, modifiez la priorité de la règle du Contrôle Internet. Vous pouvez également utiliser le commutateur pour désactiver la règle d'accès aux ressources Internet à tout moment sans la supprimer de la liste.

Paramètres de la règle du Contrôle Internet

Paramètre	Description
Nom de la règle	Nom de la règle du Contrôle Internet.
Condition	• **Activé**. • **Désactivé**. Vous pouvez utiliser le commutateur pour désactiver la règle d'accès aux ressources Internet à tout moment.
Action	• **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle. • **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet. • **Avertir**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.
Contenu du filtre	• **Par catégories**. 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 *Fichiers graphiques*).
Adresses	• **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. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Si l'Analyse des connexions chiffrées est désactivée, seul le filtrage selon le nom du serveur est accessible pour le protocole HTTPS.
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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.
Planification de 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. Par exemple, vous pouvez limiter l'accès à Internet via un navigateur uniquement pendant les heures ouvrables.

Filtrage selon les adresses des ressources Internet

Pour contrôler l'accès à des ressources Internet individuelles, vous devez créer une règle de Contrôle Internet, créer une liste d'adresses Internet et sélectionner une action du Contrôle Internet. Lors de la création d'une liste d'adresses Internet, vous pouvez saisir des adresses URL ou utiliser des masques.

Les règles peuvent inclure une planification de règles et une liste d'utilisateurs auxquels la règle s'applique. Par exemple, vous pouvez restreindre l'accès aux sites Internet pendant les heures de travail uniquement, ou autoriser la visite de sites Internet à des utilisateurs appartenant à certains groupes.

Comment activer un filtre d'adresses Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.

4. Cochez la case **Contrôle Internet**.

5. Cliquez sur le bouton **Ajouter** dans le groupe **Paramètres du Contrôle Internet**.

   La fenêtre **Règle d'accès aux sites** s'ouvre.

6. Configurez la règle d'accès aux ressources Internet :

   a. Dans le champ **Nom**, saisissez le nom de la règle.

   b. Dans la liste déroulante **Appliquer aux adresses**, choisissez **À certaines adresses**.

   c. Composez 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.

   > Si l'Analyse des connexions chiffrées est désactivée, seul le filtrage selon le nom du serveur est accessible pour le protocole HTTPS.

   d. Dans la liste déroulante **Appliquer aux utilisateurs**, sélectionnez le filtre approprié pour les utilisateurs :

   - **À tous les utilisateurs**. Le Contrôle Internet ne filtrera pas les ressources Internet par adresse.
   - **À certains utilisateurs ou groupes**. Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   e. Dans la liste déroulante **Action**, sélectionnez une option :

   - **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.
   - **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.
   - **Avertir**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

   f. Dans la liste déroulante **Calendrier des règles**, sélectionnez une planification ou créez-en une autre.

7. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

   > Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

8. Enregistrez vos modifications.

Comment activer un filtre d'adresses de ressources Internet dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.
5. Activez le commutateur **Contrôle Internet ACTIVÉ**.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Liste des règles**.
7. Configurez la règle d'accès aux ressources Internet :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Sélectionnez l'état **Activé** 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 sans la supprimer de la liste.

   c. Dans le groupe **Action**, sélectionnez l'option requise :

   - **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.
   - **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.
   - **Informer**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

   d. Sous **Zone**, sélectionnez **Sites Internet individuels**.

   e. Configurez le filtre de contenu :

   - **Adresse personnelle**. Composez 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.

     Si l'Analyse des connexions chiffrées est désactivée, seul le filtrage selon le nom du serveur est accessible pour le protocole HTTPS.

   - **Type 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 *Fichiers graphiques*).

f. Sous **Utilisateur ou groupe**, sélectionnez les utilisateurs auxquels vous souhaitez que le Contrôle Internet applique la règle.

Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

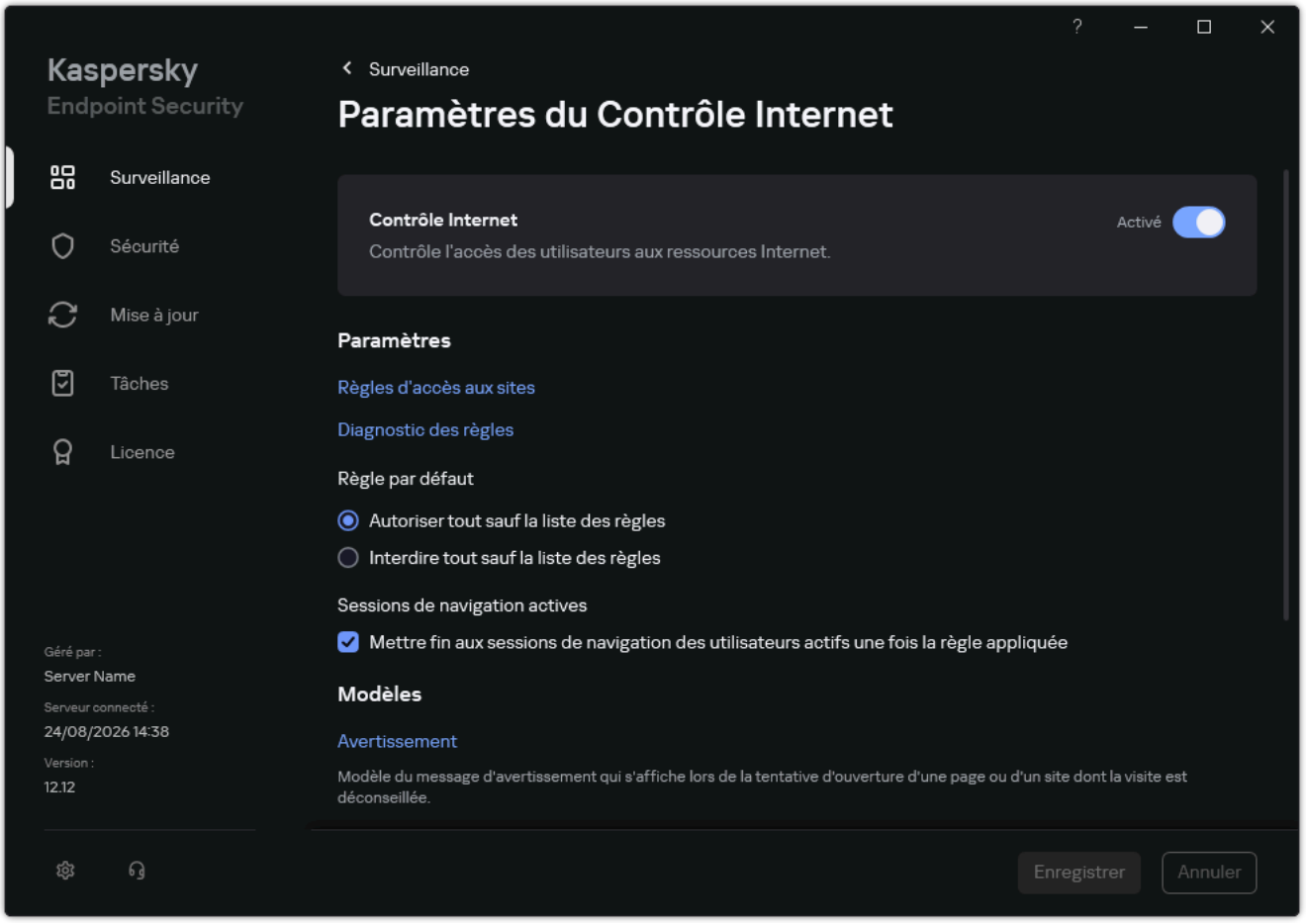
g. Dans le groupe **Planification de l'accès**, sélectionnez une planification ou créez-en une autre.

8. Enregistrez vos modifications.

Comment activer un filtre d'adresses Internet 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 **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Cliquez sur le bouton **Règles d'accès aux sites** dans le groupe **Paramètres**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

La fenêtre **Règle d'accès aux sites** s'ouvre.

5. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

6. Sélectionnez l'état **Activé** 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 requise :

   - **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.

   - **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.

   - **Avertir**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

8. Sous **Adresses**, sélectionnez **À certaines adresses**.

   Composez 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.

   > Si l'Analyse des connexions chiffrées est désactivée, seul le filtrage selon le nom du serveur est accessible pour le protocole HTTPS.

9. 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 filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

10. Dans la liste déroulante **Planification de l'application de la règle**, sélectionnez une planification ou créez-en une autre.

11. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

    > Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

    Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

12. Enregistrez vos modifications.

En conséquence, la nouvelle règle du Contrôle Internet est ajoutée à la liste. Si nécessaire, modifiez la priorité de la règle du Contrôle Internet. Vous pouvez également utiliser le commutateur pour désactiver la règle d'accès aux ressources Internet à tout moment sans la supprimer de la liste.

Filtrage selon le contenu des ressources Internet

Pour contrôler l'accès en fonction du contenu des ressources Internet, le Contrôle Internet propose un filtre de catégorie et un filtre de type de données.

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.

Vous pouvez restreindre l'accès des utilisateurs à un site Internet en fonction du type de données, par exemple pour masquer les images. Kaspersky Endpoint Security détermine le type de données selon le format du fichier et non pas selon son extension. Le Contrôle Internet distingue les types de données suivants :

- Vidéo
- Son
- Fichiers des suites bureautiques
- Fichiers exécutables
- Archives
- Fichiers graphiques
- Scripts

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 graphiques*.

Les règles peuvent inclure une planification de règles et une liste d'utilisateurs auxquels la règle s'applique. Par exemple, vous pouvez restreindre l'accès aux sites Internet pendant les heures de travail uniquement, ou autoriser la visite de sites Internet à des utilisateurs appartenant à certains groupes.

Comment activer un filtre de contenu de ressources Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.
4. Cochez la case **Contrôle Internet**.
5. Cliquez sur le bouton **Ajouter** dans le groupe **Paramètres du Contrôle Internet**.

   La fenêtre **Règle d'accès aux sites** s'ouvre.

6. Configurez la règle d'accès aux ressources Internet :

   a. Dans le champ **Nom**, saisissez le nom de la règle.

   b. Dans la liste déroulante **Filtrer le contenu**, sélectionnez le filtre de contenu approprié :

   - **Par catégories**. 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 *Fichiers graphiques*).
   - **Par catégories et types de données**. Les filtres par catégories de contenu et types de données sont activés.

   Une fois que vous avez sélectionné les filtres, configurez les paramètres des filtres.

   c. Dans la liste déroulante **Appliquer aux utilisateurs**, sélectionnez le filtre approprié pour les utilisateurs :

   - **À tous les utilisateurs**. Le Contrôle Internet ne filtrera pas les ressources Internet par adresse.
   - **À certains utilisateurs ou groupes**. Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Dans la liste déroulante **Action**, sélectionnez une option :

   - **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.
   - **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.
   - **Avertir**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

   e. Dans la liste déroulante **Calendrier des règles**, sélectionnez une planification ou créez-en une autre.

7. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

   Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

8. Enregistrez vos modifications.

Comment activer un filtre de contenu de ressources Internet dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.
5. Activez le commutateur **Contrôle Internet ACTIVÉ**.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Liste des règles**.
7. Configurez la règle d'accès aux ressources Internet :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Sélectionnez l'état **Activé** 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.

   c. Dans le groupe **Action**, sélectionnez l'option requise :

   - **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.
   - **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.
   - **Informer**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

   d. Sous **Zone**, sélectionnez **Catégorie de contenu**.

   e. Configurez le filtre de contenu :

   - **Catégorie de contenu**. Vous pouvez contrôler l'accès des utilisateurs aux ressources Internet par catégorie (par exemple, la catégorie *Réseaux sociaux*).
   - **Type 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 *Fichiers graphiques*).

f. Sous **Utilisateur ou groupe**, sélectionnez les utilisateurs auxquels vous souhaitez que le Contrôle Internet applique la règle.

Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

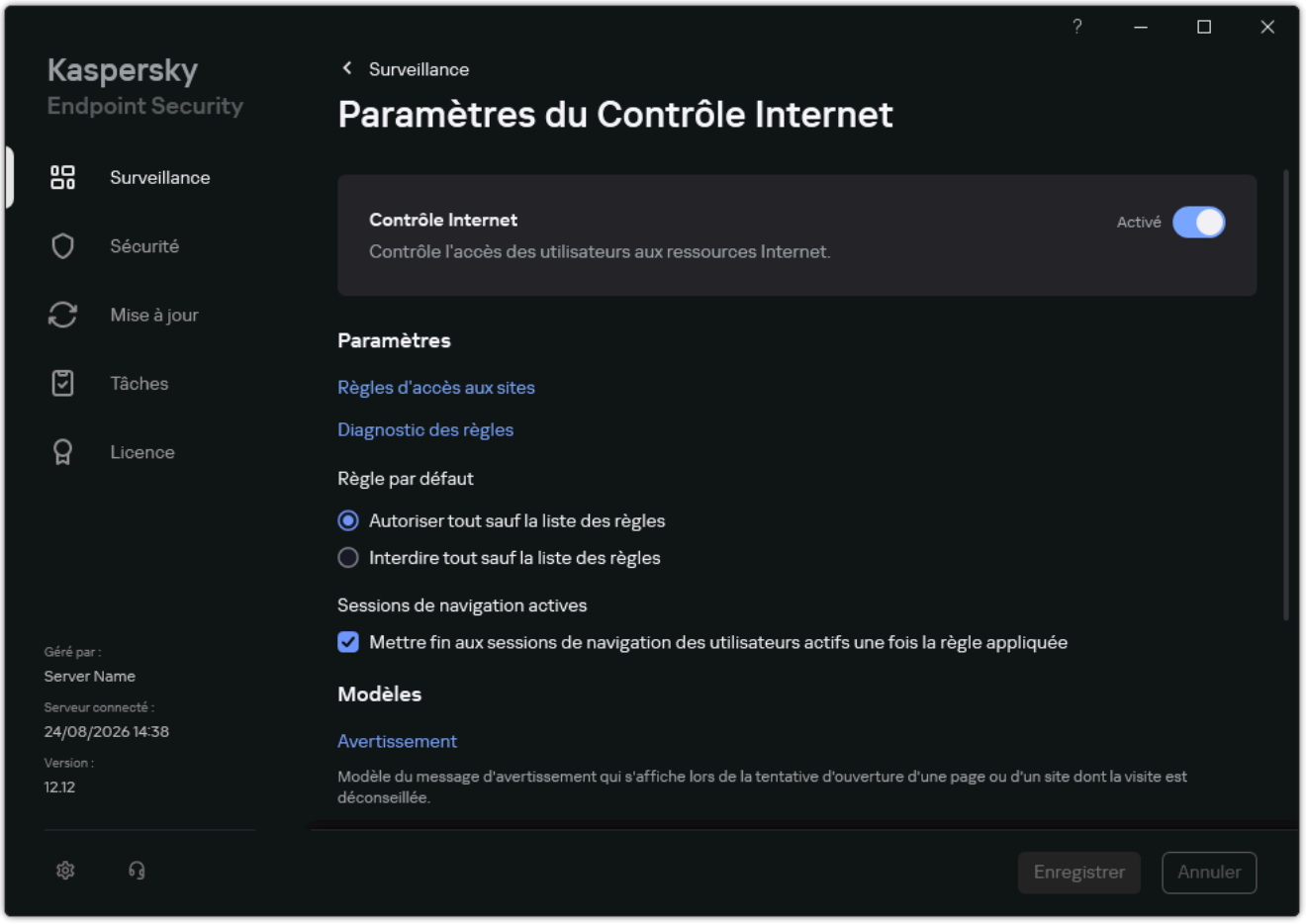
g. Dans le groupe **Planification de l'accès**, sélectionnez une planification ou créez-en une autre.

8. Enregistrez vos modifications.

Comment activer un filtre de contenu de ressources Internet 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 **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Cliquez sur le bouton **Règles d'accès aux sites** dans le groupe **Paramètres**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

La fenêtre **Règle d'accès aux sites** s'ouvre.

5. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

6. Sélectionnez l'état **Activé** 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 requise :

- **Autoriser**. Le Contrôle Internet permet l'accès aux ressources Internet qui correspondent aux paramètres de la règle.
- **Interdire**. Le Contrôle Internet bloque l'accès aux ressources Internet qui correspondent aux paramètres de la règle et affiche un message de refus d'accès au site Internet.
- **Avertir**. Lorsque l'utilisateur tente d'accéder à une ressource Internet correspondant à la règle, le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Internet est déconseillée. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

8. Dans le groupe **Contenu du filtre**, sélectionnez le filtre de contenu approprié :

- **Par catégories**. 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 *Fichiers graphiques*).

Pour configurer le filtre de contenu, procédez comme suit :

a. Cliquez sur le lien **Paramètres**.

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 **Utilisateurs**, sélectionnez le filtre approprié pour les utilisateurs :

- **À tous les utilisateurs**. Le Contrôle Internet ne filtrera pas les ressources Internet par adresse.
- **À certains utilisateurs et/ou groupes**. Le Contrôle Internet filtrera uniquement les adresses de ressources Internet de la liste. 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. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Pour créer une liste d'utilisateurs auxquels vous souhaitez appliquer la règle, procédez comme suit :

  a. Cliquez sur **Ajouter**.

  b. Dans la fenêtre qui s'ouvre, sélectionnez les utilisateurs ou les groupes 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.

10. 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 **Modifier ou ajouter une nouvelle**.

    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.

11. Si vous voulez que Contrôle Internet mette fin à la connexion avec la ressource Internet interdite immédiatement après l'application de la stratégie, cochez la case **Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée**.

    > Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions.

    Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.

12. Enregistrez vos modifications.

En conséquence, la nouvelle règle du Contrôle Internet est ajoutée à la liste. Si nécessaire, modifiez la priorité de la règle du Contrôle Internet. Vous pouvez également utiliser le commutateur pour désactiver la règle d'accès aux ressources Internet à tout moment sans la supprimer de la liste.

Vérification du fonctionnement des règles d'accès aux sites Internet

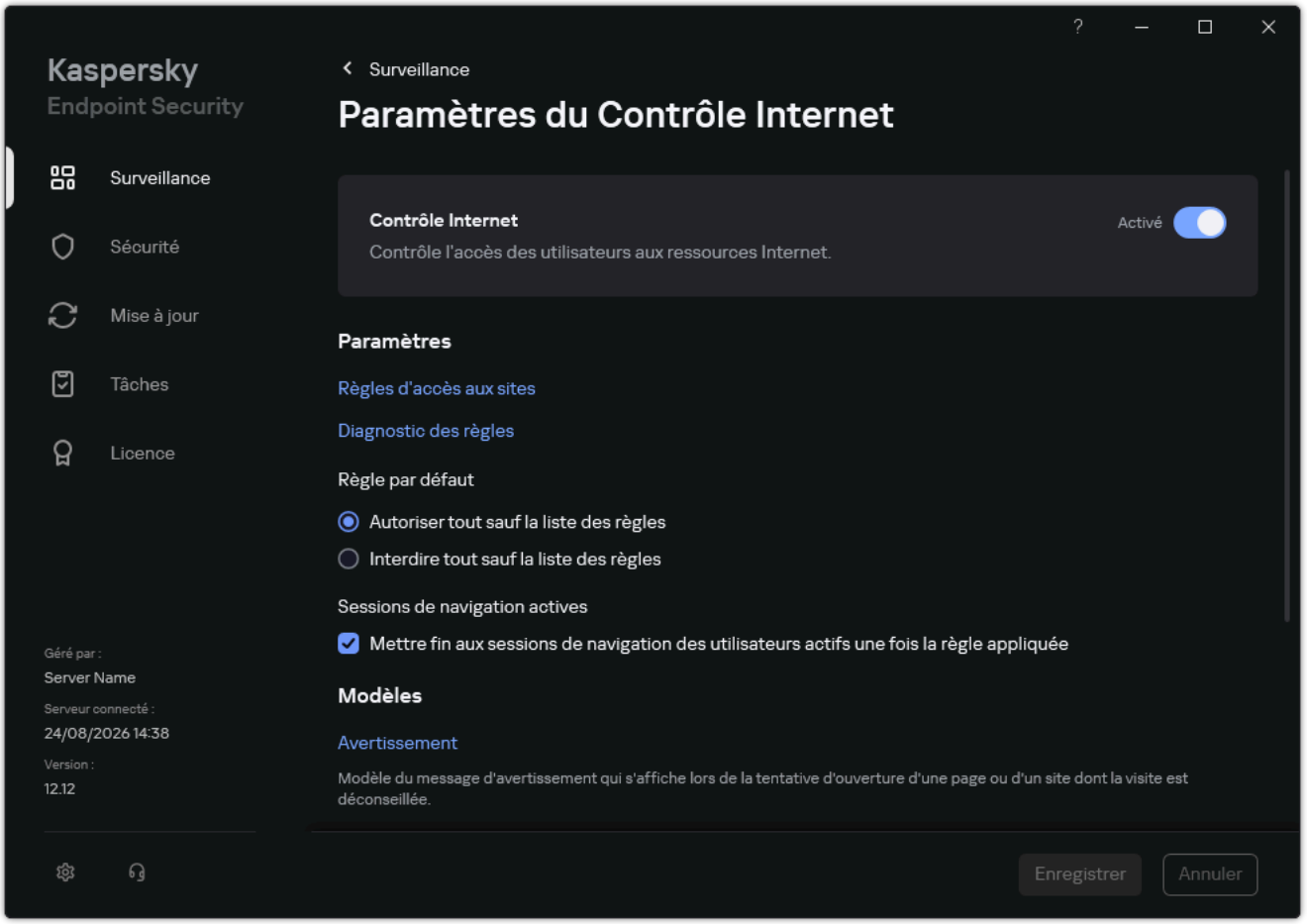
Lors de la configuration du Contrôle Internet, il se peut que vous bloquiez par inadvertance l'accès à des ressources Internet dont les utilisateurs ont besoin pour leur travail. Pour découvrir quelle règle du Contrôle Internet bloque l'accès aux ressources Internet, vous pouvez utiliser l'outil de *diagnostic des règles du Contrôle Internet*. Le diagnostic des règles de Contrôle Internet n'est disponible que dans l'interface de Kaspersky Endpoint Security. Dans la console de Kaspersky Security Center, il n'est pas possible de déterminer quelle règle de Contrôle Internet inclut une ressource donnée.

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.

Pour vérifier le fonctionnement des règles d'accès aux sites Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du 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.

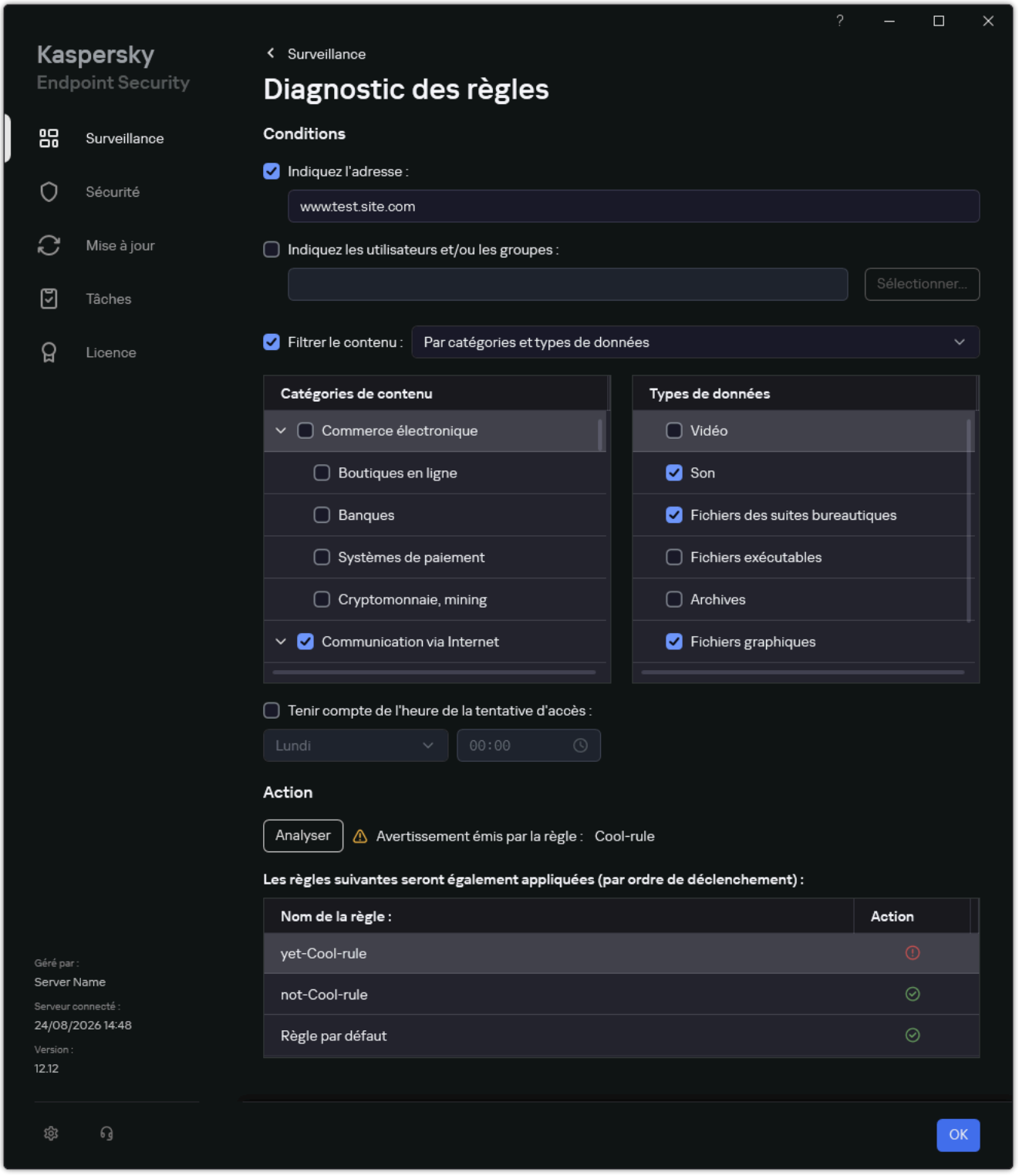
5. Définissez la liste des utilisateurs et/ou des groupes d'utilisateurs si vous voulez vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet pour des utilisateurs et / ou des groupes d'utilisateurs spécifiques.

6. Cochez la case **Filtrer le contenu** et sélectionnez l'option requise dans la liste déroulante (**Par catégories**, **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 certaines catégories de contenu et/ou certaines 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 **Analyser**.

A 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 **Analyser**. 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.



Résultat du test d'accès aux ressources Internet

Exportation et importation de règles du Contrôle Internet

Vous pouvez exporter la liste des règles du Contrôle Internet dans un fichier XML ou JSON. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.
4. Pour exporter la liste des règles du Contrôle Internet, 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.
5. Pour importer la liste des règles du Contrôle Internet, 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. Ouvrez le fichier.

      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.
6. Enregistrez vos modifications.

Exportation et importation d'une liste de règles du Contrôle Internet dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez 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. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des règles dans un fichier JSON dans le dossier des téléchargements par défaut.

6. Pour importer la liste des règles dans le groupe **Liste des règles**, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des règles.

   b. Ouvrez le fichier.

      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 JSON.

7. Enregistrez vos modifications.

Exportation et importation des adresses des ressources Internet de la règle du Contrôle 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 dans la Console d'administration (MMC)
- Au format JSON dans la Web Console
- Au format CSV dans l'interface de l'application

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.

Vous pouvez également exporter/importer toutes les règles du Contrôle Internet et pas seulement les adresses des ressources Internet d'une règle individuelle.

Comment exporter/importer les adresses des ressources Internet de la règle du Contrôle Internet dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.

5. Dans le groupe **Paramètres du Contrôle Internet**, sélectionnez la règle dont vous souhaitez exporter ou importer la liste des adresses de ressources Internet.

   Les propriétés de la règle du Contrôle Internet sont affichées.

6. Pour exporter la liste des ressources Internet, procédez comme suit dans la liste des adresses :

   a. Sélectionnez les adresses que vous souhaitez exporter.

      Si vous n'avez sélectionné aucune adresse, Kaspersky Endpoint Security exportera toutes les adresses.

   b. Appuyez sur le bouton .

   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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste des adresses de ressources Internet dans un fichier TXT.

7. Pour importer la liste des ressources Internet, procédez comme suit dans la liste des adresses :

   a. Appuyez sur le bouton .

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier TXT à partir duquel vous souhaitez importer la liste des ressources Internet.

   b. Ouvrez le fichier.

      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.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exporter/importer les adresses des ressources Internet de la règle du Contrôle Internet dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.

5. Dans le groupe **Liste des règles**, sélectionnez la règle dont vous souhaitez exporter ou importer la liste des adresses de ressources Internet.

   Les propriétés de la règle du Contrôle Internet sont affichées.

6. Cliquez sur le bouton **Modifier** dans le groupe **Zone** → **Sites Internet individuels**.

7. Pour exporter la liste des ressources Internet, procédez comme suit dans la liste des adresses :

   a. Sélectionnez les adresses que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des adresses des ressources Internet dans un fichier JSON dans le dossier des téléchargements par défaut.

8. Pour importer la liste des ressources Internet, procédez comme suit dans la liste des adresses :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des adresses des ressources Internet.

   b. Ouvrez le fichier.

      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 JSON.

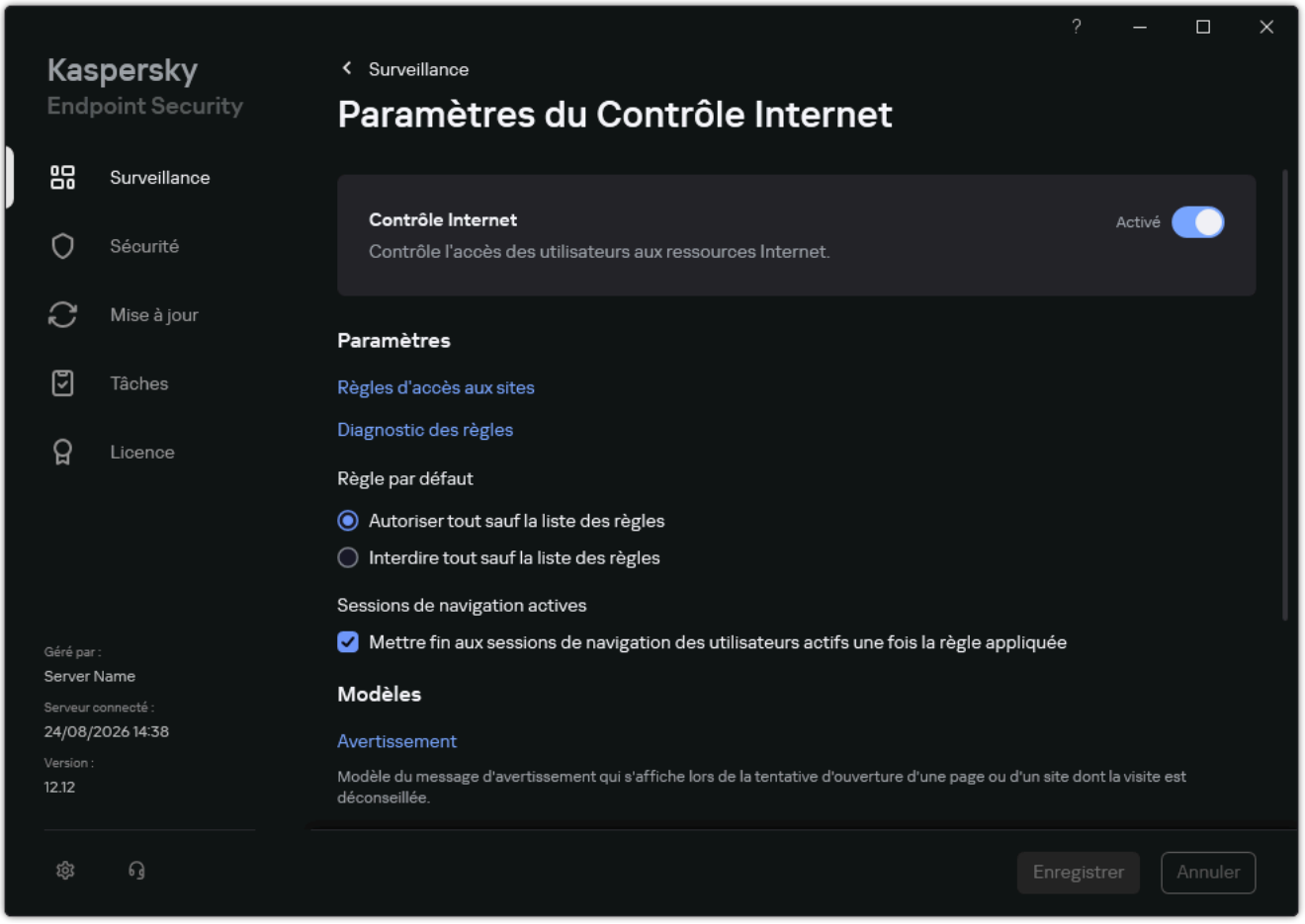
   Vous pouvez exporter et importer des groupes de sites Internet de la même manière.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exporter/importer les adresses des ressources Internet de la règle du Contrôle Internet 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 **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Cliquez sur le bouton **Règles d'accès aux sites** dans le groupe **Paramètres**.

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 **Exporter**.

   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format CSV dans lequel vous voulez exporter la liste des adresses de ressources Internet et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   d. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste des adresses de ressources Internet dans un fichier CSV.

6. Pour importer la liste des ressources Internet, procédez comme suit dans le groupe **Adresses** :

   a. Cliquez sur **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier CSV à partir duquel vous souhaitez importer la liste des ressources Internet.

   b. Ouvrez le fichier.

      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 CSV.

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.

Navigateurs prenant en charge la fonction de surveillance : Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. La surveillance de l'activité des utilisateurs ne fonctionne pas dans les autres navigateurs.

Kaspersky Endpoint Security génère les événements suivants liés à l'activité de l'utilisateur sur Internet :

- blocage d'un site (*Critique* état ⊗).
- visite sur un site Internet déconseillé (*Avertissement* état ⚠).
- visite sur un site Internet autorisé (*Information* état ⓘ).

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.

Injection d'un script d'interaction dans une page Internet

Comment injecter un script d'interaction avec les pages Internet dans le trafic Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
4. Dans le groupe **Analyse des connexions chiffrées**, cochez la case **Implanter un script dans le trafic Internet pour interagir avec les pages Internet**.
5. Enregistrez vos modifications.

Comment injecter un script d'interaction avec les pages Internet dans le trafic Internet dans Web Console et Cloud Console

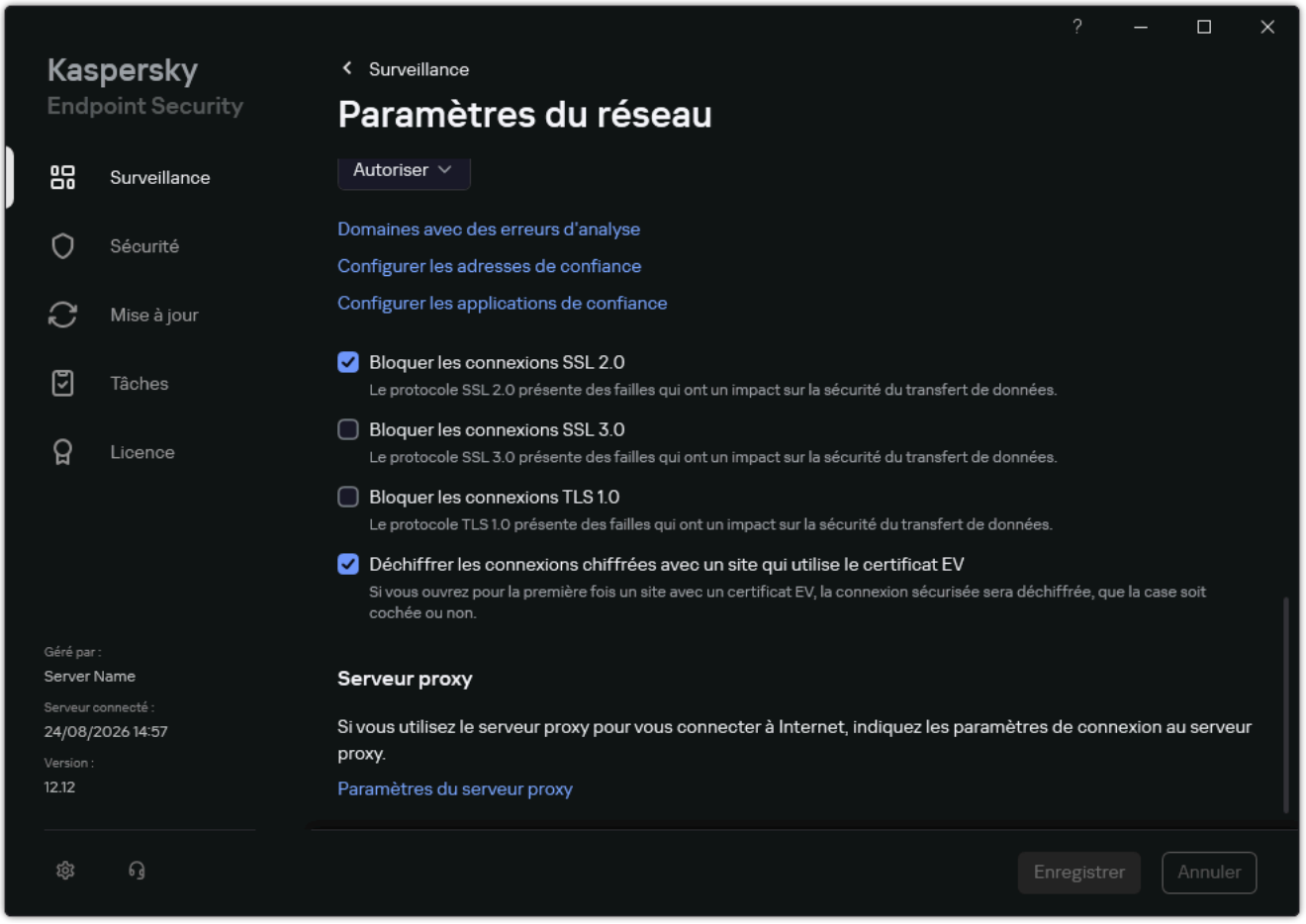
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
5. Sous **Surveillance des connexions Internet**, désactivez le commutateur **Surveillance des connexions Internet ACTIVÉE**.
6. Enregistrez vos modifications.

Comment injecter un script d'interaction avec les pages Internet dans le trafic Internet 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** → **Paramètres du réseau**.



Paramètres réseau des applications

3. Dans le groupe **Traitement du trafic**, cochez la case **Implanter un script dans le trafic Internet pour interagir avec les pages Internet**.

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.

Configuration de l'enregistrement des événements de Contrôle Internet

Pour configurer l'enregistrement des événements de Contrôle Internet sur l'ordinateur de l'utilisateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.

3. Cliquez sur le bouton **Configurer les notifications** dans le groupe **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 de notifications par email, 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.

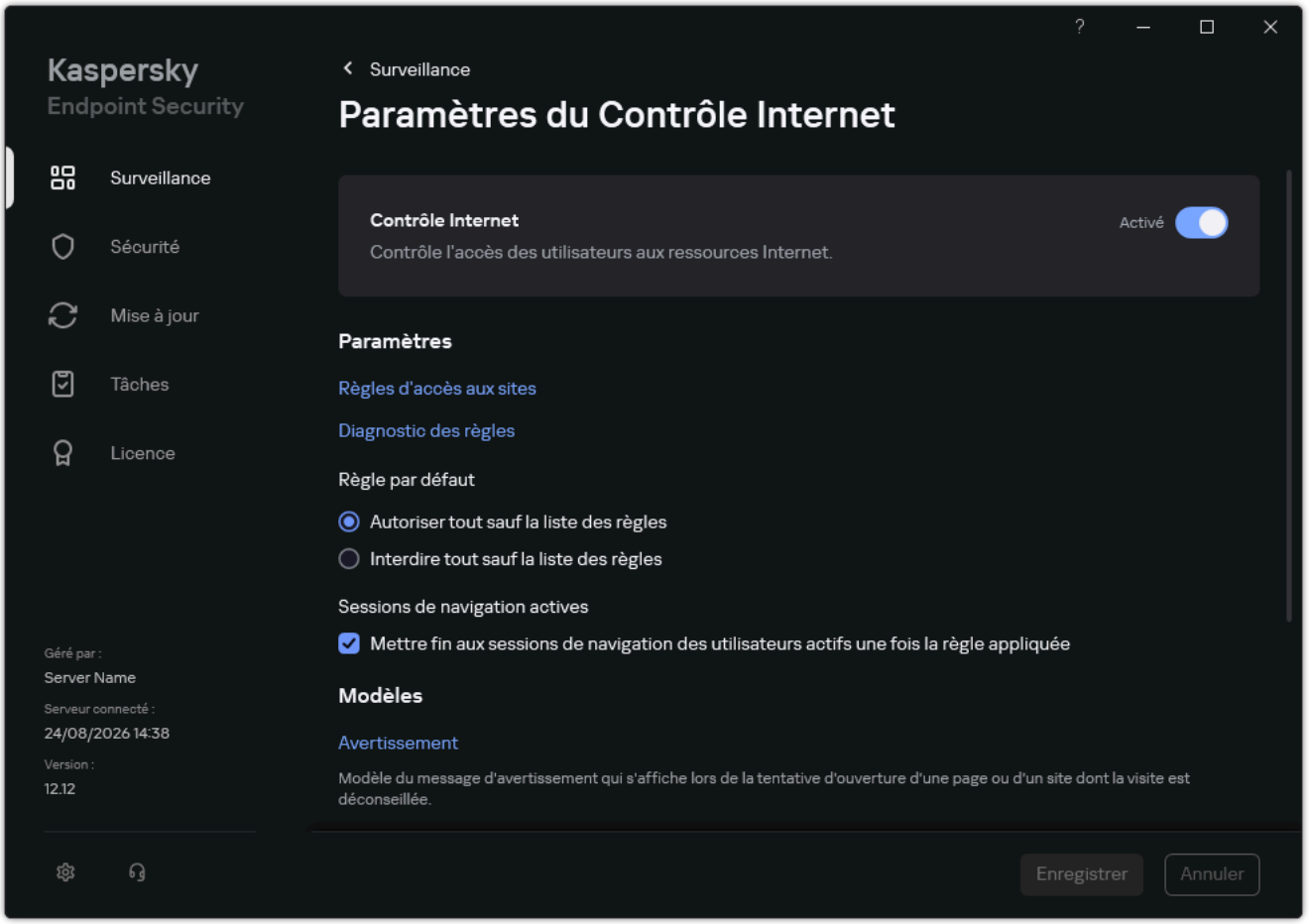
- Si vous utilisez Kaspersky Security Center Cloud Console, le Contrôle Internet regroupe les événements et envoie uniquement le protocole et le domaine du site Internet. Par exemple, si un utilisateur visite les pages Internet déconseillées http://www.example.com/main, http://www.example.com/contact et http://www.example.com/gallery, Kaspersky Endpoint Security envoie un seul événement avec l'objet http://www.example.com.

Enregistrement des événements liés aux visites sur des sites Internet autorisés

Pour activer l'enregistrement des événements liés aux visites sur des sites Internet autorisés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

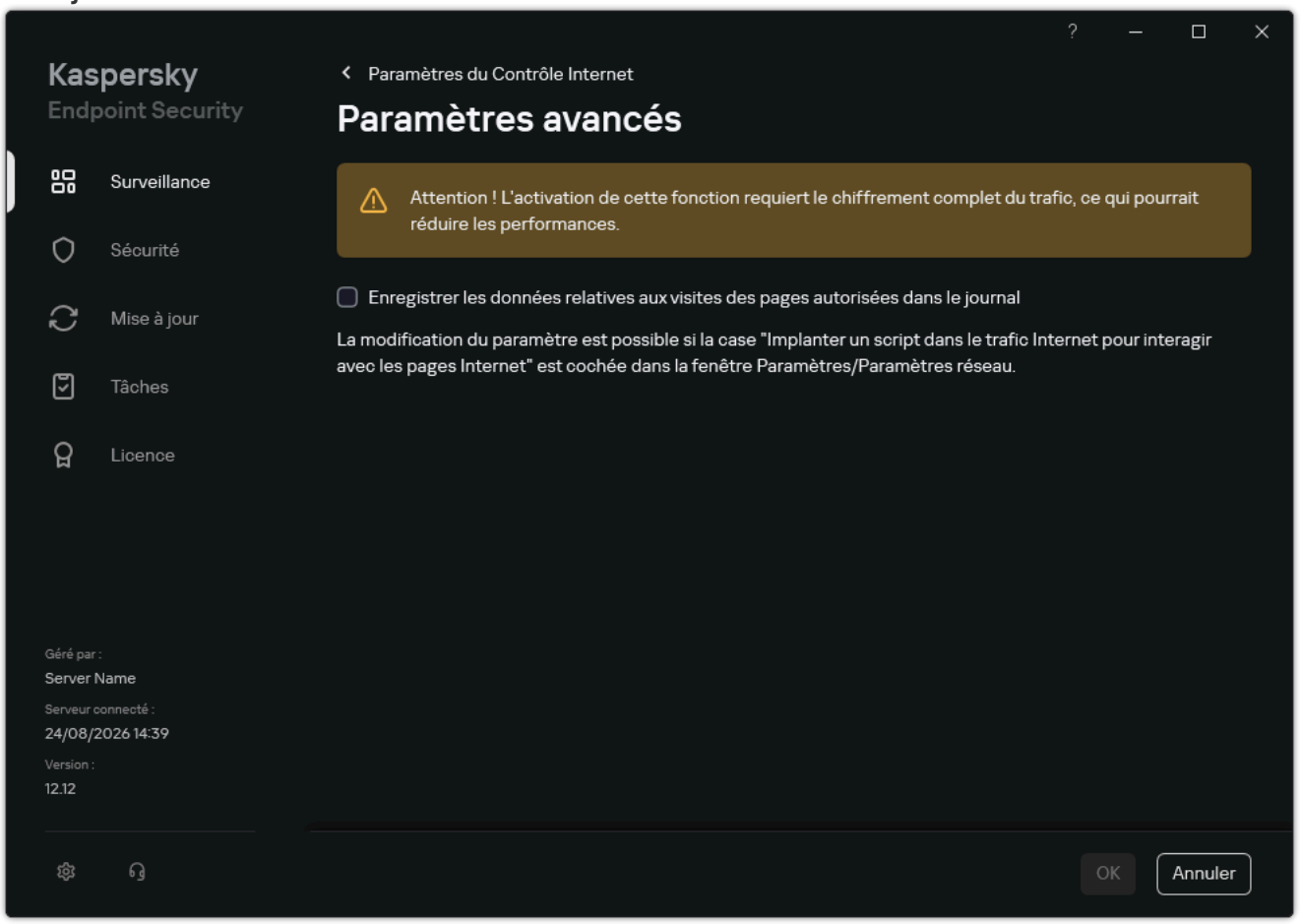
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Cliquez sur le bouton **Paramètres avancés** dans le groupe **Avancé**.

4. Dans la fenêtre qui s'ouvre, cochez la case **Enregistrer les données relatives aux visites des pages autorisées dans le journal**.



Paramètres avancés du Contrôle Internet

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

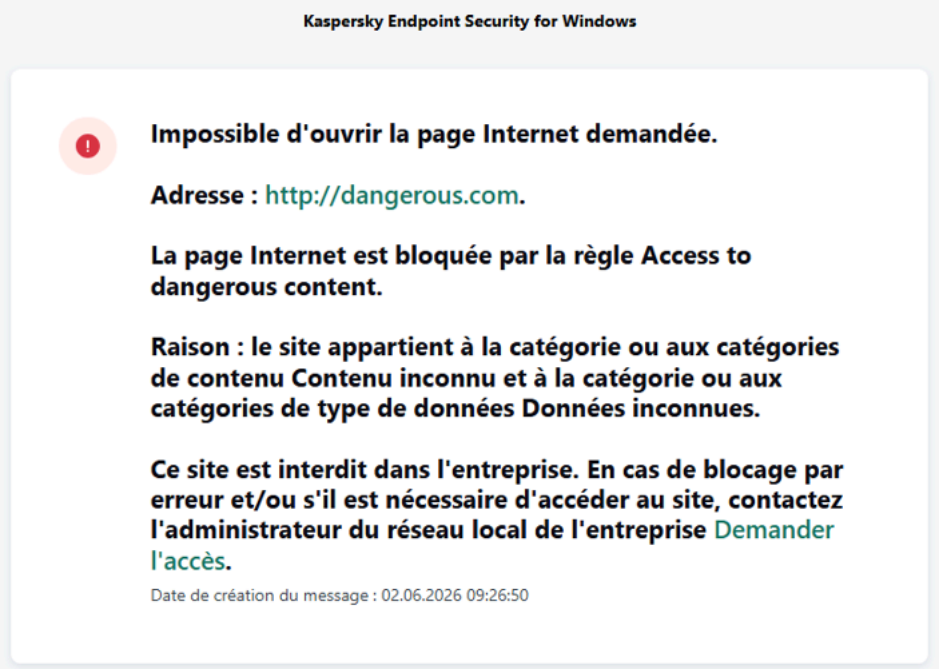
En fonction de l'action définie dans les propriétés des règles du Contrôle Internet, lorsque les utilisateurs essaient d'accéder aux sites Internet, Kaspersky Endpoint Security affiche un message (en remplaçant la réponse du serveur HTTP par une page HTML avec le message) de l'un des types suivants :

- 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.

  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 (cf. ill. ci-dessous) si l'option **Interdire** a été sélectionnée dans les paramètres 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.



Message sur le blocage des ressources Internet

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. Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.

Comment modifier le modèle du message du Contrôle Internet dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle Internet**.
4. Cliquez sur le bouton **Modèles** dans le groupe **Paramètres des modèles de notification**.

5. Configurez les modèles de messages du Contrôle Internet :

   - **Avertissement**. 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.

   - **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 pour l'administrateur**. 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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Par défaut**.

6. Enregistrez vos modifications.

Comment modifier le modèle du message du Contrôle Internet dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle Internet**.

5. Dans le bloc **Modèles de messages**, cliquez sur le lien **Notification sur le blocage du site Internet** et configurez les modèles pour les messages du Contrôle Internet :

   - **Avertissement**. 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.

   - **Notification 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 pour l'administrateur**. 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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

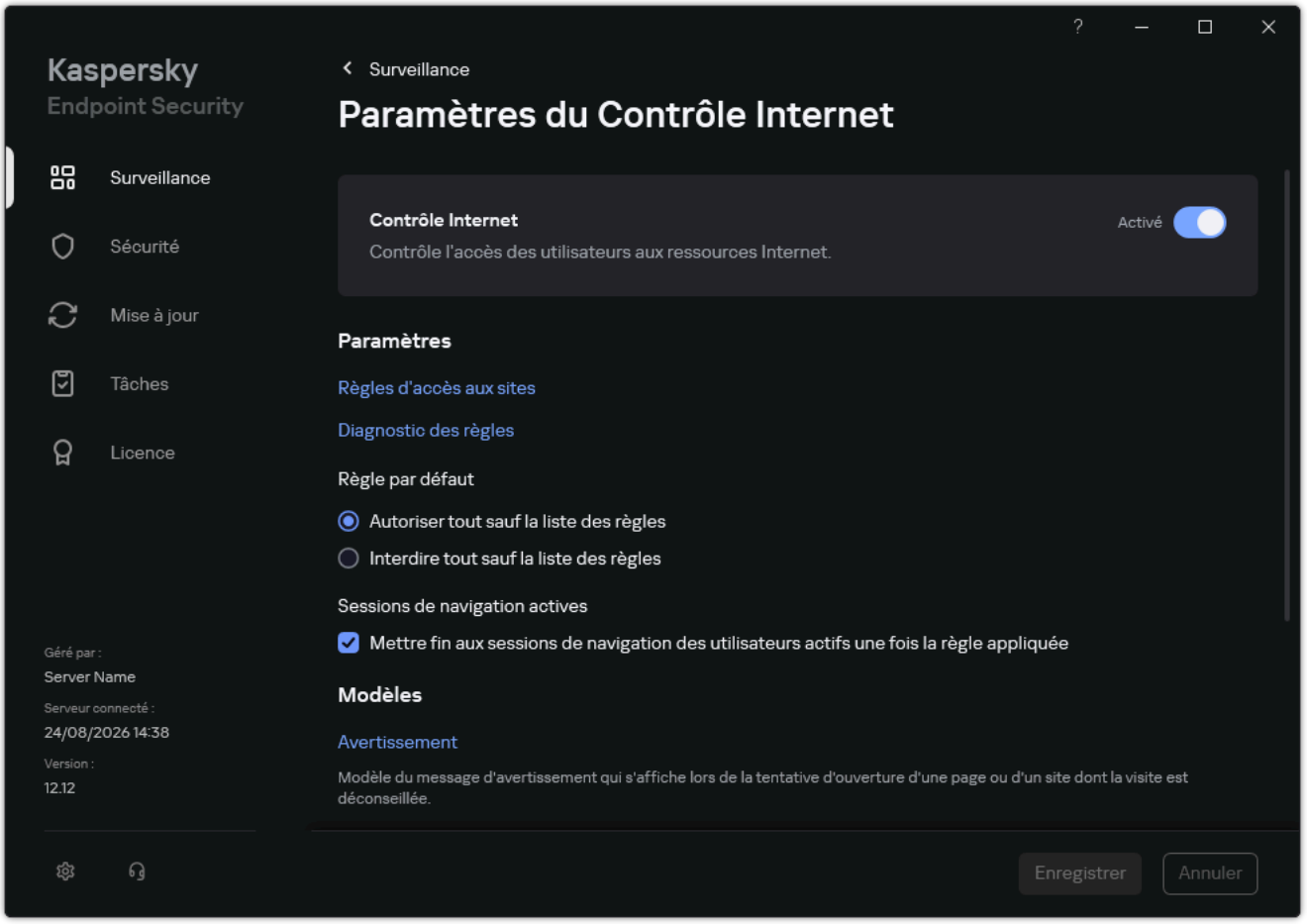
Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Rétablir les valeurs par défaut**.

6. Enregistrez vos modifications.

Comment modifier le modèle du message du Contrôle Internet 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 **Contrôles de sécurité** → **Contrôle Internet**.



Paramètres du Contrôle Internet

3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle Internet :

- **Avertissement**. 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.

- **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 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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Réinitialiser les paramètres**.

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 d'adresse `example.com` couvre 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.

Exemples d'application des règles de création de masques d'adresses

Non.	Masque d'adresse	Adresse du site Internet analysée	Est-ce que l'adresse analysée satisfait au masque d'adresse	Commentaire
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

Contrôle Internet pour les machines virtuelles

Le Contrôle Internet contrôle le trafic sur l'ordinateur ainsi que sur la machine virtuelle déployée localement sur l'ordinateur. Cette opération fonctionne sans qu'il soit nécessaire d'installer l'application Kaspersky Endpoint Security sur la machine virtuelle locale. Cela signifie que si l'utilisateur tente d'ouvrir un site Internet bloqué par une règle du Contrôle Internet dans le navigateur de la *machine virtuelle*, l'application installée sur le système d'exploitation hôte de l' *ordinateur* interdit l'accès à ce site.

Le fonctionnement du Contrôle Internet est différent selon les machines virtuelles.

Oracle VM VirtualBox

Kaspersky Endpoint Security prend en charge les règles du Contrôle Internet sur les machines virtuelles Oracle VM VirtualBox sans aucune limitation. L'application peut contrôler entièrement le trafic de la machine virtuelle. Si un filtre par utilisateur est configuré dans les règles du Contrôle Internet, l'application fonctionne correctement, car tous les processus des machines virtuelles sont lancés par l'utilisateur local.

VMware Workstation

Kaspersky Endpoint Security prend en charge les règles du Contrôle Internet sur les machines virtuelles VMware Workstation avec certaines limitations. L'application ne prend pas en charge les règles avec un filtre par utilisateur configuré. Les processus de la machine virtuelle sont exécutés par l'utilisateur système (SYSTEM). De ce fait, il est impossible d'identifier l'utilisateur qui tente d'ouvrir le site Internet sur la machine virtuelle.

Microsoft Hyper-V

Kaspersky Endpoint Security ne prend pas en charge les règles du Contrôle Internet sur les machines virtuelles Microsoft Hyper-V.

Variables dans les modèles de message du Contrôle Internet

Vous pouvez utiliser les variables suivantes dans les modèles de messages utilisateur ou administrateur :

- **Nom d'utilisateur** – `%USER_NAME%`.

  Nom du compte utilisateur actuel de l'ordinateur sur lequel le message a été généré, dans le format `<device name>\<user alias>` (par exemple, `DESKTOP-123\John.Smith`).

- **Adresse de la ressource Internet** – `%CANONIC_REQUEST_URL%`.

  Adresse de la ressource Internet bloquée.

- **Nom de la règle** – `%RULE%`.

  Nom de la règle qui a bloqué la ressource Internet.

- **Adresse pour les messages** – `%COMPLAIN_EMAIL%`.

  Adresse email pour les commentaires concernant les blocs de ressources Internet. En cliquant sur l'adresse email, une fenêtre s'ouvre dans laquelle l'utilisateur peut écrire un message à l'administrateur.

- **Nom de catégorie de contenu** – `%CONTENT_CATEGORY_LIST%`.

  Catégorie de site à laquelle appartient la ressource bloquée (par exemple, *Systèmes de paiement*).

- **Nom de catégorie de type de données** – `%TYPE_CATEGORY_LIST%`.

  Catégorie de type de données sur la ressource Internet bloquée (par exemple, *Fichiers graphiques*).

- **Lien vers la ressource Internet demandée** – `%CONTINUE_PAGE%`.

  Lien vers la page Internet demandée (par exemple, `http://www.example.com/pagename.html`).

- **Lien vers le site** – `%CONTINUE_SITE%`.

  Lien vers le site qui contient la page Internet demandée (par exemple, `http://www.example.com/`).

- **Lien d'accès aux domaines** – `%CONTINUE_DOMAIN%`.

  Lien cliquable permettant d'accéder à toutes les pages Internet existantes du nom de domaine. Par exemple, si l'adresse de la page Internet bloquée est `http://www.example.com`, la variable `%CONTINUE_DOMAIN%` est remplacée par le lien `http://*.example.com`. Ce lien permet d'accéder à toutes les adresses Internet du nom de domaine de base `http://www.example.com/`, y compris les sous-domaines, par exemple, `http://start.example.com/*` ou `http://domain.domain.example.com/*`, où le caractère `*` représente n'importe quelle séquence de caractères (y compris une chaîne vide).

Contrôle des appareils

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à un 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.

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 **Avancé** → **Stockages** → **Matériel**.

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 – ⊘.

- Selon les règles (imprimantes et appareils portables uniquement) – .
- Dépend du bus de connexion (sauf Wi-Fi) – .
- Interdire avec des exceptions (Wi-Fi uniquement) – .

- **Bus de connexion**. Un *bus de connexion* est une interface qui permet de connecter des appareils à l'ordinateur (USB, FireWire, etc.). Si le mode **Dépend du bus de connexion** est sélectionné pour le type d'appareil, l'application autorise ou interdit l'accès à l'appareil en fonction de l'interface de connexion (par exemple, 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.

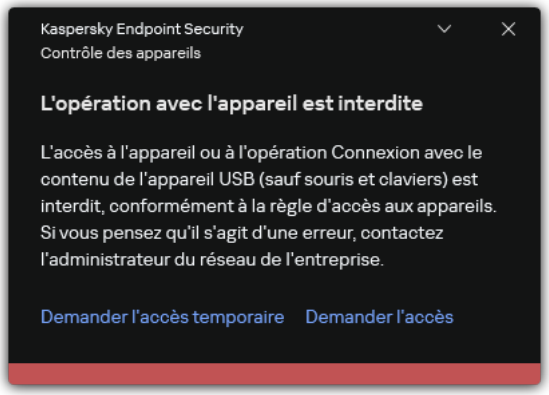
  Vous pouvez ajouter des appareils de confiance en fonction des données suivantes :

  - **Appareils en fonction de l'identifiant**. 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'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers.
  - **Appareils en fonction du modèle**. Chaque appareil possède un Vendor ID (VID) et un 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 ajouter des appareils à la liste 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 des PID similaires (par exemple, des appareils du même fabricant), vous pouvez ajouter des appareils à la liste 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.

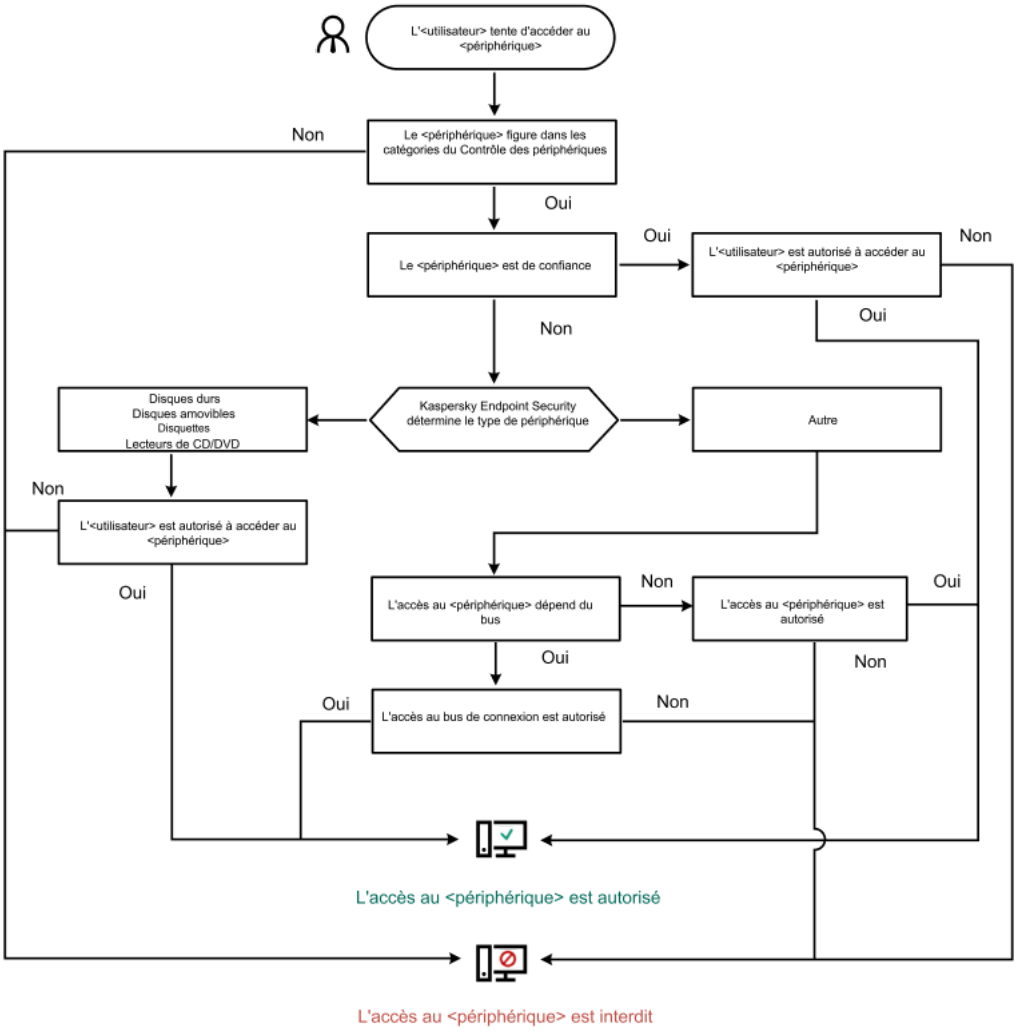
Quand l'appareil se connecte à un ordinateur auquel l'accès est interdit par le Contrôle des appareils, Kaspersky Endpoint Security bloque l'accès et affiche une notification (cf. ill. ci-dessous).



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.

À propos des règles d'accès

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. 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 (y compris les clés USB)	✓	✓	✓	✓	✓
Disquettes	✓	✓	✓	✓	✓
Lecteurs de CD/DVD	✓	✓	✓	✓	✓
Appareils portables (MTP)	✓	✓	✓	✓	✓
Imprimantes locales	✓	–	✓	✓	–
Imprimantes réseau	✓	–	✓	✓	–
Modems	✓	–	–	–	–
Lecteurs de bande	✓	–	–	–	–
Appareils multifonctions	✓	–	–	–	–
Appareils de lecture des cartes à puce	✓	–	–	–	–
Appareils Windows CE USB ActiveSync	✓	–	–	–	–
Adaptateurs réseau externes	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Caméras et scanners	✓	–	–	–	–

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

Si l'option **Dépend du bus de connexion** est sélectionnée pour la règle d'accès selon le type d'appareil, l'application autorise ou interdit l'accès à l'appareil en fonction de l'interface de connexion. 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.

Les règles d'accès au bus de connexion déterminent uniquement l'autorisation (état ✓) ou l'interdiction (état ⊘) de la connexion d'appareils. La priorité des règles d'accès au type d'appareil est supérieure à celle des règles d'accès au bus de connexion.

> Le clavier et la souris ne peuvent pas être verrouillés à l'aide du Contrôle des appareils. Si vous interdisez l'accès au bus de connexion USB, l'utilisateur continuera à utiliser un clavier et une souris connectés via USB. Le module Protection BadUSB est conçu pour empêcher les appareils USB infectés imitant des claviers de se connecter à l'ordinateur.

Obtention d'informations sur les appareils installés

Kaspersky Security Center reçoit des informations sur les appareils installés en provenance des sources suivantes : l'Agent d'administration et Kaspersky Endpoint Security. Les informations sur les appareils installés sont nécessaires à la gestion des accès et à la création d'une liste d'appareils de confiance.

Informations sur le matériel informatique

Si l'Agent d'administration est installé sur un appareil Windows, il transmet au Serveur d'administration les informations suivantes sur le matériel de l'appareil :

- Mémoire vive
- appareils de stockage (y compris les disques durs)
- carte mère
- Processeur
- adaptateur réseau
- moniteurs

- processeur graphique
- carte son

L'Agent d'administration fournit ces informations à chaque synchronisation avec Kaspersky Security Center. Vous pouvez consulter le matériel d'un ordinateur dans les propriétés de celui-ci (**Registre du matériel**).

Informations sur le matériel

Kaspersky Endpoint Security fournit des informations sur le matériel installé : imprimantes, disques amovibles, appareils portables (MTP), etc. Pour recevoir des informations sur le matériel, vous devez appliquer une stratégie active autorisant la transmission d'informations sur les appareils installés (cette transmission est activée par défaut).

Comment activer la transmission des données sur les appareils installés dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Transfert des données au Serveur d'administration**.
6. Cochez la case **Appareils installés**.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer la transmission des données sur les appareils installés dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.
5. Cliquez sur le bouton **Paramètres avancés** dans le groupe **Transfert des données au Serveur d'administration**.
6. Cochez la case **À propos des appareils installés**.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Vous pouvez ensuite consulter la liste des appareils installés dans la console Kaspersky Security Center (**Stockages** → **Matériel**).

Gestion de l'accès aux appareils par type

Le Contrôle des appareils permet de gérer l'accès aux appareils par type. Le type de l'appareil est déterminé par le système d'exploitation au moment de la connexion de l'appareil. Vous pouvez rechercher le type d'appareil à l'aide de l'outil Gestionnaire d'appareils intégré au système d'exploitation. Pour gérer l'accès aux appareils, vous devez configurer les règles. 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. 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.

Par défaut, le Contrôle des appareils autorise l'accès à tous les appareils pour tous les utilisateurs.

Vous pouvez configurer l'accès aux appareils comme suit :

- **Autoriser**.

  Kaspersky Endpoint Security accorde à tous les utilisateurs un accès complet aux appareils.

- **Interdire**.

  Kaspersky Endpoint Security bloque les connexions des appareils. L'application permet de connecter uniquement les appareils de confiance.

- **Dépend du bus de connexion**.

  Kaspersky Endpoint Security détermine l'interface de connexion des appareils et restreint l'accès aux appareils en fonction de l'état de leur connexion au bus. L'application permet également de connecter des appareils de confiance.

- **Selon les règles**.

  Pour certains types d'appareils, vous pouvez désigner des utilisateurs individuels ou un groupe d'utilisateurs autorisés à utiliser les appareils, configurer une planification de l'accès aux appareils et définir des autorisations de lecture et d'écriture. L'application permet également de connecter des appareils de confiance.

Soyez prudent lors de la configuration de l'accès aux appareils de type **Disques durs**. Si vous bloquez l'accès au disque système, l'application peut provoquer un blocage avec écran bleu (BSOD) lors du démarrage du système d'exploitation.

Si un appareil n'entre pas dans le schéma de classification du Contrôle des appareils, l'accès à cet appareil ne peut pas être restreint.

Comment gérer l'accès aux appareils par type dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.

6. Configurez les règles d'accès pour les appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus de connexion**, **Selon les règles**.

      Pour sélectionner le mode d'accès **Selon les règles**, vous devez double-cliquer dessus pour ouvrir les propriétés de la règle d'accès.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus de connexion**, vous devez configurer les règles d'accès aux interfaces de connexion sous l'onglet **Bus de connexion**.

   c. Pour les appareils de stockage (les supports amovibles, par exemple), vous pouvez configurer les autorisations d'accès pour des utilisateurs individuels. Vous pouvez également planifier l'accès aux appareils et configurer les autorisations en lecture et en écriture.

      Vous pouvez ajouter des appareils à la liste des applications 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.

   d. Si nécessaire, configurez les règles d'impression.

   e. Si nécessaire, configurez les règles d'accès aux appareils Bluetooth.

   f. Si nécessaire, configurez les règles de connexion Wi-Fi de l'ordinateur.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment gérer l'accès aux appareils par type dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Sous les **Règles d'accès aux appareils**, sélectionnez l'onglet **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Configurez les règles d'accès pour les appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus**, **Personnalisé**.

      Si le mode d'accès est manquant dans le menu déroulant, ouvrez les propriétés de la règle d'accès en double-cliquant sur le type d'appareil.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus**, vous devez configurer les règles d'accès aux interfaces de connexion sous l'onglet **Bus de connexion**.

c. Pour les appareils de stockage (les supports amovibles, par exemple), vous pouvez configurer les autorisations d'accès pour des utilisateurs individuels. Vous pouvez également planifier l'accès aux appareils et configurer les autorisations en lecture et en écriture.

   Vous pouvez ajouter des appareils à la liste des applications 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.

d. Si nécessaire, configurez les règles d'impression.

e. Si nécessaire, configurez les règles d'accès aux appareils Bluetooth.

f. Si nécessaire, configurez les règles de connexion Wi-Fi de l'ordinateur.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment gérer l'accès aux appareils 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 **Contrôles de sécurité** → **Contrôle des appareils**.

3. Dans le groupe **Paramètres d'accès**, cliquez sur le lien **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

4. Configurez les règles d'accès pour les appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus de connexion**, **Selon les règles**.

      Si le mode d'accès est manquant dans le menu déroulant, ouvrez les propriétés de la règle d'accès en double-cliquant sur le type d'appareil.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus de connexion**, vous devez configurer les règles d'accès aux interfaces de connexion sous l'onglet **Bus de connexion**.

   c. Pour les appareils de stockage (les supports amovibles, par exemple), vous pouvez configurer les autorisations d'accès pour des utilisateurs individuels. Vous pouvez également planifier l'accès aux appareils et configurer les autorisations en lecture et en écriture.

      Vous pouvez ajouter des appareils à la liste des applications 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.

   d. Si nécessaire, configurez les règles d'impression.

   e. Si nécessaire, configurez les règles d'accès aux appareils Bluetooth.

   f. Si nécessaire, configurez les règles de connexion Wi-Fi de l'ordinateur.

5. Enregistrez vos modifications.

Par conséquent, lorsqu'un utilisateur tente d'accéder à un appareil, l'application bloque l'accès conformément aux règles. Kaspersky Endpoint Security enregistre également un événement correspondant. Si vous souhaitez autoriser l'accès à des appareils isolés, vous pouvez ajouter ces appareils à la liste des appareils de confiance.

Gestion de l'accès aux appareils par bus de connexion

Pour modifier la règle d'accès au bus de connexion, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Bus de connexion** dans le groupe **Paramètres d'accès**.

   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**.

   Si vous avez modifié l'accès au bus de connexion **Port série** (COM) ou **Port parallèle** (LPT), vous devez redémarrer l'ordinateur pour activer la règle d'accès.
6. Enregistrez vos modifications.

Distinction des droits d'accès des utilisateurs aux appareils

Vous pouvez configurer les droits d'accès des utilisateurs selon le type d'appareil ou aux appareils de confiance.

Différenciation des droits d'accès des utilisateurs selon le type d'appareil

Le Contrôle des appareils permet de configurer les droits d'accès des utilisateurs aux données sur les *appareils de stockage*. Pour ces appareils, vous pouvez configurer les autorisations d'écriture et de lecture. Le Contrôle des appareils prend en charge les types d'*appareils de stockage*:

- Disques durs
- Disques amovibles (y compris les clés USB)
- Disquettes
- Lecteurs de CD/DVD
- Appareils portables (MTP) Les appareils portables (MTP) incluent, par exemple, les appareils mobiles, les appareils photo, les lecteurs multimédias, etc.

Ainsi, vous pouvez par exemple autoriser l'utilisation des supports amovibles uniquement au groupe d'administrateurs. Pour les autres types d'appareils, vous pouvez interdire ou autoriser l'accès à tous les utilisateurs. Vous pouvez également configurer les droits d'accès des utilisateurs aux imprimantes.

Comment configurer les droits d'accès des utilisateurs aux données sur les appareils de stockage dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.

6. Pour configurer les règles d'accès aux appareils de stockage, double-cliquez pour ouvrir la liste des règles.

7. Configurer la règle d'accès aux appareils de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils de stockage.

   b. Dans le champ **Priorité de la règle**, définissez la priorité de la *règle d'écriture*. 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

8. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

   Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

9. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer les droits d'accès des utilisateurs aux données sur les appareils de stockage dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans le groupe **Règles d'accès aux appareils**, dans le tableau des règles d'accès, ouvrez les propriétés des règles d'accès pour les appareils de stockage.

6. Dans le groupe **Règles d'accès aux appareils**, sélectionnez l'option **Personnalisé**.

7. Configurer la règle d'accès aux appareils de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Utilisateurs et leurs droits**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils de stockage.

   b. Dans le champ **Priorité**, définissez la priorité de la *règle d'écriture*. 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   c. Sous **Utilisateur ou groupe**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Sous **Planification de l'accès**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

      Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

   e. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

   f. Cliquez sur **Enregistrer**.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment configurer les droits d'accès des utilisateurs aux données sur les appareils de stockage 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 **Contrôles de sécurité** → **Contrôle des appareils**.

3. Dans le groupe **Paramètres d'accès**, cliquez sur le lien **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

4. Pour configurer les règles d'accès aux appareils de stockage, faites un clic droit pour ouvrir la liste des règles.

5. Configurer la règle d'accès aux appareils de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Droits des utilisateurs**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils de stockage.

   b. Dans le champ **Priorité**, définissez la priorité de la *règle d'écriture*. 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   c. Sous **Utilisateurs**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory ou saisir un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

6. Sous **Planification de l'accès aux appareils**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

   Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

7. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

8. Enregistrez vos modifications.

Distinction des droits d'accès des utilisateurs aux 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. Vous pouvez configurer les droits d'accès des utilisateurs dans les propriétés de l'appareil de confiance.

Gestion de l'accès aux appareils mobiles

Kaspersky Endpoint Security vous permet de contrôler l'accès aux données sur les appareils mobiles fonctionnant sous Android et iOS. Les appareils mobiles appartiennent à la catégorie des appareils portables (MTP). Par conséquent, pour configurer l'accès aux données sur les appareils mobiles, vous devez modifier les paramètres d'accès relatifs aux 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 et du mode de connexion USB sélectionné. Kaspersky Endpoint Security vous permet de configurer des autorisations d'accès individuelles pour les données des appareils mobiles dans les applications ADB, iTunes ou le gestionnaire de fichiers. Dans tous les autres cas, le Contrôle des appareils autorise l'accès aux appareils mobiles conformément aux règles d'accès aux appareils portables (MTP).

Accès aux appareils mobiles

Les appareils mobiles appartiennent à la catégorie des appareils portables (MTP), par conséquent, leurs paramètres sont les mêmes. Vous pouvez sélectionner l'un des modes d'accès suivants aux appareils mobiles :

- **Autoriser**. Kaspersky Endpoint Security permet un accès complet aux appareils mobiles. Vous pouvez ouvrir, créer, modifier, copier ou supprimer des fichiers sur des appareils mobiles à l'aide du gestionnaire de fichiers ou des applications ADB et iTunes. Vous pouvez également charger la batterie de l'appareil en connectant l'appareil mobile à un port USB de l'ordinateur.

- **Interdire**. Kaspersky Endpoint Security limite l'accès aux appareils mobiles dans le gestionnaire de fichiers et les applications ADB et iTunes. L'application n'autorise l'accès qu'à appareils mobiles de confiance. Vous pouvez également charger la batterie de l'appareil en connectant l'appareil mobile à un port USB de l'ordinateur.

- **Dépend du bus de connexion**. Kaspersky Endpoint Security autorise la connexion aux appareils mobiles en fonction de l'état de la connexion USB (**Autoriser** ou **Interdire**).

- **Selon les règles**. Kaspersky Endpoint Security limite l'accès aux appareils mobiles conformément aux règles. Dans les règles, vous pouvez configurer les droits d'accès (lecture/écriture), sélectionner les utilisateurs ou un groupe d'utilisateurs pouvant avoir accès aux appareils mobiles, et configurer un horaire d'accès aux appareils mobiles. Vous pouvez également restreindre l'accès aux données sur les appareils mobiles à l'aide des applications ADB et iTunes.

Configuration des règles d'accès aux appareils mobiles

Les règles d'accès pour les appareils portables (MTP), les appareils ADB et les appareils iTunes sont configurées différemment. Pour les appareils portables (MTP) et les appareils ADB, vous pouvez configurer des règles pour des utilisateurs individuels ou des groupes d'utilisateurs et créer un programme selon lequel les règles s'appliqueront. Pour les appareils iTunes, cette opération n'est pas possible. Vous pouvez uniquement autoriser ou refuser l'accès aux données via l'application iTunes pour tous les utilisateurs.

Comment configurer les règles d'accès aux appareils mobiles dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
4. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.
5. Dans le menu contextuel relatif au type d'appareil **Appareils portables (MTP)**, configurez le mode d'accès aux appareils mobiles : **Autoriser** ✓, **Interdire** ⊘ ou **Dépend du bus de connexion** ◔.
6. Pour configurer les règles d'accès aux appareils mobiles, double-cliquez pour ouvrir la liste des règles.
7. Configurer la règle d'accès aux appareils mobiles :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils mobiles.

   b. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

8. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils mobiles pour les utilisateurs.

   Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

9. Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

10. Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

    Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

11. Sous **Accès via iTunes**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

    Kaspersky Endpoint Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.

12. Enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils mobiles dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans le groupe **Règles d'accès aux appareils**, cliquez sur le lien **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Sélectionnez le type d'appareil **Appareils portables (MTP)**.

   Cette action ouvre les droits d'accès aux appareils portables (MTP).

7. Configurez le mode d'accès aux appareils mobiles : **Autoriser**, **Interdire**, **Dépend du bus** ou **Personnalisé**.

8. À l'aide du commutateur **Accès via iTunes pour tous les utilisateurs ACTIVÉ**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

   Kaspersky Endpoint Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.

9. Si vous sélectionnez le mode **Personnalisé**, vous devez ajouter des règles d'accès pour les appareils. Pour ce faire, sous **Utilisateurs et leurs droits**, cliquez sur le bouton **Ajouter** et configurez la règle d'accès aux appareils mobiles :

   a. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   b. Sous **Utilisateur ou groupe**, sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès aux appareils mobiles. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   c. Sous **Planification de l'accès**, configurez une planification d'accès aux appareils mobiles pour les utilisateurs.

      > Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

   d. Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

   e. Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

      Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

10. Enregistrez vos modifications.

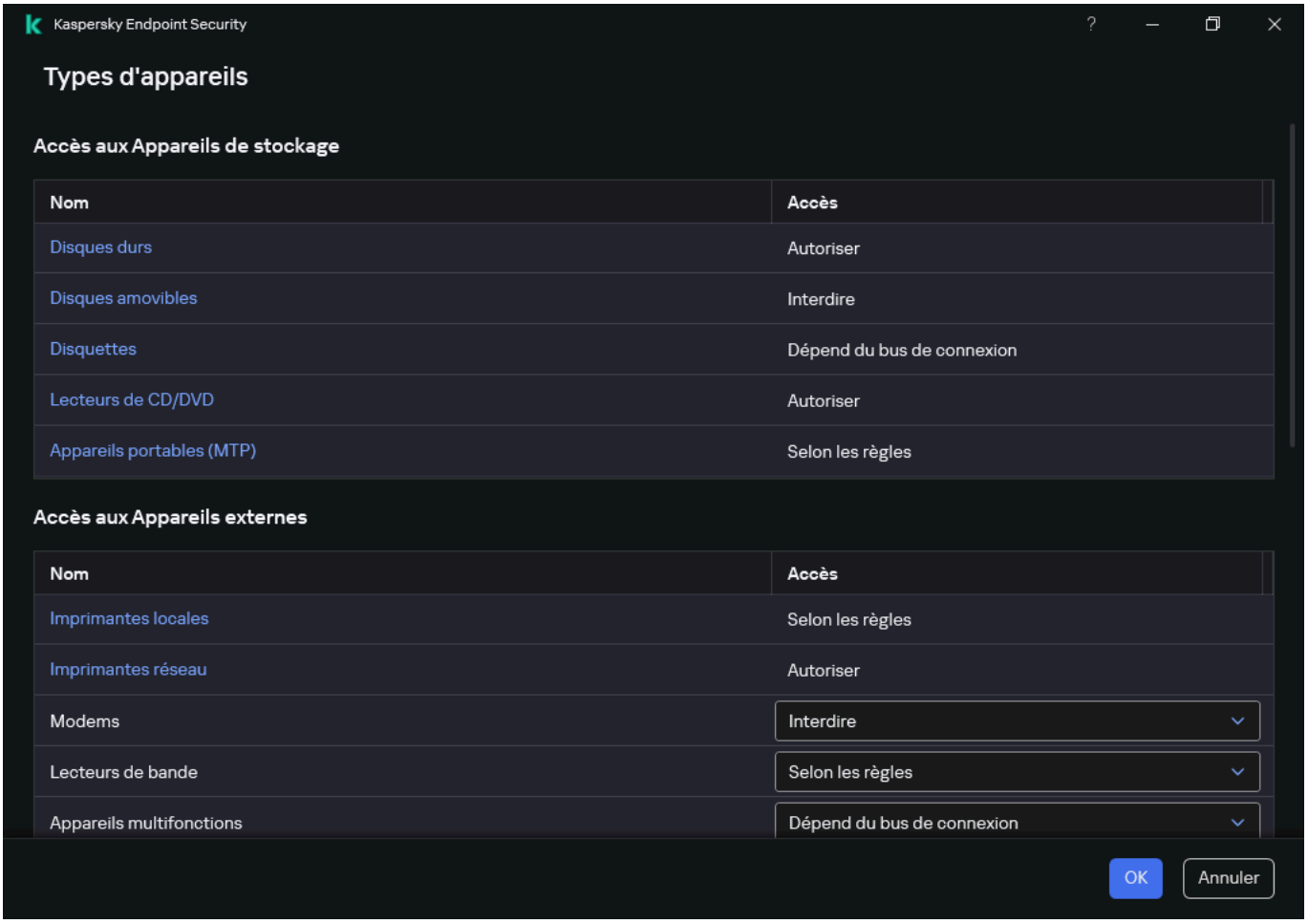
Comment configurer les règles d'accès aux appareils mobiles dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Appareils et réseaux Wi-Fi** dans le groupe **Paramètres d'accès**.

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.



Types d'appareils dans le module Contrôle des appareils

4. Dans le groupe **Accès aux Appareils de stockage**, cliquez sur le lien **Appareils portables (MTP)**.

   Cette action ouvre une fenêtre contenant les règles d'accès aux appareils portables (MTP).

5. Sous **Accès**, configurez le mode d'accès aux appareils mobiles : **Autoriser**, **Bloquer**, **Dépend du bus de connexion** ou **Selon les règles**.

6. Si vous sélectionnez le mode **Selon les règles**, vous devez ajouter des règles d'accès pour les appareils :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Droits des utilisateurs**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils mobiles.

   b. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

c. Sous **Condition**, activez la règle d'accès aux appareils mobiles.

d. Sous **Règles d'accès**, configurez les autorisations d'accès aux appareils mobiles pour les utilisateurs.

- Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

- Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

  Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

e. Sous **Utilisateurs**, sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès aux appareils mobiles. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

f. Sous **Planification de l'accès aux appareils**, configurez une planification d'accès aux appareils pour les utilisateurs.

> Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

g. Sous **Accès via iTunes**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

> Kaspersky Endpoint Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.

7. Enregistrez vos modifications.

L'accès des utilisateurs aux appareils mobiles est dès lors limité conformément aux règles. Si vous avez interdit l'accès aux appareils mobiles dans les applications ADB et iTunes, lorsque vous connectez un appareil mobile, les applications ADB et iTunes ne peuvent pas le détecter.

Appareils mobiles de confiance

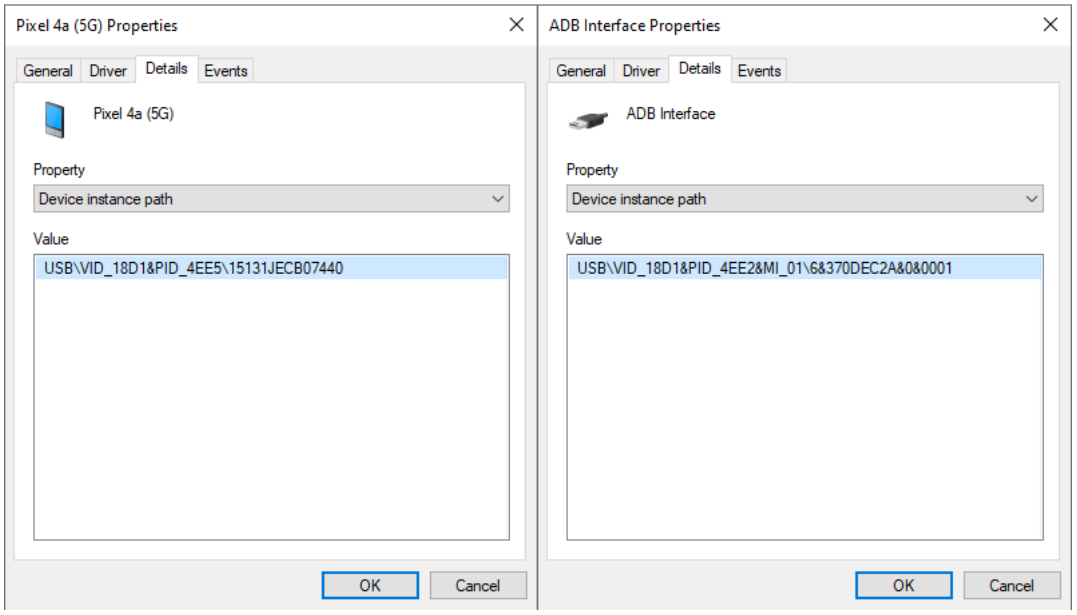
Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

La procédure d'ajout d'un appareil mobile de confiance est exactement la même que pour les autres types d'appareils de confiance. Vous pouvez ajouter un appareil mobile par identifiant ou par modèle d'appareil.

Pour ajouter un appareil mobile de confiance par identifiant, vous aurez besoin d'un identifiant unique (Hardware ID – HWID). Vous pouvez trouver l'identifiant dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). L'outil Gestionnaire des appareils vous permet de réaliser cette opération. Les identifiants des appareils portables (MTP) ainsi que des appareils ADB et iTunes sont différents même pour le même appareil mobile. L'identifiant d'un appareil portable (MTP) peut ressembler à ceci : `15131JECB07440`. L'identifiant d'un appareil ADB peut se présenter comme suit : `6&370DEC2A&0&0001`. L'ajout d'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers. Vous pouvez également utiliser des masques.

> 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.

Pour ajouter un appareil mobile de confiance par modèle d'appareil, vous avez besoin de son Vendor ID (VID) et de son Product ID (PID). Vous pouvez trouver les identifiants dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). Modèle de saisie du VID et du PID : `VID_18D1&PID_4EE5`. 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.



L'identifiant de l'appareil dans le Gestionnaire des appareils

Gestion de l'accès aux appareils Bluetooth

Kaspersky Endpoint Security permet de gérer l'accès aux appareils Bluetooth. Les appareils Bluetooth incluent les claviers, souris, casques, imprimantes sans fil, etc. Vous pouvez également utiliser le Bluetooth pour la communication, p. ex., avec un appareil mobile.

> Lorsque des appareils Bluetooth sont connectés ou déconnectés, l'application peut créer plusieurs événements sur l'appareil. La raison en est que le système d'exploitation peut détecter un appareil Bluetooth comme plusieurs appareils de types différents. Kaspersky Endpoint Security gère également l'adaptateur Bluetooth via lequel l'appareil est connecté en tant qu'appareil distinct. C'est pourquoi l'application crée un événement pour chacun des appareils détectés.

Vous pouvez sélectionner l'un des modes d'accès suivants aux appareils Bluetooth :

- **Autoriser et ne pas enregistrer** . Kaspersky Endpoint Security permet de connecter n'importe quel appareil Bluetooth et n'enregistre pas les informations sur la connexion dans le journal des événements. Vous pouvez connecter des appareils de saisie Bluetooth (claviers, souris, etc.), envoyer des données via Bluetooth ou encore gérer d'autres appareils Bluetooth (casque, écouteurs, etc.).

- **Autoriser** . Kaspersky Endpoint Security permet de connecter n'importe quel appareil Bluetooth. Vous pouvez connecter des appareils de saisie Bluetooth (claviers, souris, etc.), envoyer des données via Bluetooth ou encore gérer d'autres appareils Bluetooth (casque, écouteurs, etc.).

- **Interdire** . Kaspersky Endpoint Security restreint l'accès aux appareils Bluetooth. Vous pouvez autoriser la connexion uniquement aux appareils d'entrée Bluetooth (la classe Human Interface Devices). Ces appareils comprennent les claviers, les souris, les joysticks, etc.

Il n'est pas possible de créer une liste d'appareils Bluetooth de confiance. Si vous avez restreint l'accès aux appareils Bluetooth, vous ne pouvez connecter que des appareils d'entrée Bluetooth.

Comment configurer les règles d'accès aux appareils Bluetooth dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Dans le menu contextuel relatif au type d'appareil **Bluetooth**, configurez le mode d'accès aux appareils Bluetooth : **Autoriser** , **Interdire** ou **Autoriser et ne pas enregistrer** .

7. Si vous sélectionnez le mode **Interdire**, vous pouvez autoriser la connexion uniquement des appareils de saisie Bluetooth (claviers, souris, etc.). Pour ce faire, sous **Exclusions**, cochez la case **Appareils d'entrée (souris et claviers)**.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils Bluetooth dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans le groupe **Règles d'accès aux appareils**, cliquez sur le lien **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Sélectionnez le type d'appareil **Appareils Bluetooth**.

   Cette action ouvre les paramètres d'accès aux appareils Bluetooth.

7. Configurez le mode d'accès aux appareils Bluetooth : **Autoriser**, **Interdire**, **Autoriser et ne pas enregistrer**.

8. Si vous sélectionnez le mode **Interdire**, vous pouvez autoriser la connexion uniquement des appareils de saisie Bluetooth (claviers, souris, etc.). Pour ce faire, sous **Exclusions**, cochez la case **Appareils d'entrée (souris et claviers)**.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

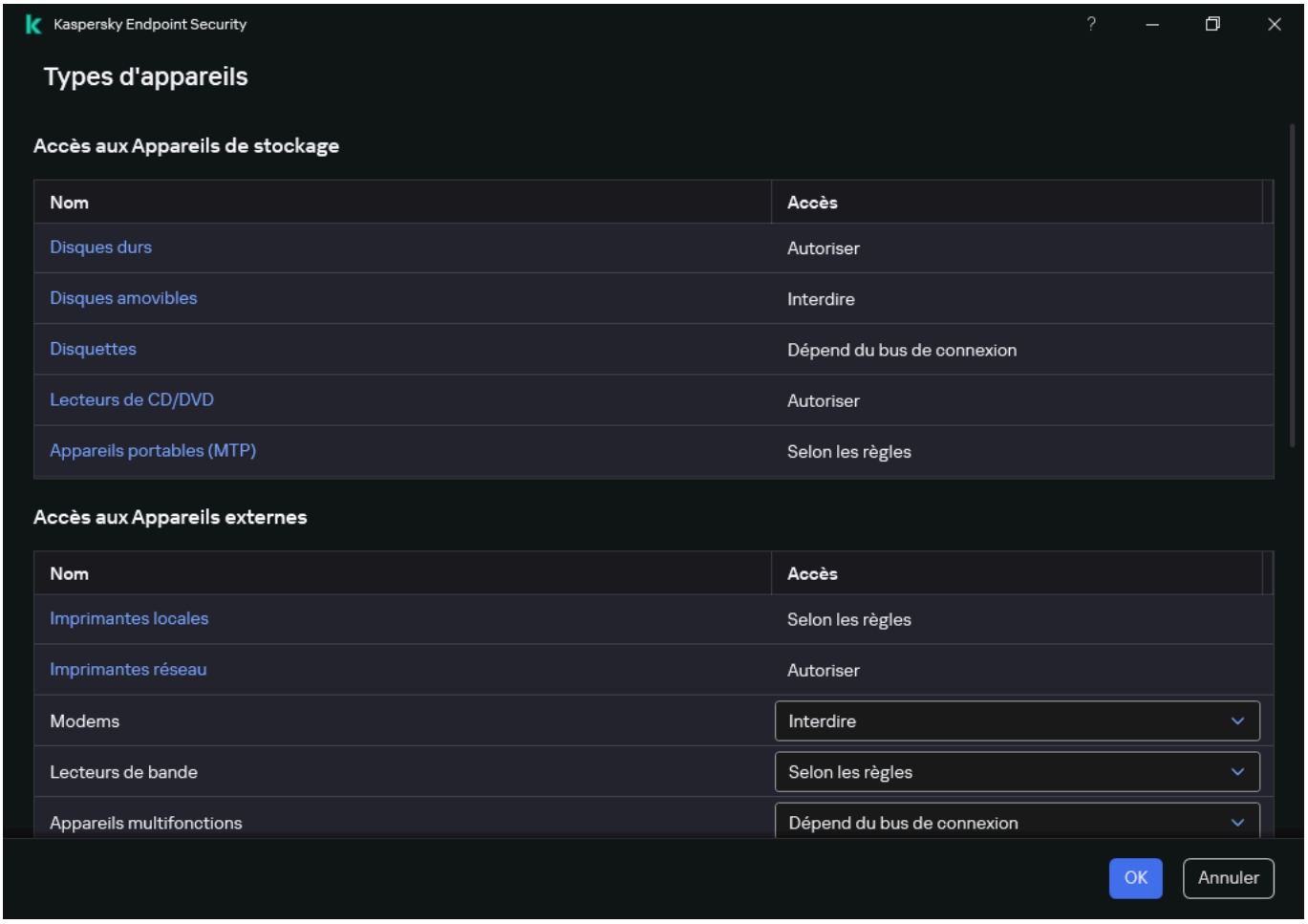
Comment configurer les règles d'accès aux appareils Bluetooth dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Appareils et réseaux Wi-Fi** dans le groupe **Paramètres d'accès**.

   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.



Types d'appareils dans le module Contrôle des appareils

4. Dans le groupe **Accès aux Appareils externes**, cliquez sur le lien **Bluetooth**.

   Cette action ouvre les paramètres d'accès aux appareils Bluetooth.

5. Sous **Accès**, configurez le mode d'accès aux appareils Bluetooth : **Autoriser**, **Bloquer**, **Autoriser et ne pas enregistrer**.

6. Si vous sélectionnez le mode **Bloquer**, vous pouvez autoriser la connexion uniquement des appareils de saisie Bluetooth (claviers, souris, etc.). Pour ce faire, sous **Exclusions**, cochez la case **Appareils d'entrée (souris et claviers)**.

7. Enregistrez vos modifications.

Contrôle de l'impression

La gestion de l'impression n'est pas prise en charge sur les ordinateurs basés sur l'architecture ARM.

Vous pouvez utiliser le contrôle de l'impression pour configurer l'accès des utilisateurs aux imprimantes locales et réseau.

Contrôle de l'imprimante locale

Kaspersky Endpoint Security permet de configurer l'accès aux imprimantes locales à deux niveaux : *connexion* et *impression*.

Kaspersky Endpoint Security contrôle la connexion de l'imprimante locale via les bus suivants : USB, Port série, Port parallèle (LPT).

Kaspersky Endpoint Security contrôle la connexion des imprimantes locales aux ports COM et LPT uniquement au niveau du bus. Ainsi, pour interdire la connexion de l'imprimante via les ports COM et LPT, il faut sélectionnez le mode d'accès Dépend du bus de connexion aux imprimantes locales et interdire les connexions aux bus COM et LPT.

Pour les imprimantes connectées en USB, l'application exerce un contrôle à deux niveaux : type d'appareil (imprimantes locales) et bus de connexion (USB).

Vous pouvez sélectionner l'un des modes d'accès suivants aux imprimantes locales via USB :

- **Autoriser** ✓. Kaspersky Endpoint Security accorde un accès complet aux imprimantes locales à tous les utilisateurs. Les utilisateurs peuvent connecter des imprimantes et imprimer des documents en utilisant les moyens que le système d'exploitation met à leur disposition.

- **Interdire** ⊘. Kaspersky Endpoint Security bloque la connexion des imprimantes locales. L'application ne permet de connecter que des imprimantes de confiance.

- **Dépend du bus de connexion**. Kaspersky Endpoint Security autorise la connexion aux imprimantes locales en fonction de l'état de la connexion au bus USB (**Autoriser** ou **Interdire**).

- **Selon les règles**. Pour contrôler l'impression, vous devez ajouter *des règles d'impression*. Dans les règles, vous pouvez sélectionner les utilisateurs ou un groupe d'utilisateurs pour lesquels vous souhaitez autoriser ou bloquer l'accès à l'impression de documents sur des imprimantes locales.

Contrôle des imprimantes réseau

Kaspersky Endpoint Security permet de configurer l'accès à l'impression sur les imprimantes réseau. Vous pouvez sélectionner l'un des modes d'accès suivants sur les imprimantes réseau :

- **Autoriser et ne pas enregistrer**. Kaspersky Endpoint Security ne contrôle pas l'impression sur les imprimantes réseau. L'application accorde l'accès à l'impression à tous les utilisateurs et n'enregistre pas les informations sur l'impression dans le journal des événements.

- **Autoriser**. Kaspersky Endpoint Security accorde l'accès à l'impression sur les imprimantes du réseau à tous les utilisateurs.

- **Interdire**. Kaspersky Endpoint Security limite l'accès aux imprimantes réseau pour tous les utilisateurs. L'application n'autorise l'accès qu'aux imprimantes de confiance.

- **Selon les règles**. Kaspersky Endpoint Security accorde l'accès à l'impression conformément aux règles d'impression. Dans les règles, vous pouvez sélectionner les utilisateurs ou un groupe d'utilisateurs qui seront autorisés à imprimer des documents sur l'imprimante réseau ou qui ne pourront pas le faire.

Ajout de règles d'impression pour les imprimantes

Comment ajouter des règles d'impression dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

4. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

5. Dans le menu contextuel **Imprimantes locales** and **Imprimantes réseau**, configurez le mode d'accès pour les imprimantes concernées : **Autoriser**, **Interdire**, **Autoriser et ne pas enregistrer** (pour les imprimantes réseau uniquement) ou **Dépend du bus de connexion** (pour les imprimantes locales uniquement).

6. Pour configurer les règles d'impression sur les imprimantes locales et réseau, double-cliquez sur les listes de règles pour les ouvrir.

7. Sélectionnez **Selon les règles** comme mode d'accès à l'imprimante.

8. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle d'impression.

   a. Cliquez sur **Ajouter**.

      Une fenêtre s'ouvre pour ajouter une nouvelle règle d'impression.

   b. Attribuez une priorité à l'entrée de la règle. Une entrée de règle comprend les attributs suivants : compte utilisateur, action (autoriser/bloquer) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

   c. Sous **Action**, configurez l'accès de l'utilisateur à l'impression sur l'imprimante.

   d. Cliquez sur **Utilisateurs et groupes** et sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   e. Cliquez sur **OK**.

9. Enregistrez vos modifications.

Comment ajouter des règles d'impression dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans le groupe **Règles d'accès aux appareils**, cliquez sur le lien **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Sélectionnez le type d'appareil **Imprimantes locales** ou **Imprimantes réseau**.

   Les règles d'accès à l'imprimante s'ouvrent.

7. Configurez le mode d'accès pour les imprimantes concernées : **Autoriser**, **Interdire**, **Autoriser et ne pas enregistrer** (pour les imprimantes réseau uniquement), **Dépend du bus** (pour les imprimantes locales uniquement) ou **Personnalisé**.

8. Si vous sélectionnez le mode **Personnalisé**, vous devez ajouter des règles d'impression pour les imprimantes locales ou réseau. Pour ce faire, cliquez sur le bouton **Ajouter** dans le tableau des règles d'impression.

   Les paramètres de la nouvelle règle d'impression s'affichent.

9. Attribuez une priorité à l'entrée de la règle. Une entrée de règle comprend les attributs suivants : compte utilisateur, action (autoriser/bloquer) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

10. Sous **Action**, configurez l'accès de l'utilisateur à l'impression sur l'imprimante.

11. Sous **Utilisateur ou groupe**, sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

12. Enregistrez vos modifications.

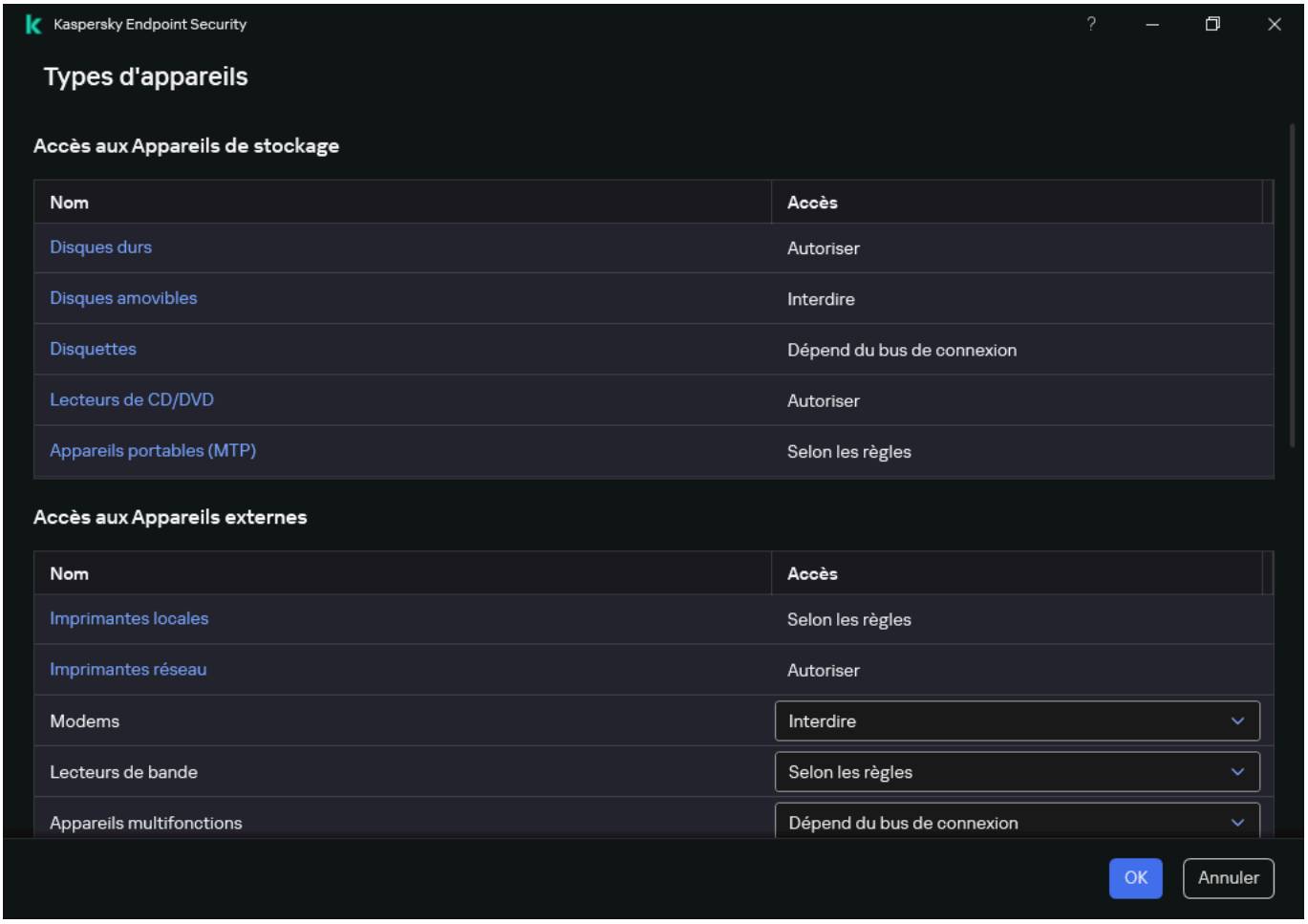
Comment ajouter des règles d'impression dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Appareils et réseaux Wi-Fi** dans le groupe **Paramètres d'accès**.

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.



Types d'appareils dans le module Contrôle des appareils

4. En dessous de **Accès aux Appareils externes**, cliquez sur **Imprimantes locales** ou **Imprimantes réseau**.

   Une fenêtre s'ouvre avec les règles d'accès à l'imprimante.

5. Sous **Accès aux imprimantes locales** ou **Accès aux imprimantes réseau**, configurez le mode d'accès aux imprimantes : **Autoriser**, **Bloquer**, **Autoriser et ne pas enregistrer** (pour les imprimantes réseau uniquement), **Dépend du bus de connexion** (pour les imprimantes locales uniquement) ou **Selon les règles**.

6. Si vous sélectionnez le mode **Selon les règles**, vous devez ajouter des règles d'impression pour les imprimantes. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle d'impression.

   a. Cliquez sur **Ajouter**.

      Une fenêtre s'ouvre pour ajouter une nouvelle règle d'impression.

   b. Attribuez une priorité à l'entrée de la règle. Une entrée de règle comprend les attributs suivants : compte utilisateur, autorisations (autoriser/bloquer) 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 vous permet d'attribuer une priorité comprise entre 0 et 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.

c. Sous **Action**, configurez les autorisations d'utilisateur pour l'accès à l'impression.

d. Sous **Utilisateurs et groupes**, sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

7. Enregistrez vos modifications.

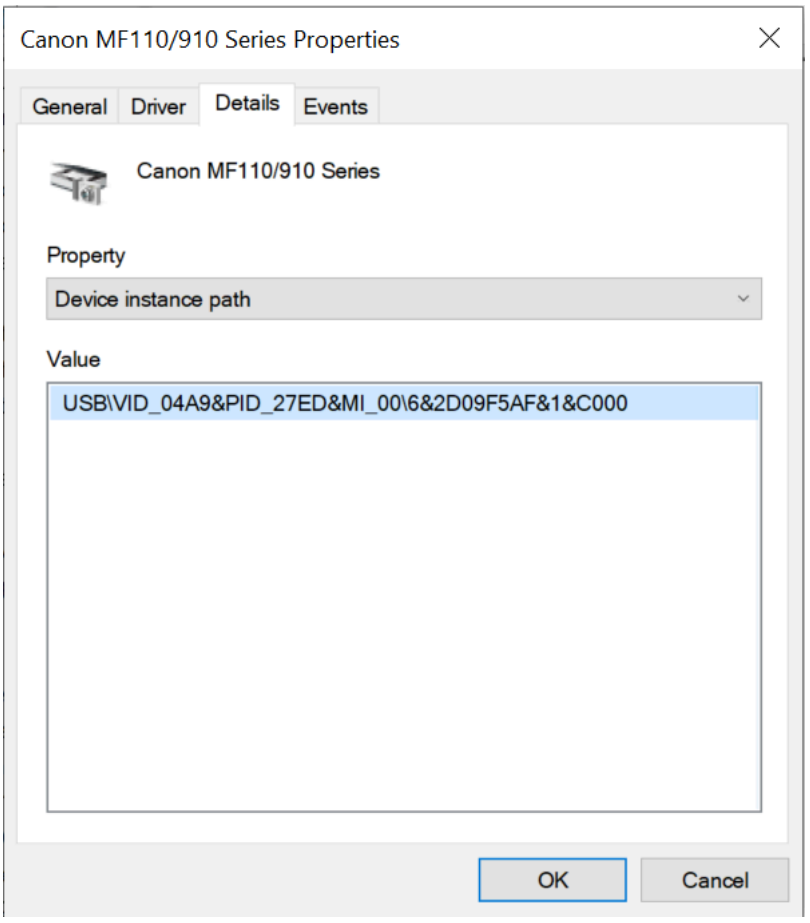
Imprimantes de confiance

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.

La procédure d'ajout d'imprimantes de confiance est exactement la même que pour les autres types d'appareils de confiance. Vous pouvez ajouter des imprimantes locales par identifiant ou par modèle d'appareil. Vous ne pouvez ajouter des imprimantes réseau que par identifiant d'appareil.

Pour ajouter une imprimante locale de confiance par identifiant, vous aurez besoin d'un identifiant unique (Hardware ID – HWID). Vous pouvez trouver l'identifiant dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). L'outil Device Manager vous permet de réaliser cette opération. L'identifiant d'une imprimante locale peut se présenter comme suit : `6&2D09F5AF&1&C000`. L'ajout d'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers. Vous pouvez également utiliser des masques.

Pour ajouter une imprimante locale de confiance par modèle d'appareil, vous avez besoin de son Vendor ID (VID) et de son Product ID (PID). Vous pouvez trouver les identifiants dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). Modèle de saisie du VID et du PID : `VID_04A9&PID_27FD`. 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.



L'identifiant de l'appareil dans le Gestionnaire des appareils

Pour ajouter une imprimante réseau de confiance, vous avez besoin de l'identifiant de l'appareil. Pour les imprimantes réseau, l'identifiant de l'appareil peut être le nom réseau de l'imprimante (nom de l'imprimante partagée), l'adresse IP de l'imprimante ou l'URL de l'imprimante.

Contrôle des connexions Wi-Fi

Le Contrôle des appareils permet de gérer la connexion Wi-Fi de l'ordinateur (portable). Les réseaux Wi-Fi publics peuvent être non sécurisés, et leur utilisation peut entraîner une perte de données. Le Contrôle des appareils vous permet de bloquer la connexion d'un utilisateur au réseau Wi-Fi ou de l'autoriser à se connecter uniquement aux réseaux de confiance. Par exemple, vous pouvez autoriser la connexion uniquement au réseau Wi-Fi de l'entreprise qui est suffisamment sécurisé. 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.

Sur les ordinateurs fonctionnant sous Windows 11, vous devez activer le service de localisation pour contrôler les connexions Wi-Fi. Pour ce faire, vous devez activer le **Services d'emplacement** dans les paramètres du système d'exploitation (**Paramètres** → **Confidentialité & sécurité** → **Emplacement**). Si le service de localisation est désactivé, Kaspersky Endpoint Security ne contrôle pas la connexion aux réseaux Wi-Fi.

Comment limiter les connexions Wi-Fi dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

4. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

5. Dans le menu contextuel du type d'appareil **Wi-Fi** sélectionnez l'action du Contrôle des appareils qui est prise lors de la connexion au réseau Wi-Fi : **Autoriser** (✓), **Interdire** (⊘), ou **Interdire avec des exceptions** (▤).

6. Si vous choisissez l'option **Interdire avec des exceptions**, créez une liste de réseaux Wi-Fi de confiance :

   a. Double-cliquez pour ouvrir la liste des réseaux Wi-Fi de confiance.

   b. Cliquez sur le bouton **Ajouter** dans le groupe **Réseaux Wi-Fi de confiance**.

   c. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance (voir la figure ci-dessous) :

   - **Nom du réseau**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.

   - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.

     > À partir de la version 12.0 de Kaspersky Endpoint Security for Windows, le protocole WPA3 est pris en charge dans l'application. Si une stratégie de Kaspersky Endpoint Security version 12.2 est appliquée sur un ordinateur, le protocole WPA2 est sélectionné sur les ordinateurs disposant de Kaspersky Endpoint Security version 11.11.0 ou une version antérieure ; le protocole WPA2 / WPA3 est sélectionné pour les versions 12.0 à 12.1 ; le protocole WPA3 est sélectionné pour les versions 12.2 et les versions ultérieures.

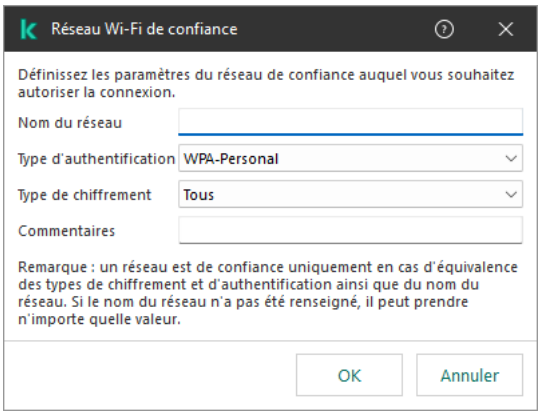
   - **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.

   - **Commentaires**. Plus d'informations sur le réseau Wi-Fi ajouté.

   Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

   > Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

7. Enregistrez vos modifications.



Paramètres du réseau Wi-Fi de confiance

Comment limiter les connexions Wi-Fi dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Sous les **Règles d'accès aux appareils**, sélectionnez l'onglet **Appareils et réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Dans le groupe **Réseaux Wi-Fi**, cliquez sur le lien **Wi-Fi**.

7. Dans la fenêtre qui s'ouvre, sélectionnez l'action du Contrôle des appareils prise lors de la connexion au réseau Wi-Fi : **Autoriser**, **Interdire** ou **Interdire avec des exclusions**.

8. Si vous choisissez l'option **Interdire avec des exclusions**, créez une liste de réseaux Wi-Fi de confiance :

   a. Double-cliquez pour ouvrir la liste des réseaux Wi-Fi de confiance.

   b. Cliquez sur le bouton **Ajouter** dans le groupe **Réseaux Wi-Fi de confiance**.

   c. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance (voir la figure ci-dessous) :

   - **Nom**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.

   - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.

     À partir de la version 12.0 de Kaspersky Endpoint Security for Windows, le protocole WPA3 est pris en charge dans l'application. Si une stratégie de Kaspersky Endpoint Security version 12.2 est appliquée sur un ordinateur, le protocole WPA2 est sélectionné sur les ordinateurs disposant de Kaspersky Endpoint Security version 11.11.0 ou une version antérieure ; le protocole WPA2 / WPA3 est sélectionné pour les versions 12.0 à 12.1 ; le protocole WPA3 est sélectionné pour les versions 12.2 et les versions ultérieures.

- **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.
- **Commentaires**. Plus d'informations sur le réseau Wi-Fi ajouté.

Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

> Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

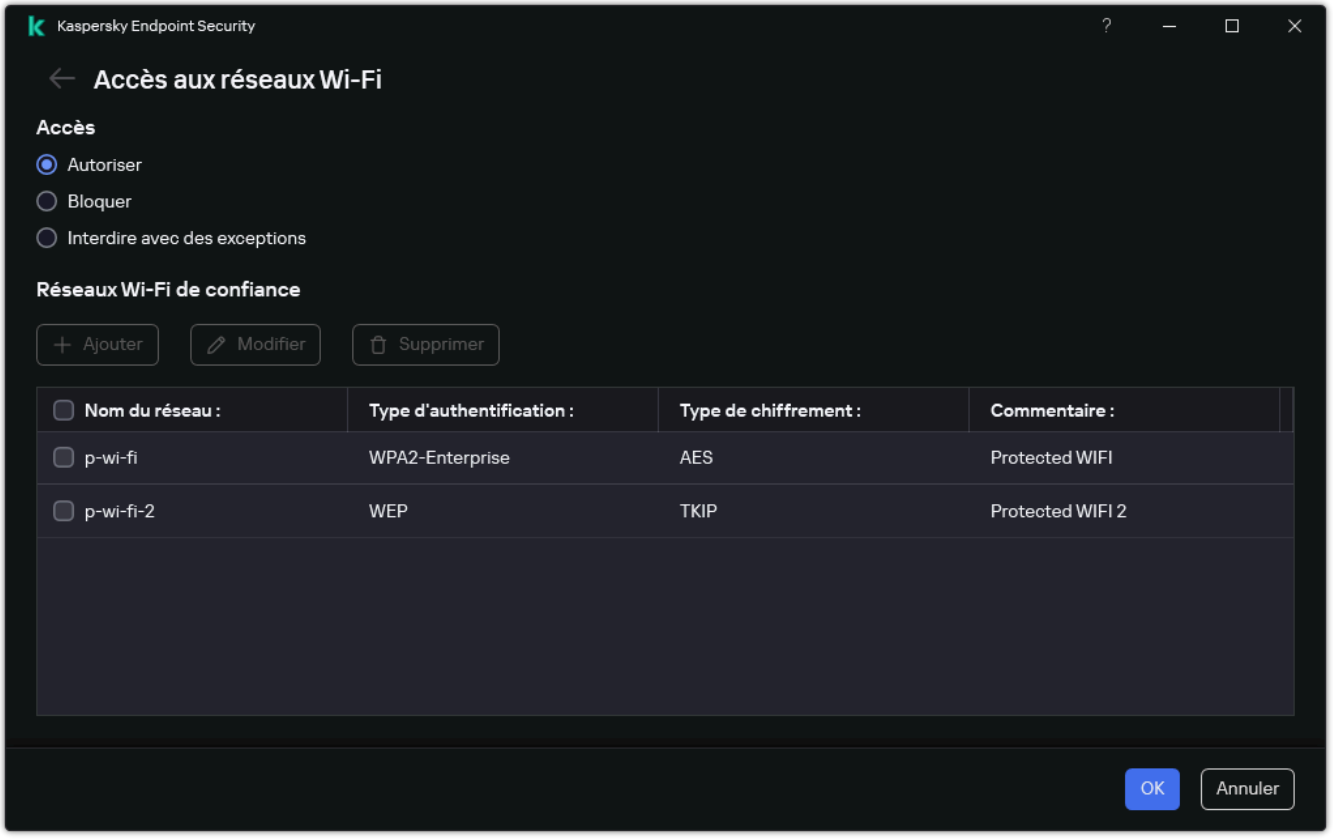
9. Enregistrez vos modifications.

Comment limiter les connexions Wi-Fi 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 **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Appareils et réseaux Wi-Fi** dans le groupe **Paramètres d'accès**.

   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.



Paramètres d'accès Wi-Fi

5. Sous **Accès**, sélectionnez l'action du Contrôle des appareils prise lors de la connexion au réseau Wi-Fi : **Autoriser**, **Bloquer**, ou **Interdire avec des exceptions**.

6. Si vous choisissez l'option **Interdire avec des exceptions**, créez une liste de réseaux Wi-Fi de confiance :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Réseaux Wi-Fi de confiance**.

   b. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance (voir la figure ci-dessous) :

   - **Nom du réseau**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.
   - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.

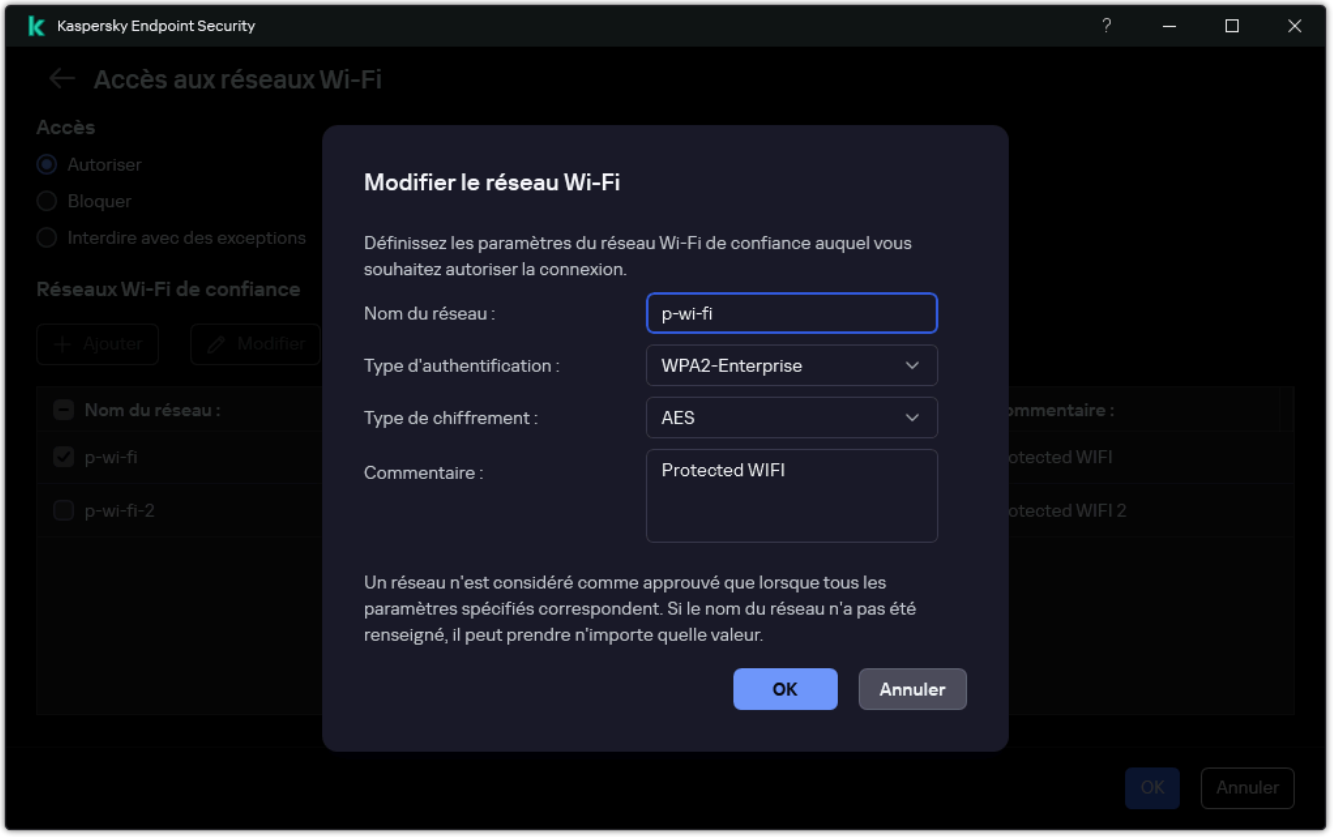
     À partir de la version 12.0 de Kaspersky Endpoint Security for Windows, le protocole WPA3 est pris en charge dans l'application. Si une stratégie de Kaspersky Endpoint Security version 12.2 est appliquée sur un ordinateur, le protocole WPA2 est sélectionné sur les ordinateurs disposant de Kaspersky Endpoint Security version 11.11.0 ou une version antérieure ; le protocole WPA2 / WPA3 est sélectionné pour les versions 12.0 à 12.1 ; le protocole WPA3 est sélectionné pour les versions 12.2 et les versions ultérieures.

   - **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.
   - **Commentaire**. Plus d'informations sur le réseau Wi-Fi ajouté.

   Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

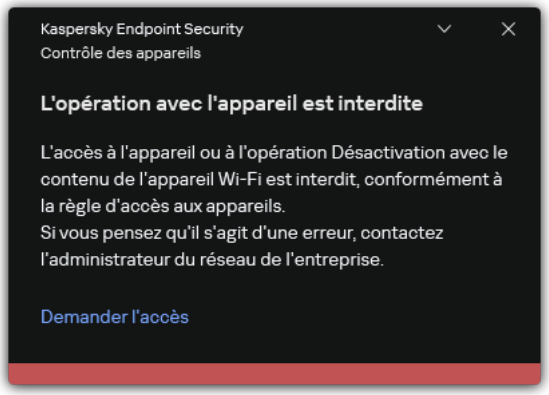
   Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

7. Enregistrez vos modifications.



Paramètres du réseau Wi-Fi de confiance

Par conséquent, lorsqu'un utilisateur tente de se connecter à un réseau Wi-Fi qui n'est pas répertorié comme étant de confiance, l'application bloque la connexion et affiche une notification (voir la figure ci-dessous).



Notification du Contrôle des appareils

Surveillance de l'utilisation des disques amovibles

La surveillance de l'utilisation des disques amovibles comprend :

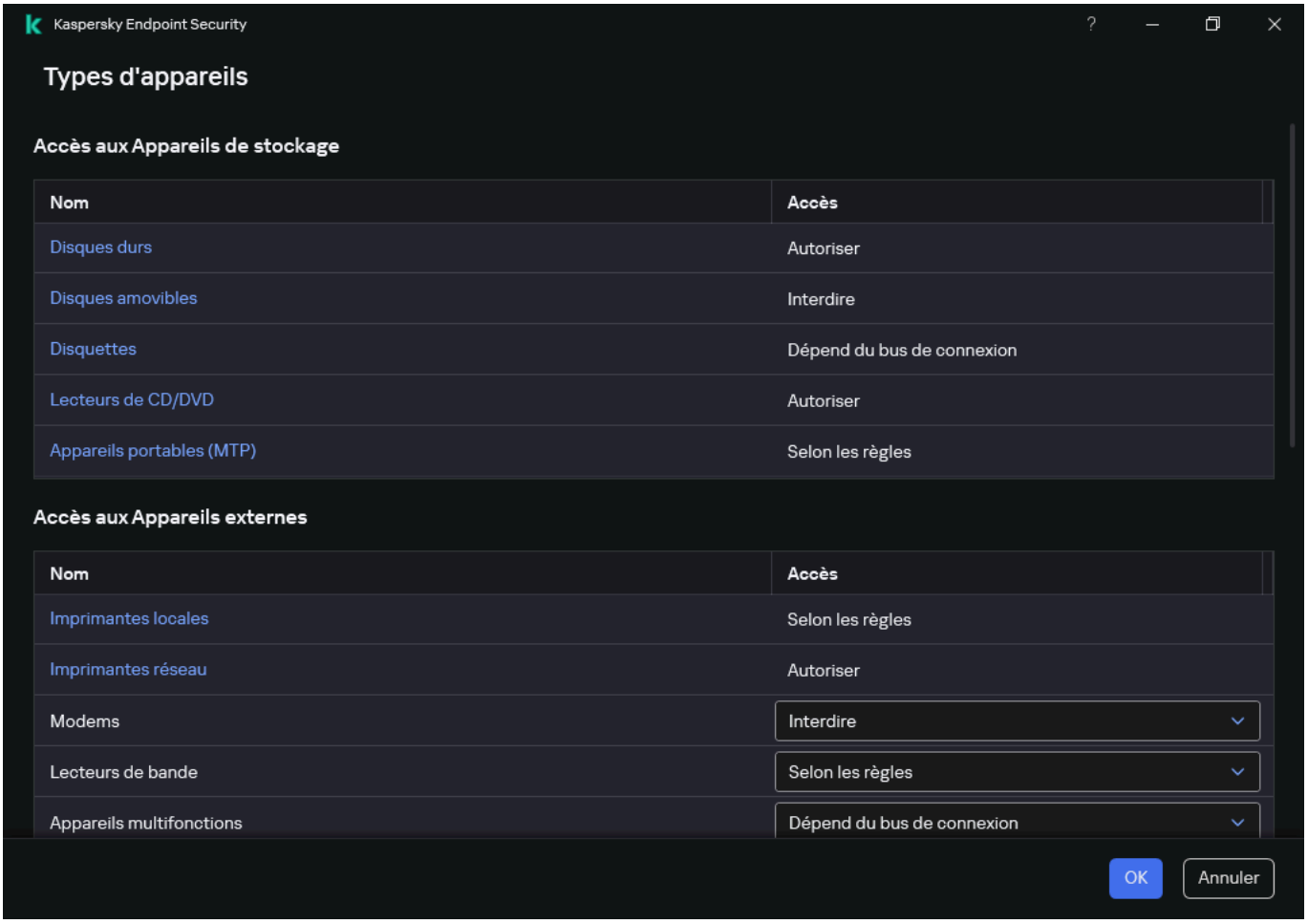
- La surveillance des opérations exécutées sur les fichiers des disques amovibles.
- La surveillance de la connexion et de la déconnexion des disques amovibles de confiance.

  Kaspersky Endpoint Security permet de surveiller la connexion et la déconnexion de tous les appareils de confiance et pas seulement des disques amovibles. Vous pouvez activer la enregistrement des événements dans le journal dans les paramètres de notification du module Contrôle des appareils. Les événements présentent le niveau de gravité *Message d'information*.

Pour permettre la surveillance de l'utilisation des disques amovibles, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Appareils et réseaux Wi-Fi** dans le groupe **Paramètres d'accès**.

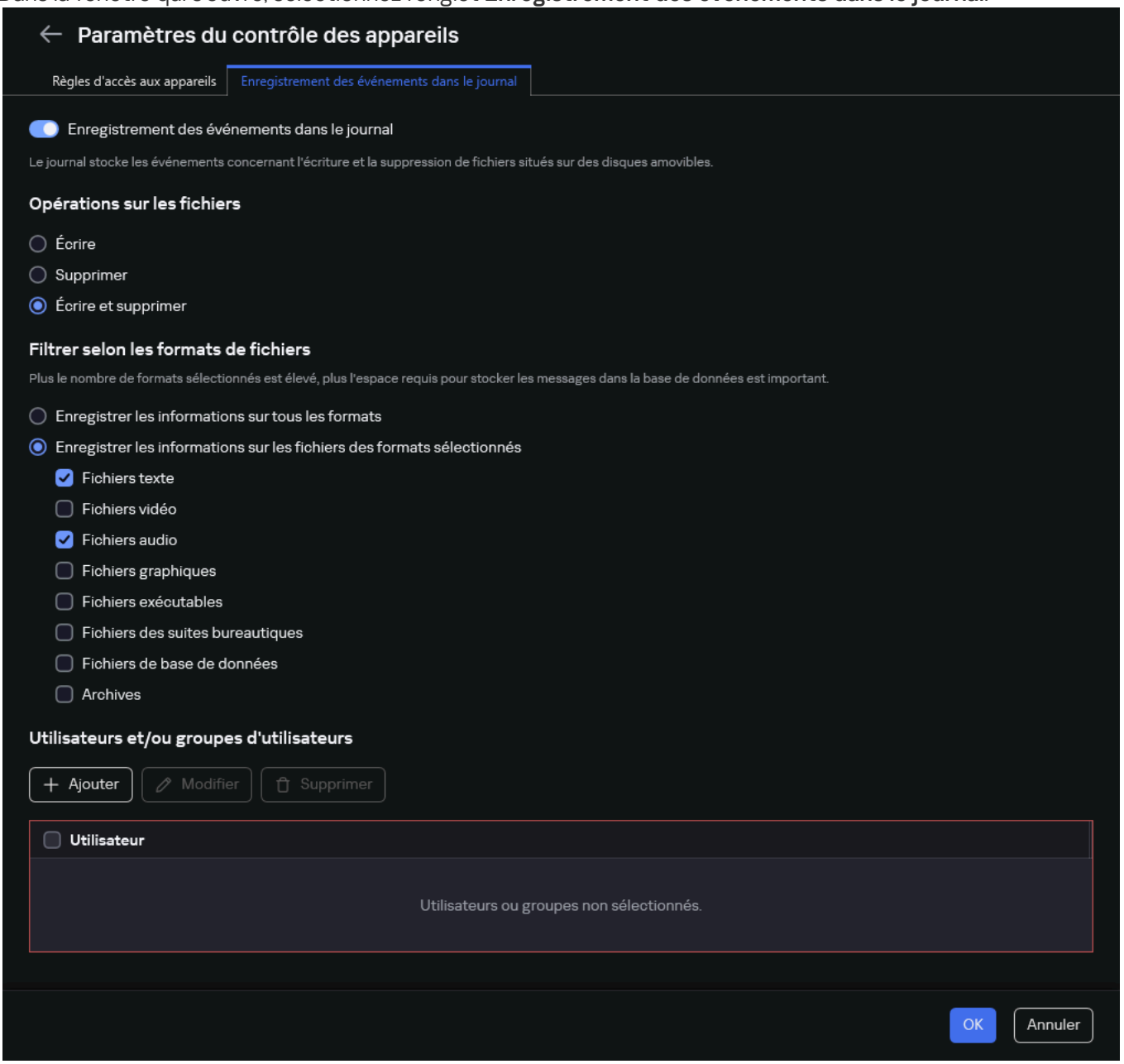
La fenêtre qui s'ouvre présente les règles d'accès pour tous les appareils qui sont inclus dans la classification des modules du Contrôle des appareils.



Types d'appareils dans le module Contrôle des appareils

4. Dans le groupe **Accès aux Appareils de stockage**, sélectionnez l'option **Disques amovibles**.

5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Enregistrement des événements dans le journal**.



Les paramètres de surveillance de l'utilisation des disques amovibles

6. Activez le commutateur **Enregistrement des événements dans le journal**.

7. Dans le groupe **Opérations sur les fichiers**, sélectionnez les opérations que vous voulez surveiller : **Écrire**, **Supprimer**.

8. Dans le groupe **Filtrer selon les formats de fichiers**, sélectionnez les formats des fichiers dont les opérations associées doivent être enregistrées par le Contrôle des appareils.

9. Sélectionnez les utilisateurs ou le groupe d'utilisateurs dont vous souhaitez surveiller l'utilisation des disques amovibles.

10. Enregistrez vos modifications.

Par conséquent, lorsque les utilisateurs génèreront 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
- 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.14.2\environment`
   - Pour les systèmes d'exploitation 32 bits :
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\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.

Il n'est pas recommandé d'ajouter plus de 5000 appareils de confiance, car cela peut entraîner une instabilité du système.

Kaspersky Endpoint Security permet d'ajouter un appareil à la liste de confiance des manières suivantes :

- Si Kaspersky Security Center n'est pas déployé 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 permet de contrôler l'utilisation des appareils de confiance (connexion et déconnexion). Vous pouvez activer la enregistrement des événements dans le journal dans les paramètres de notification du module Contrôle des appareils. Les événements présentent le niveau de gravité *Messages d'information*.

Ajout d'un appareil à la liste des appareils de confiance

Kaspersky Security Center reçoit des informations relatives aux appareils si Kaspersky Endpoint Security est installé sur les ordinateurs, si le Contrôle des appareils est activé et si la transmission des données des appareils est activée. 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.

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.

Vous pouvez ajouter un appareil à la liste des appareils de confiance en fonction des données suivantes :

- **Appareils en fonction de l'identifiant**. 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'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers.

- **Appareils en fonction du modèle**. Chaque appareil possède un Vendor ID (VID) et un 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 ajouter des appareils à la liste 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 des PID similaires (par exemple, des appareils du même fabricant), vous pouvez ajouter des appareils à la liste 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_*`.

Comment ajouter un appareil à la liste des appareils de confiance dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Appareils de confiance**.

6. 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.

7. Cliquez sur le bouton **Ajouter** et sélectionnez une méthode pour ajouter un appareil à la liste des appareils de confiance.

8. Pour filtrer les appareils, sélectionnez un type d'appareil dans la liste déroulante **Type d'appareil** (par exemple, **Disques amovibles**).

   > Kaspersky Endpoint Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.

9. 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 le même temps, la liste des appareils dans Kaspersky Security Center reste vide lorsque vous cliquez sur le bouton **Mettre à jour**. Pour afficher correctement la liste des appareils, vous pouvez utiliser la méthode d'ajout d'un identifiant d'appareil selon un masque.

10. 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.

11. Cliquez sur **Mettre à jour**.

    Le tableau affiche une liste d'appareils qui satisfont aux paramètres de filtrage spécifiés.

12. Cochez les cases en regard des noms des appareils que vous souhaitez ajouter à la liste des appareils de confiance.

13. Dans le champ **Commentaires**, saisissez une description de la raison de l'ajout des appareils à la liste de confiance.

14. À droite du champ **Autoriser les utilisateurs et/ou les groupes d'utilisateurs**, cliquez sur le bouton **Sélectionner**.

    Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

    Par défaut, l'accès aux appareils de confiance est autorisé pour le groupe Tous.

15. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment ajouter un appareil à la liste des appareils de confiance dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zone de confiance**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Appareils**.

   Une fenêtre reprenant la liste des appareils de confiance s'ouvre.

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 **Ajouter**.

   Le formulaire d'ajout d'un appareil de confiance s'ouvre.

9. Sous **Utilisateur ou groupe**, sélectionnez les utilisateurs auxquels vous souhaitez autoriser l'accès aux appareils de confiance.

   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   Par défaut, l'accès aux appareils de confiance est autorisé pour le groupe Tous.

10. Pour filtrer les appareils, sélectionnez un type d'appareil dans la liste déroulante **Type d'appareil** (par exemple, **Disques amovibles**).

    > Kaspersky Endpoint Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.

11. Si vous ne connaissez pas l'identifiant exact ou le modèle exact de l'appareil, cochez la case **Utiliser un masque**.

12. Sélectionnez la manière dont vous souhaitez ajouter l'appareil : par identifiant ou par modèle d'appareil (VID et PID).

    > 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 le même temps, la liste vide des appareils s'affiche dans Kaspersky Security Center. Pour afficher correctement la liste des appareils, vous pouvez utiliser la méthode d'ajout d'un identifiant d'appareil selon un masque.

13. Pour filtrer les appareils, saisissez dans le champ **Rechercher des appareils de confiance** 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.

    Le tableau affiche une liste d'appareils qui satisfont aux paramètres de filtrage spécifiés.

14. Cochez les cases en regard des noms des appareils que vous souhaitez ajouter à la liste des appareils de confiance.

15. Dans le champ **Commentaires**, saisissez une description de la raison de l'ajout des appareils à la liste de confiance.

16. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment ajouter un appareil à la liste des appareils de confiance 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 **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Appareils de confiance** dans le groupe **Paramètres d'accès**.

   Cette action permet d'exporter une liste d'appareils de confiance.

4. Cliquez sur **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.

   > Kaspersky Endpoint Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.

6. Dans le champ **Commentaire**, 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.

   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

8. 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Appareils de confiance** dans le groupe **Paramètres d'accès**.

   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 **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. Enregistrez le fichier.

      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. Ouvrez le fichier.

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 reçoit un message avec la demande dans la console Kaspersky Security Center.

   La console Kaspersky Security Center dispose d'une sélection d'événements prédéfinis *Requêtes des utilisateurs* pour faciliter le suivi facile des messages des utilisateurs.
3. 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.
4. L'administrateur met à jour les paramètres de Kaspersky Endpoint Security sur l'ordinateur de l'utilisateur.

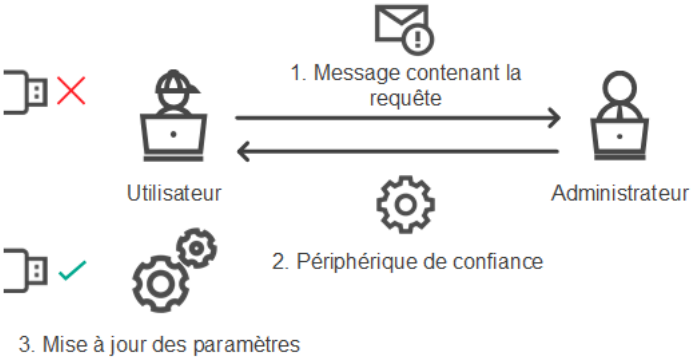


Schéma de l'octroi de l'accès à un appareil en mode en ligne

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 les demandes 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.

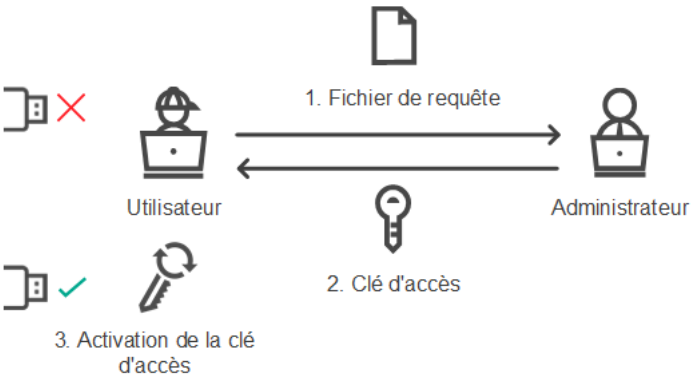


Schéma d'accès à l'appareil en mode hors ligne

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 :

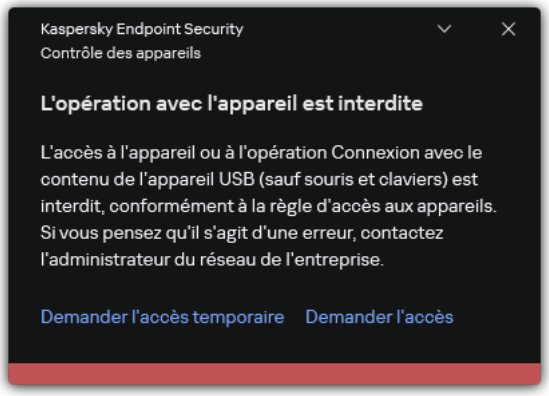
1. Connectez l'appareil à l'ordinateur.

   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**.

   Cette action ouvre une fenêtre avec un message pour l'administrateur. Le message contient des informations relatives à l'appareil bloqué.

3. Cliquez sur **Envoyer**.



Notification du Contrôle des appareils

Ensuite, l'administrateur de la console de Kaspersky Security Center reçoit l'événement *Message envoyé à l'administrateur sur l'interdiction de l'accès à l'appareil*. L'événement contient le nom d'utilisateur, le nom de l'ordinateur, des informations sur l'appareil auquel l'utilisateur tente d'accéder ainsi que d'autres informations. Vous pouvez configurer la manière dont l'administrateur est informé de ces événements et, par exemple, choisir de recevoir des notifications par email. La console Kaspersky Security Center dispose d'une sélection d'événements prédéfinis *Requêtes des utilisateurs* pour faciliter le suivi facile des messages des utilisateurs.

Pour autoriser l'accès, vous devez ajouter l'appareil à la liste de confiance. Après avoir mis à jour les paramètres de Kaspersky Endpoint Security sur l'ordinateur, l'utilisateur peut accéder à l'appareil.

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 les demandes 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**.

   Une fenêtre reprenant la liste des appareils connectés s'ouvre.

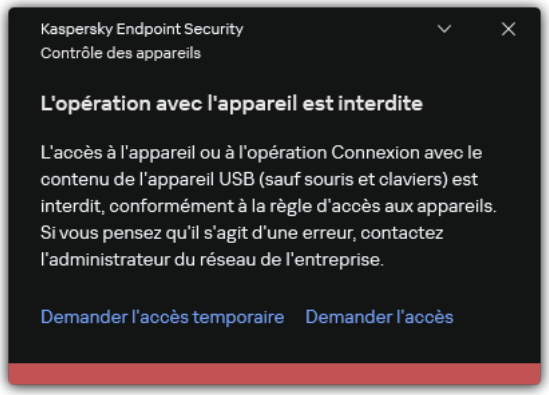
3. Sélectionnez dans la liste des appareils connectés celui auquel vous souhaitez accéder.

4. Cliquez sur **Créer un fichier de requête**.

5. Indiquez dans le champ **Durée de l'accès** 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

Comment l'administrateur peut créer une clé d'accès pour l'appareil bloqué 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. 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. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez 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**.

   Par défaut, le paramètre **Durée de l'accès** 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.

Comment l'administrateur peut créer une clé d'accès pour l'appareil bloqué dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Dans la liste des postes clients, sélectionnez l'ordinateur à l'utilisateur duquel vous souhaitez octroyer un accès temporaire à l'appareil bloqué.
3. Cliquez sur le bouton points de suspension (**...**) au-dessus de la liste des ordinateurs, puis cliquez sur le bouton **Autoriser l'accès à l'appareil en mode déconnecté**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la section **Contrôle des appareils**.
5. Cliquez sur le bouton **Aperçu** 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.
6. Le cas échéant, modifiez la valeur du paramètre **Durée d'accès (heures)**.

   Par défaut, le paramètre **Durée d'accès (heures)** prend la valeur définie par l'utilisateur lors de la création du fichier de demande.

7. Spécifiez la période pendant laquelle la clé d'accès peut être activée sur l'appareil.

   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.

8. 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

3. Cliquez sur le bouton **Demande d'accès à l'appareil** dans le groupe **Demande d'accès**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Activer la clé d'accès**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier avec la clé d'accès à l'appareil envoyé par l'administrateur du réseau local de l'entreprise.

   Une fenêtre reprenant des informations sur l'accès octroyé s'ouvre.

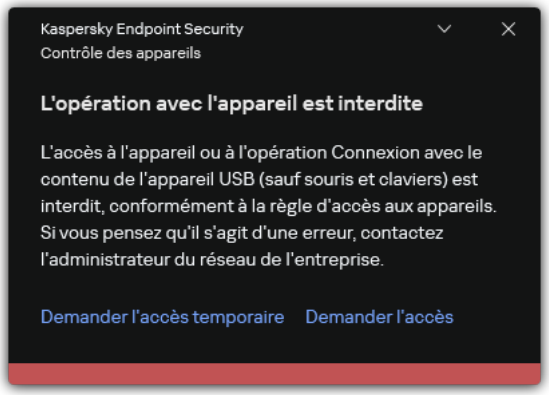
6. Cliquez sur **OK**.

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. Les experts de Kaspersky fournissent un modèle de message à l'utilisateur décrivant les raisons pour lesquelles l'accès à l'appareil a été bloqué (voir la figure ci-dessous).

Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.



Notification du Contrôle des appareils

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. Pour ce faire, l'utilisateur doit cliquer sur le bouton **Demander l'accès** ou **Demander l'accès temporaire** et envoyer un message à l'administrateur en décrivant la situation. Vous pouvez également préparer un modèle de message destiné à l'administrateur, en y ajoutant des informations susceptibles d'éclairer votre décision d'autoriser ou de bloquer l'accès à l'appareil. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à l'appareil**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Comment modifier les modèles des messages du Contrôle des appareils dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.

4. Cliquez sur le bouton **Modèles** dans le groupe **Paramètres des modèles de notification**.

5. Cela ouvre une fenêtre ; dans cette fenêtre, configurez les modèles du Contrôle des applications :

   - **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 pour 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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Variable** et sélectionnez la variable requise dans la liste des options disponibles.

Vous pouvez également restaurer le texte du modèle par défaut.

6. Enregistrez vos modifications.

Comment modifier les modèles des messages du Contrôle des appareils dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des appareils**.

5. Dans le groupe **Modèles de messages**, configurez les modèles pour les messages du Contrôle des applications :

   - **Message pour l'utilisateur**. 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 pour 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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut.

6. Enregistrez vos modifications.

Comment modifier les modèles des messages du Contrôle des appareils 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 **Contrôles de sécurité** → **Contrôle des applications**.

3. Dans le groupe **Modèles des messages**, configurez les modèles pour les messages du Contrôle des applications :

   - **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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Anti-Bridging** dans le groupe **Paramètres d'accès**.
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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Anti-Bridging** dans le groupe **Paramètres d'accès**.
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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des appareils**.
3. Cliquez sur le bouton **Anti-Bridging** dans le groupe **Paramètres d'accès**.
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 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 suite 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 les 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 **Déclenchements de règles dans le mode Apprentissage intelligent**.

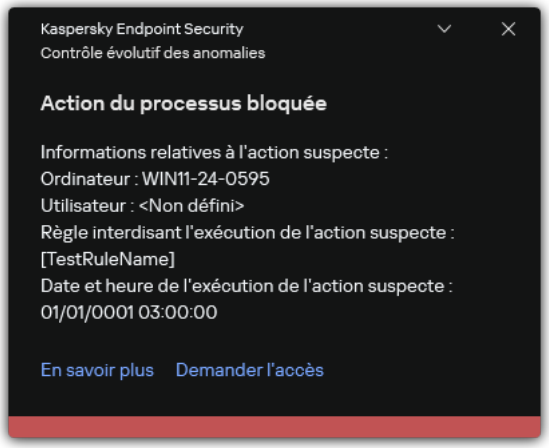
2. Analyse du rapport sur les déclenchements des règles

   L'administrateur analyse le rapport sur le déclenchement des règles ou le contenu du stockage **Déclenchements de règles dans le mode Apprentissage intelligent**. 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 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 **Déclenchements de règles dans le mode Apprentissage intelligent**. Nous vous recommandons de vérifier le rapport sur le déclenchement des règles et le contenu du stockage **Déclenchements de règles dans le mode Apprentissage intelligent**.

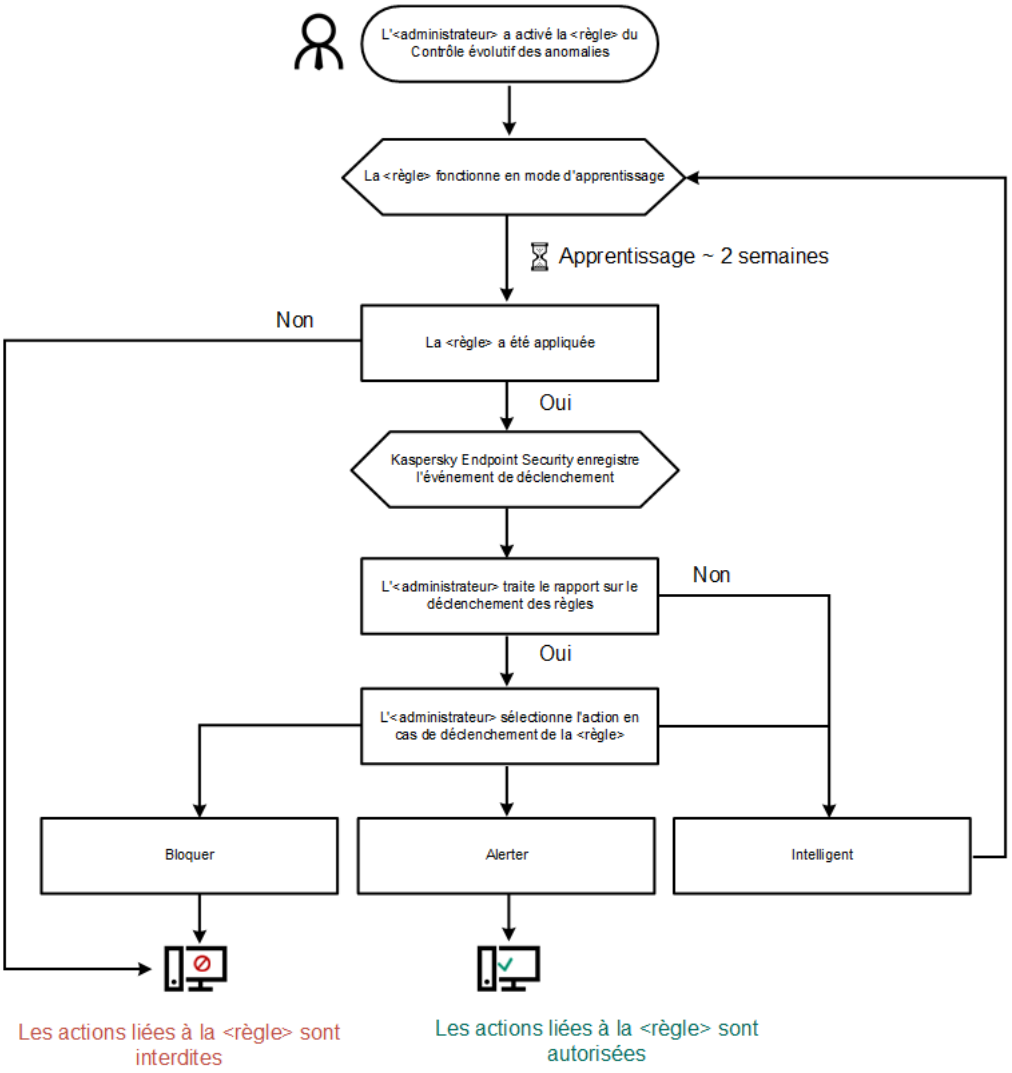
Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



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

Apprentissage du Contrôle évolutif des anomalies

Le Contrôle évolutif des anomalies inclut un ensemble de règles (modèles de comportement). 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. Le Contrôle évolutif des anomalies ne bloque pas l'activité de l'application sur l'ordinateur, mais informe uniquement l'administrateur. Vous pouvez également sélectionner manuellement l'action qui est exécutée lorsqu'une règle de Contrôle évolutif des anomalies est déclenchée.

Comment consulter la liste des règles du Contrôle évolutif des anomalies dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

5. Cochez la case **Contrôle évolutif des anomalies**.

6. Sous **Paramètres des règles du Contrôle évolutif des anomalies**, consultez la liste des règles.

   Par défaut, toutes les règles fonctionnent en mode **Intelligente**.

7. Le cas échéant, confirmez la mise à jour de la règle du Contrôle évolutif des anomalies.

8. Si nécessaire, sélectionnez une action lorsqu'une règle du Contrôle évolutif des anomalies est déclenchée :

   - **Bloquer**. 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.

   - **Informer**. 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.

9. Le cas échéant, désactivez les règles que vous ne souhaitez pas utiliser.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment consulter les règles du Contrôle évolutif des anomalies dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

5. Activez le commutateur **Contrôle évolutif des anomalies ACTIVÉ**.

6. Sous **Règles**, consultez la liste des règles.

   Par défaut, toutes les règles fonctionnent en mode **Intelligente**.

7. Le cas échéant, confirmez la mise à jour de la règle du Contrôle évolutif des anomalies.

8. Si nécessaire, sélectionnez une action lorsqu'une règle du Contrôle évolutif des anomalies est déclenchée :

   - **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.

   - **Informer**. 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.

9. Le cas échéant, désactivez les règles que vous ne souhaitez pas utiliser.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment consulter la liste des règles du Contrôle évolutif des anomalies 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 **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Activez le commutateur **Contrôle évolutif des anomalies**.

4. Dans le groupe **Règles**, cliquez sur le lien **Modifier les règles**.

   La liste des règles du Contrôle évolutif des anomalies s'ouvre. Par défaut, toutes les règles fonctionnent en mode **Intelligente**.

5. Le cas échéant, confirmez la mise à jour de la règle du Contrôle évolutif des anomalies.

6. Si nécessaire, sélectionnez une action lorsqu'une règle du Contrôle évolutif des anomalies est déclenchée :

   - **Bloquer**. 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.

   - **Informer**. 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. Le cas échéant, désactivez les règles que vous ne souhaitez pas utiliser.

8. Enregistrez vos modifications.

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, au cours de l'apprentissage, une règle ne s'est jamais déclenchée, le Contrôle évolutif des anomalies considère ce comportement comme atypique et fait passer l'état de la règle à l'état **Blocage intelligent**. Par la suite, l'application bloque toute activité répondant à cette règle.

Si une règle se déclenche pendant l'apprentissage, vous devez configurer manuellement l'action que l'application applique à l'activité détectée qui correspond à cette règle. Si vous ne sélectionnez pas l'action lors du déclenchement de la règle, le Contrôle évolutif des anomalies continue en mode d'apprentissage.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Cliquez sur le bouton **Modifier les règles** dans le groupe **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 suites bureautiques*) et développez l'ensemble.

5. Sélectionnez une règle (par exemple, *Lancement de Windows PowerShell depuis une suite bureautique*).

6. Utilisez le commutateur dans la colonne **Condition** 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Cliquez sur le bouton **Modifier les règles** dans le groupe **Règles**.

   La liste des règles du Contrôle évolutif des anomalies s'ouvre.

4. Sélectionnez une règle dans le tableau.

5. Cliquez sur **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 état Apprendre intelligemment 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 **Déclenchements de règles dans le mode Apprentissage intelligent** du Serveur d'administration de Kaspersky Security Center. À l'issue de l'état Apprendre intelligemment, 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.

   - **Bloquer**. 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.

   - **Informer**. 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.
3. Cliquez sur le bouton **Modifier les règles** dans le groupe **Règles**.

   La liste des règles du Contrôle évolutif des anomalies s'ouvre.
4. Sélectionnez une règle dans le tableau.
5. Cliquez sur **Modifier**.

   La fenêtre des propriétés des règles du Contrôle évolutif des anomalies s'ouvre.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions**.

   La fenêtre de propriétés des exclusions s'ouvre.
7. Sélectionnez l'utilisateur pour lequel vous souhaitez configurer une exclusion.

   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   > 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`).

   - **Hachage du processus source**. hash SHA256 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://<object>`, où `<object>` 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**. hash SHA256 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**. hash SHA256 du fichier.

    - **Objet cible**. Commande pour lancer le processus cible. Saisissez la commande selon le modèle suivant `object://<command>`, par exemple, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Vous pouvez également utiliser des masques, par exemple, `object://*C:\Windows\temp\*`.

    - **Hachage de l'objet cible**. hash SHA256 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Cliquez sur le bouton **Modifier les règles** dans le groupe **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 **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. Enregistrez le fichier.

5. Pour importer la liste des exclusions, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

   c. Ouvrez le fichier.

   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 règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Cliquez sur le bouton **Modifier les règles** dans le groupe **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.

Des modèles spéciaux sont disponibles pour les messages destinés à l'administrateur concernant le blocage d'actions potentiellement dangereuses. Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.

Pour modifier le modèle de message, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

3. Dans le groupe **Modèles**, configurez les modèles des messages du Contrôle évolutif des anomalies :

   - **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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'action de l'application**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Réinitialiser les paramètres**.

4. Enregistrez vos modifications.

Surveillance des opérations du Contrôle évolutif des anomalies

Le Contrôle évolutif des anomalies inclut plusieurs outils de surveillance. La surveillance du Contrôle évolutif des anomalies a pour principal objectif de configurer le module pendant l'apprentissage.

Rapports du Contrôle évolutif des anomalies

Le Contrôle évolutif des anomalies utilise les rapports suivants :

- **Rapport sur l'état des règles du Contrôle évolutif des anomalies**. Le rapport contient des informations sur l'état des règles du Contrôle évolutif des anomalies (*Off*, *Apprentissage intelligent*, *Blocage intelligent*, *Prévenir*, *Interdire*). Ce rapport permet d'analyser le niveau d'apprentissage du Contrôle évolutif des anomalies et d'évaluer le nombre de règles qui sont passées du mode *Apprentissage intelligent* au mode de fonctionnement normal (par exemple, *Blocage intelligent*).

- **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**. Le rapport contient des informations sur les déclencheurs de règle. Le rapport affiche également le mode de déclenchement des règles : *Interdire* (y compris *Blocage intelligent*) ou *Prévenir*. Ce rapport permet d'évaluer l'activité du Contrôle évolutif des anomalies sur les ordinateurs des utilisateurs.

Comment consulter les rapports du Contrôle évolutif des anomalies dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

4. Exécutez une des actions suivantes :

   - Si vous souhaitez consulter le rapport sur l'état des règles du Contrôle évolutif des anomalies, cliquez sur le lien **Rapport sur l'état des règles du Contrôle évolutif des anomalies**.

   - Si vous souhaitez consulter le rapport sur le déclenchement des règles du Contrôle évolutif des anomalies, cliquez sur le lien **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**.

5. Le processus de création du rapport est lancé.

   Le rapport s'ouvre dans une nouvelle fenêtre.

Comment consulter les rapports du Contrôle évolutif des anomalies dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle évolutif des anomalies**.

5. Dans le groupe **Règles**, exécutez une des actions suivantes :

   - Si vous souhaitez consulter le rapport sur l'état des règles du Contrôle évolutif des anomalies, sélectionnez **Consulter le rapport** → **État des règles**.

   - Si vous souhaitez consulter le rapport sur le déclenchement des règles du Contrôle évolutif des anomalies, cliquez sur **Consulter le rapport** → **Détections**.

6. Le processus de création du rapport est lancé.

   Le rapport s'ouvre dans une nouvelle fenêtre.

Pour générer des rapports dans la Console de Kaspersky Security Center, vous devez activer le transfert des données vers le Serveur d'administration. Le transfert de données est activé par défaut.

Comment activer le transfert des données pour le Contrôle évolutif des anomalies dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Transfert des données au Serveur d'administration**.

5. Cochez les cases suivantes :

   - **Rapport sur l'état des règles du Contrôle évolutif des anomalies**.

   - **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**.

6. Enregistrez vos modifications.

Comment activer le transfert des données pour le Contrôle évolutif des anomalies dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Intégration KSC**.

5. Sous **Transfert des données au Serveur d'administration**, cochez les cases suivantes :

   - **Rapport sur l'état des règles du Contrôle évolutif des anomalies**.

   - **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**.

6. Enregistrez vos modifications.

Stockage Déclenchements de règles dans le mode Apprentissage intelligent

En mode d'apprentissage, le Contrôle évolutif des anomalies envoie les informations relatives au déclenchement des règles à un stockage séparé, **Déclenchements de règles dans le mode Apprentissage intelligent**. Les informations sur les règles déclenchées sont représentées dans le stockage sous la forme d'une liste d'événements. Pour optimiser le Contrôle évolutif des anomalies, vous pouvez confirmer le comportement atypique sur l'ordinateur ou ajouter une exclusion de la règle.

Événements du Contrôle évolutif des anomalies

Le Contrôle évolutif des anomalies enregistre les événements déclencheurs de règle dans les modes *Interdire* (y compris *Blocage intelligent*) et *Prévenir*. Les événements suivants sont prévus à cet effet :

Action du processus bloquée

Action du processus ignorée

Les événements contiennent des informations sur l'activité suspecte, notamment les sommes de contrôle des fichiers, les utilisateurs impliqués, l'heure de déclenchement de la règle et le nom de l'ordinateur. Après avoir analysé l'événement, vous pouvez immédiatement ajouter des exclusions à la règle si vous trouvez que l'activité est authentique.

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* ou une autre catégorie), 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. L'administrateur peut créer de nombreuses règles. Une application peut correspondre aux critères de plusieurs règles. Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Kaspersky Endpoint Security vérifie si une application correspond à une règle à chaque démarrage. Kaspersky Endpoint Security compare l'application de manière séquentielle à toutes les règles du Contrôle des applications.

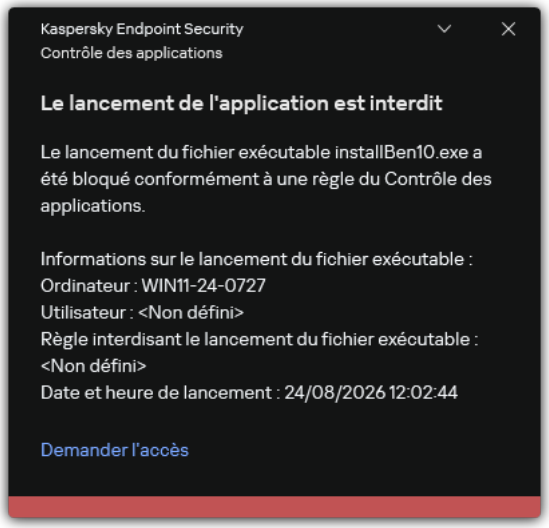
3. Sélection du mode de fonctionnement du Contrôle des applications.

   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.

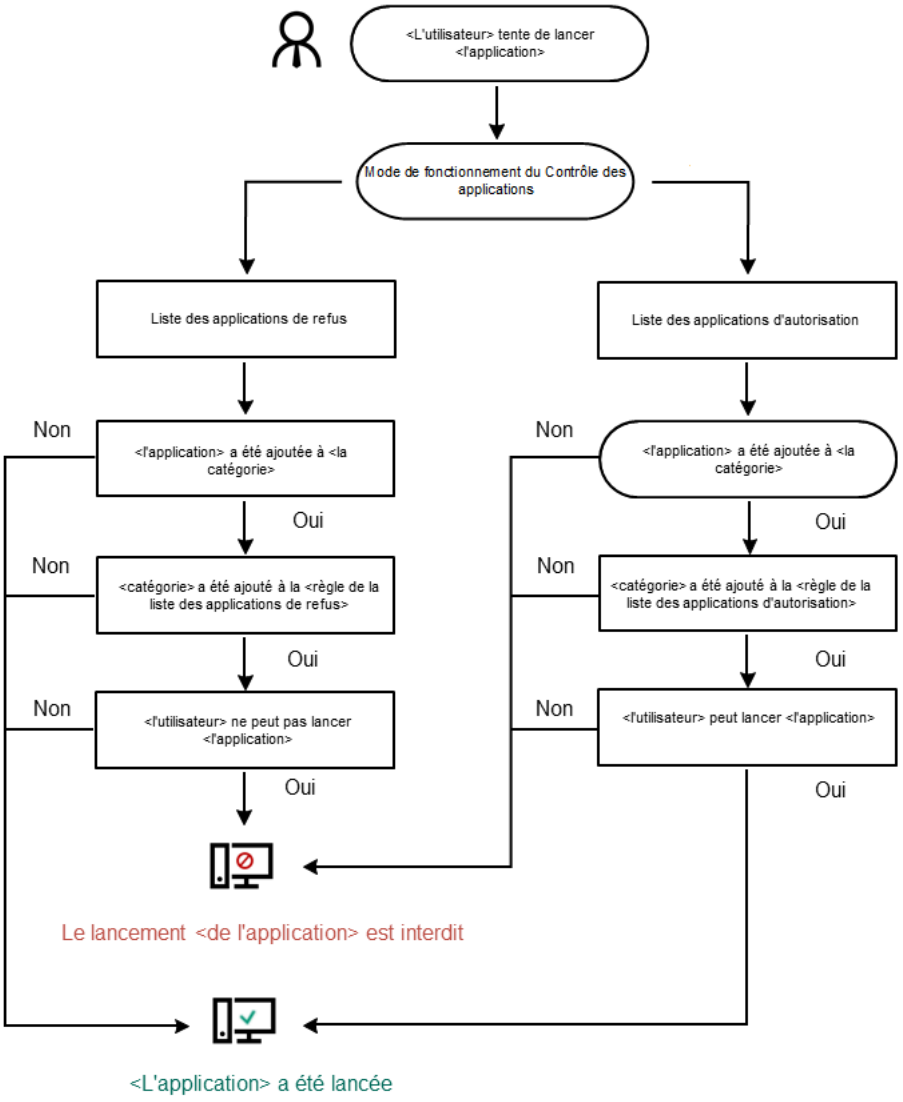
  Les règles de Contrôle des applications créées dans la Console d'administration de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.

- 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

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.
- 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 que Kaspersky Endpoint Security désigne comme catégorie KL **Autres programmes\Applications de confiance selon la réputation dans KSN** peut différer selon qu'une connexion aux serveurs KSN est disponible ou non.

- 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

Obtention d'informations sur les applications installées

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.

Consultation des informations relatives à l'application

Les informations sur les applications installées sont fournies par l'Agent d'administration de Kaspersky Security Center. Les informations sur les applications installées sont disponibles dans la console de Kaspersky Security Center, dans le dossier **Registre des applications**. L'Agent d'administration met à jour les informations à chaque synchronisation avec Kaspersky Security Center. Pour en savoir plus sur les informations envoyées par l'Agent d'administration, veuillez consulter l'aide de Kaspersky Security Center.

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 d'administration, sélectionnez **Avancé** → **Gestion des applications** → **Registre des applications**.
3. Sélectionnez l'application.
4. Dans le menu contextuel de l'application, sélectionnez l'option **Propriétés**.

Affichage des informations sur les fichiers exécutables

Vous pouvez réduire la charge de la base de données lors de la recherche d'informations sur les fichiers exécutables. Pour ce faire, il est conseillé d'exécuter la tâche *Inventaire* sur plusieurs ordinateurs de référence sur lesquels votre ensemble standard de logiciels est installé.

Les informations sur les fichiers exécutables sont fournies par Kaspersky Endpoint Security. Pour recevoir des informations sur le matériel, vous devez appliquer une stratégie active autorisant la transmission des informations sur les applications installées (cette transmission est activée par défaut).

Comment activer l'envoi d'informations sur l'application dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Transfert des données au Serveur d'administration**.
5. Cochez la case **Applications lancées**.
6. Enregistrez vos modifications.

Comment activer l'envoi d'informations sur l'application dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.
5. Cliquez sur le bouton **Paramètres avancés** dans le groupe **Transfert des données au Serveur d'administration**.
6. Dans la fenêtre qui s'ouvre, cochez la case **À propos des applications exécutables**.
7. Enregistrez vos modifications.

Vous pouvez obtenir une liste de fichiers exécutables en utilisant la tâche *Inventaire* de Kaspersky Endpoint Security. Vous pouvez consulter la liste des fichiers exécutables dans la console de Kaspersky Security Center, dans le dossier **Fichiers exécutables**.

Avant d'exécuter la tâche *Inventaire*, assurez-vous que la base de données répond aux recommandations de Kaspersky Security Center. Pour en savoir plus sur les limitations de la base de données, consultez l'aide de Kaspersky Security Center.

Comment lancer la tâche Inventaire dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur **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 (14.2)** → **Inventaire**.

Étape 2. Zone d'inventaire

Créez une liste des dossiers dans lesquels vous souhaitez que Kaspersky Endpoint Security recherche les fichiers exécutables. Configurez les paramètres de l'inventaire (cf. tableau ci-après).

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. Sélection du compte utilisateur pour lancer la tâche

Sélectionnez un compte pour exécuter la tâche de *Inventaire*. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local. Si la zone d'inventaire comprend des disques réseau ou d'autres objets dont l'accès est restreint, sélectionnez un compte utilisateur doté des autorisations requises.

Étape 5. Configuration de la planification du lancement de la tâche

Configurez la planification de la tâche, par exemple, manuellement.

Étape 6. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple, *Inventaire de référence*.

Étape 7. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. Par conséquent, les fichiers exécutables sont recherchés sur les ordinateurs des utilisateurs selon la planification configurée.

Lancement d'une tâche Inventaire dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Inventory**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Inventaire de référence*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Pour configurer la tâche, il faut accéder aux propriétés de la tâche (cf. le tableau ci-dessous).

8. Cochez la case en regard de la tâche.

9. Cliquez sur **Démarrer**.

   Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué. Les fichiers exécutables seront alors recherchés sur les ordinateurs des utilisateurs conformément à la planification définie.

Pour ouvrir la fenêtre des propriétés d'un fichier exécutable dans le dossier Fichiers exécutables :

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la Console d'administration, sélectionnez **Avancé** → **Gestion des applications** → **Fichiers exécutables**.

3. Choisissez le fichier exécutable.

4. Dans le menu contextuel du fichier exécutable, sélectionnez l'option **Propriétés**.

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.

Mise à jour des informations sur les applications installées et les fichiers exécutables

Dans Kaspersky Endpoint Security, le fonctionnement du module Contrôle des applications avec la base de données des fichiers exécutables a été optimisé. Kaspersky Endpoint Security met automatiquement à jour la base de données après la suppression du fichier de l'ordinateur. Cela permet de maintenir la base de données à jour et d'économiser les ressources de Kaspersky Security Center. Pour maintenir la base de données des applications installées à jour, l'envoi d'informations sur l'application au Serveur d'administration doit être activé (l'envoi est activé par défaut).

Paramètre	Description
Zones d'inventaire	La liste des objets qui formeront la zone d'inventaire.
Inventaire des modules DLL	Kaspersky Endpoint Security recherche des modules DLL dans la zone d'inventaire et envoie les informations à Kaspersky Security Center. L'activation de l'inventaire des modules DLL augmente considérablement la durée d'exécution de la tâche d'inventaire et la taille de la base de données.
Inventaire des fichiers de scripts	Kaspersky Endpoint Security recherche des scripts dans la zone d'inventaire et transmet les informations à Kaspersky Security Center. L'activation de l'inventaire des fichiers script augmente considérablement la durée d'exécution de la tâche Inventory et la taille de la base de données.
Exécuter uniquement lorsque l'ordinateur est inactif	Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.
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 un fichier si son analyse prend plus de (secondes) X s	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Endpoint Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Endpoint Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.
Analyser les archives	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les paquets de distribution	Analyse des paquets de distribution des applications tierces.
Ne pas décompresser les fichiers composés volumineux	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.

Comment activer le mode Applications bloquées

Le mode *Applications bloquées* permet au Contrôle des applications d'autoriser les utilisateurs à lancer n'importe quelle application, sauf celles interdites dans les règles de Contrôle des applications. Autrement dit, si aucune règle de refus n'existe, le Contrôle des applications autorise le lancement de l'application. Il s'agit du mode de fonctionnement du Contrôle des applications définies par défaut.

Avant d'activer le mode *Applications bloquées*, nous vous recommandons de tester vos règles du Contrôle des applications. Pour cela, vous pouvez activer le mode d'essai.

Comment activer le mode Applications bloquées dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.

5. Cochez la case **Contrôle des applications**.

6. Dans le groupe **Paramètres du Contrôle des applications**, utilisez la liste déroulante **Mode de contrôle** pour sélectionner **Liste de refus**.

7. De la liste déroulante **Action**, choisissez l'action pour le Contrôle des applications :

   - **Tester les règles**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.

   - **Appliquer les règles**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.

8. Sélectionnez l'état des règles du Contrôle des applications :

   - **Actif**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.

   - **Désact**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.

   - **Tester**. 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.

   Si nécessaire, ajoutez de nouvelles règles pour le Contrôle des applications.

9. Configurez les paramètres avancés du Contrôle des applications :

   - **Surveiller le téléchargement des modules DLL (augmente considérablement la charge sur le système)**. 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.

     Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Catégorie principale** ou toute autre règle qui contient la catégorie KL "**Catégorie principale\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 **Catégorie principale** est désactivée peut provoquer l'instabilité du système d'exploitation.

     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.

- **Utiliser une vérification stricte de la signature numérique**. Vous pouvez sélectionner un certificat comme condition de déclenchement d'une règle du Contrôle des applications. Si cette case est cochée, Kaspersky Endpoint Security applique les règles aux applications signées avec des certificats provenant uniquement du magasin de certificats du système de confiance. Les applications signées avec de tels certificats sont également considérées comme de confiance par les modules de protection, par exemple la tâche *Analyse des logiciels malveillants*. En revanche, si vous spécifiez un certificat provenant d'un autre magasin dans une règle de Contrôle des applications, Kaspersky Endpoint Security n'applique pas une telle règle.

  Si la case est décochée, Kaspersky Endpoint Security applique les règles aux applications signées à l'aide d'un certificat provenant du Trusted Root Certificate Store de Windows. Ces applications ne font pas partie de la zone de confiance. Les modules de protection surveillent l'activité de telles applications.

- **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.

- **Message pour 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.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer le mode Applications bloquées dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des applications**.

5. Activez le commutateur **Contrôle des applications ACTIVÉ**.

6. Dans le groupe **Mode de fonctionnement**, sélectionnez l'option **Bloquer tout ce qui ne figure pas dans la liste des règles**.

7. Dans le bloc **Action**, sélectionnez l'action pour le Contrôle des applications :

   - **Informer**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.

   - **Appliquer les règles**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.

8. Sélectionnez l'état des règles du Contrôle des applications :

   - **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.

   - **Mode d'essai**. 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.

Si nécessaire, ajoutez de nouvelles règles pour le Contrôle des applications.

9. Configurez les paramètres avancés du Contrôle des applications :

   - **Surveiller le chargement des modules DLL**. 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.

     Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Catégorie principale** ou toute autre règle qui contient la catégorie KL "**Catégorie principale\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 **Catégorie principale** est désactivée peut provoquer l'instabilité du système d'exploitation.

     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.

   - **Utiliser une vérification stricte de la signature numérique**. Vous pouvez sélectionner un certificat comme condition de déclenchement d'une règle du Contrôle des applications. Si cette case est cochée, Kaspersky Endpoint Security applique les règles aux applications signées avec des certificats provenant uniquement du magasin de certificats du système de confiance. Les applications signées avec de tels certificats sont également considérées comme de confiance par les modules de protection, par exemple la tâche *Analyse des logiciels malveillants*. En revanche, si vous spécifiez un certificat provenant d'un autre magasin dans une règle de Contrôle des applications, Kaspersky Endpoint Security n'applique pas une telle règle.

     Si la case est décochée, Kaspersky Endpoint Security applique les règles aux applications signées à l'aide d'un certificat provenant du Trusted Root Certificate Store de Windows. Ces applications ne font pas partie de la zone de confiance. Les modules de protection surveillent l'activité de telles applications.

   - **Message pour l'utilisateur**. Modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application.

   - **Message pour 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.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer le mode Applications bloquées 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 **Contrôles de sécurité** → **Contrôle des applications**.

3. Activez le commutateur **Contrôle des applications**.

4. Dans le groupe **Mode de contrôle de démarrage de l'application**, sélectionnez l'option **Liste de refus. Toutes les applications, à l'exception de celles de la liste des règles, sont autorisées**.

5. Dans le bloc **Action exécutée lors du lancement d'applications bloquées par des règles**, sélectionnez l'action pour le Contrôle des applications :

   - **Informer (mode test) et enregistrer les événements dans Rapport**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.

   - **Bloquer**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.

6. Sélectionnez l'état des règles du Contrôle des applications :

   - **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.

   - **Mode d'essai**. 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.

   Si nécessaire, ajoutez de nouvelles règles pour le Contrôle des applications.

7. Configurez les paramètres avancés du Contrôle des applications :

   - **Surveiller le chargement des modules DLL**. 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.

     Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Catégorie principale** ou toute autre règle qui contient la catégorie KL "**Catégorie principale\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 **Catégorie principale** est désactivée peut provoquer l'instabilité du système d'exploitation.

     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.

   - **Utiliser une vérification stricte de la signature numérique**. Vous pouvez sélectionner un certificat comme condition de déclenchement d'une règle du Contrôle des applications. Si cette case est cochée, Kaspersky Endpoint Security applique les règles aux applications signées avec des certificats provenant uniquement du magasin de certificats du système de confiance. Les applications signées avec de tels certificats sont également considérées comme de confiance par les modules de protection, par exemple la tâche *Analyse des logiciels malveillants*. En revanche, si vous spécifiez un certificat provenant d'un autre magasin dans une règle de Contrôle des applications, Kaspersky Endpoint Security n'applique pas une telle règle.

     Si la case est décochée, Kaspersky Endpoint Security applique les règles aux applications signées à l'aide d'un certificat provenant du Trusted Root Certificate Store de Windows. Ces applications ne font pas partie de la zone de confiance. Les modules de protection surveillent l'activité de telles applications.

- **Modèles de messages sur le blocage d'applications**. Modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application.

- **Modèle du message affiché si le lancement de l'application est bloqué**. 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.

8. Enregistrez vos modifications.

Par conséquent, le Contrôle des applications bloque les applications bloquées. Kaspersky Endpoint Security génère également les événements *Le lancement de l'application est interdit*. Vous pouvez utiliser ces événements pour générer le rapport *Rapport sur les applications interdites* dans la console de Kaspersky Security Center. Dans le résumé du rapport, vous pouvez consulter la liste des applications et des ordinateurs sur lesquels la règle du Contrôle des applications s'est déclenchée.

Contrôle des applications à partir d'un ordinateur de référence

Vous pouvez utiliser un ordinateur de référence pour créer une image avec un ensemble d'applications dont vous avez besoin. Vous pouvez ensuite utiliser cette image pour déployer le système d'exploitation et les applications sur d'autres ordinateurs. Il n'est pas toujours possible de maintenir l'image à jour. Le Contrôle des applications vous permet de maintenir une liste d'applications autorisées à partir d'un ordinateur de référence. Le Contrôle des applications inspecte automatiquement les applications installées sur l'ordinateur de référence et met à jour la catégorie. Les ordinateurs reçoivent ainsi une liste actualisée des applications autorisées.

La configuration du Contrôle des applications à partir d'un ordinateur de référence implique les étapes suivantes :

1. Création d'une catégorie mise à jour automatiquement. Lors de la création de la nouvelle catégorie, sélectionnez la **catégorie qui inclut les fichiers exécutables d'un dossier particulier** et sélectionnez votre ordinateur de référence.

   Comment créer une catégorie mise à jour automatiquement dans la Console d'administration (MMC)

   1. Ouvrez la Console d'administration de Kaspersky Security Center.

   2. Dans l'arborescence de la Console d'administration, sélectionnez **Avancé** → **Gestion des applications** → **Catégories d'applications**.

   3. Dans l'espace de travail, cliquez sur le bouton **Nouvelle catégorie**.

      L'Assistant de création d'une catégorie d'applications est lancé.

   4. Suivez les instructions de l'Assistant de création de catégories d'application.

   Étape 1. Sélection du type de catégorie

   Sélectionnez l'option **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés.** comme type de catégorie.

Étape 2. Saisie du nom de la catégorie personnalisée

Indiquez à cette étape le nom de la catégorie d'applications.

Étape 3. Paramètres

> Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés**.

À cette étape, cliquez sur le bouton **Ajouter** et indiquez les ordinateurs dont les fichiers exécutables seront ajoutés à la catégorie d'applications par Kaspersky Security Center. 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 la fonction de hachage. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :
  - **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)**.
  - **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- La case **Synchroniser les 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 **Synchroniser les données avec le stockage du Serveur d'administration** est décochée, Kaspersky Security Center ne va pas modifier la catégorie d'applications après sa création.

Étape 4. Filtre

À cette étape, configurez un filtre pour les fichiers.

Vous pouvez indiquer le type de fichier que vous souhaitez utiliser pour créer la catégorie d'applications.

- **Tous les fichiers**. La catégorie correspondra à tous les fichiers. Cette option est sélectionnée par défaut.
- **Uniquement les fichiers &hors des catégories d'applications**. La catégorie correspondra uniquement aux fichiers ne faisant pas partie des catégories d'applications.

Vous pouvez spécifier les dossiers des ordinateurs sélectionnés qui contiennent les fichiers que vous souhaitez utiliser pour créer la catégorie d'applications.

- **Tous les dossiers**. La catégorie correspondra à tous les dossiers. Cette option est sélectionnée par défaut.
- **Dossier indiqué**. La catégorie correspondra uniquement au dossier spécifié. Si vous sélectionnez cette option, vous devez indiquer un chemin d'accès au dossier.

Étape 5. Création d'une catégorie personnalisée

Quittez l'Assistant.

Comment créer une catégorie dont le contenu est ajouté automatiquement dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Applications tierces** → **Catégories d'applications**.

   Cette action permet d'ouvrir la liste des catégories d'applications.

2. Cliquez sur **Ajouter**.

   L'Assistant de création d'une catégorie d'applications est lancé.

3. Configurez les paramètres généraux de la catégorie d'applications :

   - Nom de la catégorie.
   - Méthode de création de la catégorie. Sélectionnez l'option **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés.** comme type de catégorie.

   Passez à l'étape suivante.

4. Configurez les paramètres avancés de la catégorie d'applications :

   - Indiquez les ordinateurs à partir desquels Kaspersky Security Center ajoutera les fichiers exécutables 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**.
   - Sélectionnez un algorithme de calcul pour la fonction de hachage.
   - Configurez un intervalle pour la synchronisation des données avec le stockage du Serveur d'administration.
   - Configurez un filtre pour les fichiers.

5. Quittez l'Assistant.

Lors de la création d'une catégorie mise à jour automatiquement, il peut être utile de subdiviser les fichiers en plusieurs catégories. Par exemple, les fichiers du système d'exploitation et les fichiers du dossier Program Files. Pour ce faire, vous pouvez utiliser un filtre dans les paramètres de la catégorie et sélectionner des dossiers individuels.

2. Sélection du mode du Contrôle des applications. Empêchez l'exécution de toutes les applications qui ne sont pas explicitement autorisées. Pour ce faire, sélectionnez le mode *Applications bloquées*.

3. Création d'une règle du Contrôle des applications. Dans les paramètres des règles, sélectionnez la catégorie à laquelle appartiennent les fichiers exécutables de l'ordinateur de référence.

Comment configurer le Contrôle des applications à partir d'un ordinateur de référence dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.
5. Cochez la case **Contrôle des applications**.
6. Dans le groupe **Paramètres du Contrôle des applications**, utilisez la liste déroulante **Mode de contrôle** pour sélectionner **Liste de refus**.
7. De la liste déroulante **Action**, choisissez l'action pour le Contrôle des applications :
   - **Tester les règles**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.
   - **Appliquer les règles**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.
8. Dans la liste des règles du Contrôle des applications, cliquez sur le bouton **Ajouter**.

   Cette action lance l'Assistant pour ajouter une règle du Contrôle des applications.
9. Dans la liste déroulante **Catégorie**, sélectionnez une catégorie mise à jour automatiquement à partir de l'ordinateur de référence.
10. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle du Contrôle des applications.
11. Configurez les paramètres avancés de la règle du Contrôle des applications :
    - **Interdire aux autres utilisateurs**. L'application interdit le lancement des applications de la catégorie sélectionnée pour tous les utilisateurs non répertoriés dans la liste.
    - **Programmes de mise à jour de confiance**. Kaspersky Endpoint Security considère les applications incluses dans la catégorie sélectionnée comme des mises à jour de confiance autorisées à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.
12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer le Contrôle des applications à partir d'un ordinateur de référence dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des applications**.

5. Activez le commutateur **Contrôle des applications ACTIVÉ**.

6. Dans le groupe **Mode de fonctionnement**, sélectionnez l'option **Bloquer tout ce qui ne figure pas dans la liste des règles**.

7. Dans le bloc **Action**, sélectionnez l'action pour le Contrôle des applications :

   - **Informer**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.

   - **Appliquer les règles**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.

8. Dans la liste des règles du Contrôle des applications, cliquez sur le bouton **Ajouter**.

   Cette action lance l'Assistant pour ajouter une règle du Contrôle des applications.

9. Sous **Catégories/Applications**, sélectionnez une catégorie mise à jour automatiquement à partir de l'ordinateur de référence.

10. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle du Contrôle des applications.

11. Configurez les paramètres avancés de la règle du Contrôle des applications :

    - **Utilisateurs**. L'application interdit le lancement des applications de la catégorie sélectionnée pour tous les utilisateurs non répertoriés dans la liste.

    - **Programmes de mise à jour de confiance**. Kaspersky Endpoint Security considère les applications incluses dans la catégorie sélectionnée comme des mises à jour de confiance autorisées à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment configurer le Contrôle des applications à partir d'un ordinateur de référence 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 **Contrôles de sécurité** → **Contrôle des applications**.

3. Activez le commutateur **Contrôle des applications**.

4. Dans le groupe **Mode de contrôle de démarrage de l'application**, sélectionnez l'option **Liste de refus. Toutes les applications, à l'exception de celles de la liste des règles, sont autorisées**.

5. Dans le bloc **Action exécutée lors du lancement d'applications bloquées par des règles**, sélectionnez l'action pour le Contrôle des applications :

   - **Informer (mode test) et enregistrer les événements dans Rapport**. Le Contrôle des applications ne bloque pas les applications dont l'exécution est empêchée par les règles, mais génère des événements concernant l'exécution d'applications qui seraient autrement bloquées.

   - **Bloquer**. Le Contrôle des applications bloque les applications bloquées et génère les événements correspondants.

6. Dans la liste des règles du Contrôle des applications, cliquez sur le bouton **Ajouter**.

   Cette action lance l'Assistant pour ajouter une règle du Contrôle des applications.

7. Sous **Catégorie**, sélectionnez une catégorie mise à jour automatiquement à partir de l'ordinateur de référence.

8. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle du Contrôle des applications.

9. Configurez les paramètres avancés de la règle du Contrôle des applications :

   - **Interdire aux autres utilisateurs**. L'application interdit le lancement des applications de la catégorie sélectionnée pour tous les utilisateurs non répertoriés dans la liste.

   - **Programmes de mise à jour de confiance**. Kaspersky Endpoint Security considère les applications incluses dans la catégorie sélectionnée comme des mises à jour de confiance autorisées à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.

10. Enregistrez vos modifications.

Administration des règles du Contrôle des applications

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 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.

Si vous avez sélectionné un certificat comme condition de déclenchement des règles, vous devez vous assurer que ce certificat est ajouté au stockage système sécurisé sur l'ordinateur et vérifier les paramètres d'utilisation du stockage système sécurisé dans 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.
- **Mode d'essai**. 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 condition de déclenchement de la règle de Contrôle des 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 dans la Console d'administration :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console d'administration, sélectionnez **Avancé** → **Gestion des applications** → **Catégories d'applications**.
3. Dans l'espace de travail, cliquez sur le bouton **Nouvelle catégorie**.

   L'Assistant de création de catégories personnalisée s'ouvre.
4. Suivez les instructions de l'Assistant de création d'une nouvelle catégorie.

Étape 1. Sélection du type de catégorie

Cette étape permet de choisir un des types suivants de catégories d'applications :

- Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie Si vous avez choisi ce type de catégorie, à l'étape *Configuration des conditions d'inclusion des applications dans des catégories* et à l'étape *Configuration des conditions pour exclure les applications depuis une catégorie*, vous pourrez définir les critères d'inclusion des fichiers exécutables dans la catégorie.

- Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés. Ces fichiers exécutables sont traités automatiquement et leurs métriques sont ajoutées à la catégorie 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 reprend les fichiers exécutables d'un dossier particulier. Les fichiers exécutables des applications copiés dans ce dossier particulier sont traités automatiquement et leurs métriques sont ajoutées à la catégorie 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

Lors de l'ajout d'un grand nombre de conditions aux règles du Contrôle des applications (par exemple, les hachages de fichier), la consommation des ressources de l'ordinateur augmente. Lorsque le nombre total de conditions atteint 50 000, des problèmes de performances peuvent survenir. Pour optimiser les performances, il est recommandé de vérifier les conditions et d'en réduire le nombre.

Cette étape n'est pas proposée si vous avez choisi le type de catégorie **Catégorie dont le contenu a été ajouté manuellement**.

À cette étape, dans la liste déroulante **Ajouter**, sélectionnez une des conditions suivantes d'inclusion des applications dans la catégorie :

- **Depuis la liste des fichiers exécutables**. Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.
- **Depuis les propriétés du fichier**. Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Données méta 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.
- **Hash 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 issus 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 de l'installateur msi 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.
- **D'une catégorie K&L**. 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.

- **Définir le chemin d'accès à l'application (masques pris en charge)**. Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.
- **Sélectionner un certificat dans le stockage**. 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**.

Vous pouvez choisir le magasin de certificats. Par défaut, le Contrôle des applications applique les règles uniquement aux applications signées avec un certificat provenant du magasin de certificats du système de confiance. La case **Utiliser une vérification stricte de la signature numérique** permet d'activer cette opération.

- **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 dont le contenu a été ajouté 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 :

- **Depuis la liste des fichiers exécutables**. Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.
- **Depuis les propriétés du fichier**. Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Données méta 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.
- **Hash 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 issus 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 de l'installateur msi 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.

- **D'une catégorie K&L**. 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.

- **Définir le chemin d'accès à l'application (masques pris en charge)**. Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.

- **Sélectionner un certificat dans le stockage**. 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 reprend les fichiers exécutables issus d'appareils sélectionnés**.

À cette étape, cliquez sur le bouton **Ajouter** et indiquez les ordinateurs dont les fichiers exécutables seront ajoutés à la catégorie d'applications par Kaspersky Security Center. 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 la fonction de hachage. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :

  - **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)**.

  - **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- La case **Synchroniser les 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 **Synchroniser les données avec le stockage du Serveur d'administration** est décochée, Kaspersky Security Center ne va pas modifier la catégorie d'applications après sa création.

Étape 6. Dossier du stockage

Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui reprend les fichiers exécutables d'un dossier particulier**.

À cette étape, 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 dans la catégorie des bibliothèques connectées de manière dynamique (.DLL)**. 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.

- La case **Inclure les données relatives aux 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 la fonction de hachage. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :

  - **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)**.

  - **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- La case **Analyse forcée du dossier à la recherche de la présence de modifications**. 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 **Analyse forcée du dossier à la recherche de la présence de modifications** 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.

- Le champ **Intervalle d'analyse (1–168 heures)**. 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 disponible si la case **Analyse forcée du dossier à la recherche de la présence de modifications** est cochée.

Étape 7. Création d'une catégorie personnalisée

Quittez l'Assistant.

Pour ajouter une nouvelle condition de déclenchement à la règle de Contrôle des applications dans l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 : N** ou **Exclusions : N** 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 fichier ou 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 personnalisée**. 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 (disque 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 de 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 fichier ou 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 prend en charge les caractères `*` et `?` pour la saisie du masque dans les métadonnées : **Nom du fichier**, **Nom de l'application**, **Fournisseur**.

- 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 **Émetteur** et **Sujet du certificat** 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**.

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 à partir 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 d'administration, sélectionnez **Avancé** → **Gestion 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 dans la catégorie**.

5. Dans la fenêtre qui s'ouvre, procédez comme suit :

   - Choisissez dans la partie supérieure de la fenêtre une des options suivantes :

     - **Ajoute une &nouvelle catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.

     - **Ajouter à une &catégorie d'application existante**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.

   - Sélectionnez l'une des options suivantes dans le groupe **Type de règle** :

     - **Règles pour &l'ajout aux inclusions**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.

     - **Règles pour l'ajout aux &exclusions**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.

   - Dans le groupe **Paramètre utilisé comme condition**, sélectionnez l'une des options suivantes :

     - **Détails du certificat (ou hachage SHA256 pour les fichiers sans certificat)**.

     - **Détails du certificat (les fichiers sans certificat sont ignorés)**.

- **SHA256 uniquement (les fichiers sans hachage sont ignorés)**.
- **MD5 uniquement (mode supprimé, uniquement pour Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Enregistrez vos modifications.

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 aux 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 **Sélections d'événements**.
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 dans la catégorie**.
7. Dans la fenêtre qui s'ouvre, configurez les paramètres de la catégorie d'applications :
   - Choisissez dans la partie supérieure de la fenêtre une des options suivantes :
     - **Ajoute une nouvelle catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.
     - **Ajouter à une catégorie d'application existante**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.
   - Sélectionnez l'une des options suivantes dans le groupe **Type de règle** :
     - **Règles pour l'ajout aux inclusions**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.
     - **Règles pour l'ajout aux exclusions**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.
   - Dans le groupe **Paramètre utilisé comme condition**, sélectionnez l'une des options suivantes :
     - **Détails du certificat (ou hash SHA-256 pour les fichiers sans certificat)**.
     - **Détails du certificat (les fichiers sans certificat sont ignorés)**.

- **SHA-256 uniquement (les fichiers sans hash sont ignorés)**.
- **MD5 uniquement (mode supprimé, uniquement pour Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Enregistrez vos modifications.

Ajout d'une règle du Contrôle des applications

Pour ajouter une règle de Contrôle des applications à l'aide de Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. 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.
4. Cliquez sur **Ajouter**.
   La fenêtre **Règle de Contrôle des applications** s'ouvre.
5. Exécutez une des actions suivantes :
   - Si vous voulez créer une catégorie, procédez comme suit :
     a. Cliquez sur **Créer une catégorie**.
     L'Assistant de création de catégories personnalisée s'ouvre.
     b. Suivez les instructions de l'Assistant de création d'une nouvelle catégorie.
     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 **Propriétés**.
     c. Modifier les paramètres de la catégories d'applications sélectionnée.
     d. Enregistrez vos modifications.
     e. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée sur la base de laquelle vous souhaitez créer la règle.
6. Dans le tableau **Utilisateurs et leurs droits**, cliquez sur le bouton **Ajouter**.
   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

7. Dans le tableau **Utilisateurs et leurs droits**, procédez comme suit :

   - 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 **Bloquer** sur les lignes requises.

8. 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 **Utilisateur ou groupe** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans la colonne **Utilisateur ou groupe**.

9. 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.

10. Enregistrez vos modifications.

Pour ajouter ou modifier une règle de Contrôle des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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 **Ajouter**.

   La fenêtre Paramètres de la 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. Dans le tableau **Utilisateurs et leurs droits**, cliquez sur le bouton **Ajouter**.

      Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

      La règle s'applique à tous les utilisateurs par défaut.

      Si aucun utilisateur n'est repris dans le tableau, la règle ne peut pas être enregistrée.

d. Dans le tableau **Utilisateurs 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 empêche les applications qui satisfont aux conditions de déclenchement des règles de s'exécuter pour tous les utilisateurs qui ne sont pas repris dans le tableau **Utilisateurs et leurs droits** et qui ne sont pas membres des groupes d'utilisateurs repris dans le tableau **Utilisateurs et leurs droits**.

> 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 **Utilisateurs et leurs droits** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans le tableau **Utilisateurs et leurs droits**.

f. Cochez la case **Programmes de mise à jour de confiance** si vous voulez que Kaspersky Endpoint Security considère les applications correspondant aux conditions de déclenchement de la règle comme des programmes de mise à jour de confiance. Les *programmes de mise à jour de confiance* sont des applications qui sont autorisées à créer d'autres fichiers exécutables qui seront autorisés à s'exécuter par la suite.

   Si une application déclenche plusieurs règles, Kaspersky Endpoint Security active l'indicateur *Programmes de mise à jour de confiance* si les conditions suivantes sont remplies :

   - Toutes les règles permettent à l'application de fonctionner.
   - La case **Programmes de mise à jour de confiance** est cochée pour au moins une règle.

6. Sous l'onglet **Conditions : N**, créez ou modifiez la liste des conditions d'inclusion permettant de déclencher la règle.

7. Sous l'onglet **Exclusions : N**, 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 exécutables créés par les programmes de mise à jour de confiance migre également.

8. 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 dans la Console d'administration, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. 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.

4. Dans la colonne **État**, cliquez-gauche pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :

   - **Actif**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.

   - **Désact**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.

   - **Tester**. 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.

5. Enregistrez vos modifications.

Pour modifier l'état de la règle de Contrôle des applications dans l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **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.

   - **Mode d'essai**. 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.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.

4. 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.

5. Pour importer 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. Ouvrez le fichier.

      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.

6. 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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des applications**.

5. Sous **Mode de fonctionnement**, sélectionnez une liste de règles : liste de refus ou liste d'autorisation d'application.

6. Pour exporter la liste des règles, procédez comme suit :

   a. Sélectionnez les règles que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des règles dans un fichier JSON dans le dossier des téléchargements par défaut.

7. Pour importer la liste des règles, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des règles.

   b. Ouvrez le fichier.

      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 JSON.

8. Enregistrez vos modifications.

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**.

4. Dans la fenêtre qui s'ouvre, accédez à la section **Événements**.

5. Cliquez sur le bouton **Tout effacer**.

6. Dans le tableau **Événements**, cochez la case **Le lancement de l'application est interdit**.

7. Enregistrez vos modifications.

8. Dans la liste déroulante **Sélections d'événements**, 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 le nœud **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.

3. Cliquez sur **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 de rapport**, sélectionnez **Autres** → **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. 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.

Activation et désactivation des tests de règles du Contrôle des applications

Pour activer ou désactiver le test des règles de Contrôle des applications dans Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. 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.

4. 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.

5. 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 gérer le démarrage des applications sur les ordinateurs des utilisateurs, dans la liste déroulante, sélectionnez **Appliquer les règles**.

6. Enregistrez vos modifications.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.

3. Cliquez sur le bouton **Applications bloquées** ou **Applications autorisées**.

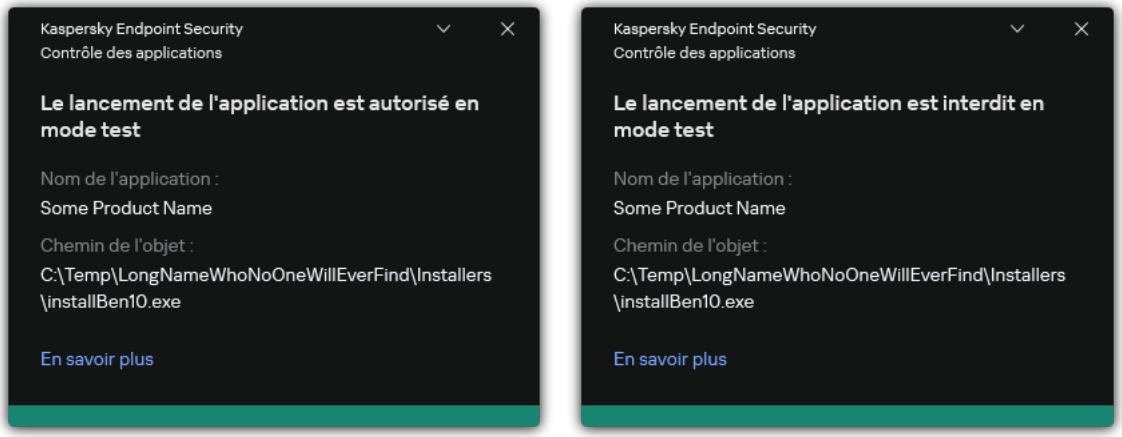
   Cette action permet d'ouvrir la liste des règles du Contrôle des applications.

4. Dans la colonne **État**, sélectionnez l'option **Mode d'essai**.

   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.

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. Vous pouvez également configurer l'affichage des notifications relatives aux tests de règles sur l'ordinateur de l'utilisateur (cf. ill. ci-dessous).



Notifications du Contrôle des applications en mode test

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 le nœud **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.

3. Cliquez sur **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 de rapport**, sélectionnez **Autres** → **Rapport sur les applications interdites en mode test**.

   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 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**.
4. Dans la fenêtre qui s'ouvre, accédez à la section **Événements**.
5. Cliquez sur le bouton **Tout effacer**.
6. Dans le tableau **Événements**, cochez les cases **Le lancement de l'application est interdit en mode test** et **Le lancement de l'application est autorisé en mode test**.
7. Enregistrez vos modifications.
8. Dans la liste déroulante **Sélections d'événements**, choisissez la sélection créée.
9. Cliquez sur le bouton **Lancer la sélection**.

Surveillance des applications

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 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, dans la section **Surveillance**, cliquez sur la mosaïque **Surveillance des applications**.

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 **Lancées au démarrage** affiche la liste des applications qui sont lancées lorsque le système d'exploitation démarre.

Si vous souhaitez masquer les informations relatives à l'activité des applications sur l'ordinateur de l'utilisateur, vous pouvez restreindre l'accès des utilisateurs à l'outil Surveillance des applications.

Masquage de la Surveillance des applications dans l'interface de l'application à l'aide de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.
4. Utilisez la case **Masquer la section Surveillance des applications** pour accorder ou révoquer l'accès à l'outil.
5. Enregistrez vos modifications.

Masquage de la Surveillance des applications dans l'interface de l'application à l'aide de Web Console et de Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Interaction avec l'utilisateur**.
5. Utilisez la case **Masquer la section Surveillance des applications** pour accorder ou révoquer l'accès à l'outil.
6. Enregistrez vos modifications.

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.

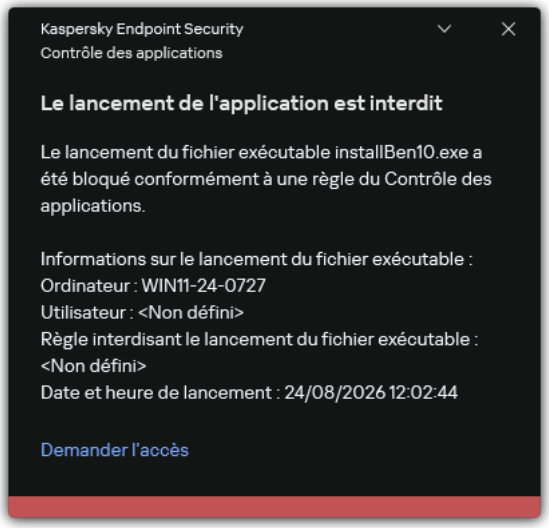
Vous pouvez utiliser les caractères génériques suivants pour créer un masque de nom de fichier ou de dossier :

- 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` 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. Les experts de Kaspersky fournissent un modèle de message à l'utilisateur décrivant les raisons pour lesquelles l'application a été bloquée (voir la figure ci-dessous). Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs. Au moment de générer un message, Kaspersky Endpoint Security récupère la valeur de la variable dans les paramètres du système d'exploitation et l'insère dans le message correspondant à l'ordinateur, à l'utilisateur et à l'événement en question.



Notification du Contrôle des applications

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. Pour cela, l'utilisateur doit cliquer sur le bouton **Demander l'accès** et envoyer un message à l'administrateur décrivant la situation. Vous pouvez également préparer un modèle de message destiné à l'administrateur, en y ajoutant des informations susceptibles d'éclairer votre décision d'autoriser ou de bloquer l'accès à l'application. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction du lancement de l'application**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Comment modifier les modèles des messages du Contrôle des applications dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle des applications**.

4. Cliquez sur le bouton **Modèles** dans le groupe **Paramètres des modèles de notification**.

5. Cela ouvre une fenêtre ; dans cette fenêtre, configurez les modèles du Contrôle des applications :

   - **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.

     Vous ne pouvez pas configurer de modèles de messages pour le Contrôle des applications en mode test. Le Contrôle des applications en mode test affiche des notifications prédéfinies.

   - **Message pour 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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Par défaut**.

6. Enregistrez vos modifications.

Comment modifier les modèles des messages du Contrôle des applications dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle des applications**.

5. Dans le bloc **Modèles de messages**, cliquez sur le lien **Messages concernant le blocage du lancement de l'application** et configurez les modèles pour les messages du Contrôle des applications :

   - **Message pour l'utilisateur**. Modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application.

     Vous ne pouvez pas configurer de modèles de messages pour le Contrôle des applications en mode test. Le Contrôle des applications en mode test affiche des notifications prédéfinies.

   - **Message pour 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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Rétablir les valeurs par défaut**.

6. Enregistrez vos modifications.

Comment modifier les modèles des messages du Contrôle des applications 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 **Contrôles de sécurité** → **Contrôle des applications**.

3. Dans le groupe **Modèles de messages sur le blocage d'applications**, configurez les modèles pour les messages du Contrôle des applications :

   - **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.

     Vous ne pouvez pas configurer de modèles de messages pour le Contrôle des applications en mode test. Le Contrôle des applications en mode test affiche des notifications prédéfinies.

   - **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.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Ajouter une variable** et sélectionnez la variable requise dans la liste des options disponibles.

   Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Réinitialiser les paramètres**.

4. Enregistrez vos modifications.

Variables dans les modèles de message du Contrôle des applications

Vous pouvez utiliser les variables suivantes dans les modèles de messages utilisateur ou administrateur :

- **Nom de la règle déclenchée** – `%RULE%`.

  Nom de la règle qui a bloqué l'exécution d'un fichier.

- **Date actuelle** – `%DATE%`.

  Date à laquelle l'exécution du fichier a été bloquée au format JJ.MM.AAAA.

- **Heure actuelle** – `%TIME%`.

  Heure à laquelle l'exécution du fichier a été bloquée au format HH:MM.

- **Nom d'utilisateur** – `%USER_NAME%`.

  Nom du compte utilisateur actuel de l'ordinateur sur lequel l'exécution du fichier a été bloquée, dans le format `<device name>\<user alias>` (par exemple, `DESKTOP-123\John.Smith`).

- **Nom de l'ordinateur** – `%COMPUTER_NAME%`.

  Nom de l'ordinateur sur lequel l'exécution du fichier a été bloquée.

- **Nom du fichier exécutable** – `%FILE_NAME%`.

  Nom du fichier exécutable de l'application bloquée.

- **Catégorie KL du fichier exécutable** – `%KL_CAT%`.

  Catégorie KL à laquelle appartient l'application bloquée (par exemple, *Navigateurs* ou une autre catégorie).

- **Chemin du fichier exécutable** – `%FILE_PATH%`.

  Chemin d'accès complet au fichier exécutable de l'application bloquée.

- **Version du fichier exécutable** – `%FILE_VERSION%`.

  Version du fichier exécutable de l'application bloquée.

- **Nom d'origine du fichier exécutable** – `%ORIGINAL_FILE_NAME%`.

  Nom d'origine du fichier exécutable de l'application bloquée. Le nom du fichier est indiqué dans les propriétés du fichier exécutable de l'application.

- **Éditeur** – `%FILE_PUBLISHER%`.

  Fournisseur de l'application bloquée.

- **Nom de l'application** – `%FILE_PRODUCT_NAME%`.

  Nom de l'application bloquée.

- **Version de l'application** – `%PRODUCT_VERSION%`.

  Version de l'application bloquée.

- **Hachage du fichier exécutable** – `%FILE_HASH%`.

  Hachage du fichier exécutable de l'application bloquée.

- **Émetteur du certificat** – `%CERT_ISSUER%`.

  Émetteur du certificat avec lequel le fichier exécutable est signé.

- **Sujet du certificat** – `%CERT_SUBJECT%`.

  Objet du certificat avec lequel le fichier exécutable est signé.

- **Empreinte du certificat** – `%CERT_THUMBPRINT%`.

  Empreinte du certificat avec lequel le fichier exécutable est signé.

Bonnes pratiques relatives à l'inventaire des fichiers exécutables

La tâche *Inventory* collecte des informations sur les fichiers exécutables (par exemple, EXE, BAT et CMD), les modules DLL et les scripts (PowerShell, JS, entre autres). Ces informations sont nécessaires pour configurer les catégories du Contrôle des applications et les autorisations des applications pour le module Prévention des intrusions. La tâche *Inventory* doit être exécutée régulièrement afin de maintenir les informations à jour. La tâche *Inventory*, tout comme la tâche *Analyse des logiciels malveillants*, est gourmande en ressources. Par conséquent, nous vous recommandons de configurer l'exécution de la tâche la nuit ou le week-end.

Étapes de l'inventaire des fichiers exécutables

1. Sélectionnez le groupe d'ordinateurs de référence sur lesquels votre ensemble habituel de logiciels est installé. Nous vous recommandons de réduire au minimum le nombre d'ordinateurs utilisés pour la procédure d'inventaire des fichiers exécutables. Moins il y a de tâches *Inventory*, moins la charge sur le Serveur d'administration de Kaspersky Security Center est élevée.

2. Déplacez les ordinateurs de référence vers un groupe d'administration distinct dans la console Kaspersky Security Center. Vous pouvez nommer le groupe, par exemple, *Ordinateurs de référence*.

3. Créez une tâche *Inventory* pour le groupe d'administration *Ordinateurs de référence*. Nous vous recommandons de conserver les paramètres de tâche par défaut.

Exemple d'inventaire des fichiers exécutables dans une organisation

Par exemple, votre organisation compte 100 ordinateurs exécutant Windows 11 25H2. Tous les ordinateurs disposent de la même version et de la même localisation du système d'exploitation. L'ensemble des mises à jour installées sur les ordinateurs est également identique.

Dans une telle organisation, il n'est pas nécessaire d'exécuter la tâche *Inventory* sur tous les ordinateurs. La plupart des fichiers exécutables présents sur ces ordinateurs sont identiques. Il suffit de créer une tâche pour un ordinateur de référence. Vous pouvez créer des tâches *Inventory* supplémentaires pour les ordinateurs dont la configuration diffère de la configuration de référence.

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 dont le contenu a été ajouté 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 à partir du 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 reprend les fichiers exécutables d'un dossier particulier**. Vous pouvez indiquer le dossier qui contient les fichiers exécutables qui vont se retrouver automatiquement dans la catégorie d'applications créée.

   - **Catégorie qui reprend les fichiers exécutables issus d'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 **Catégorie principale** 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 *Catégorie principale* 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 **Catégorie principale** 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.

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. Créez ensuite la catégorie d'applications avec la condition **Dossier de l'application** et indiquez 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 à partir du 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, Protection contre les menaces Internet, Détection comportementale et Protection contre les Exploits 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.

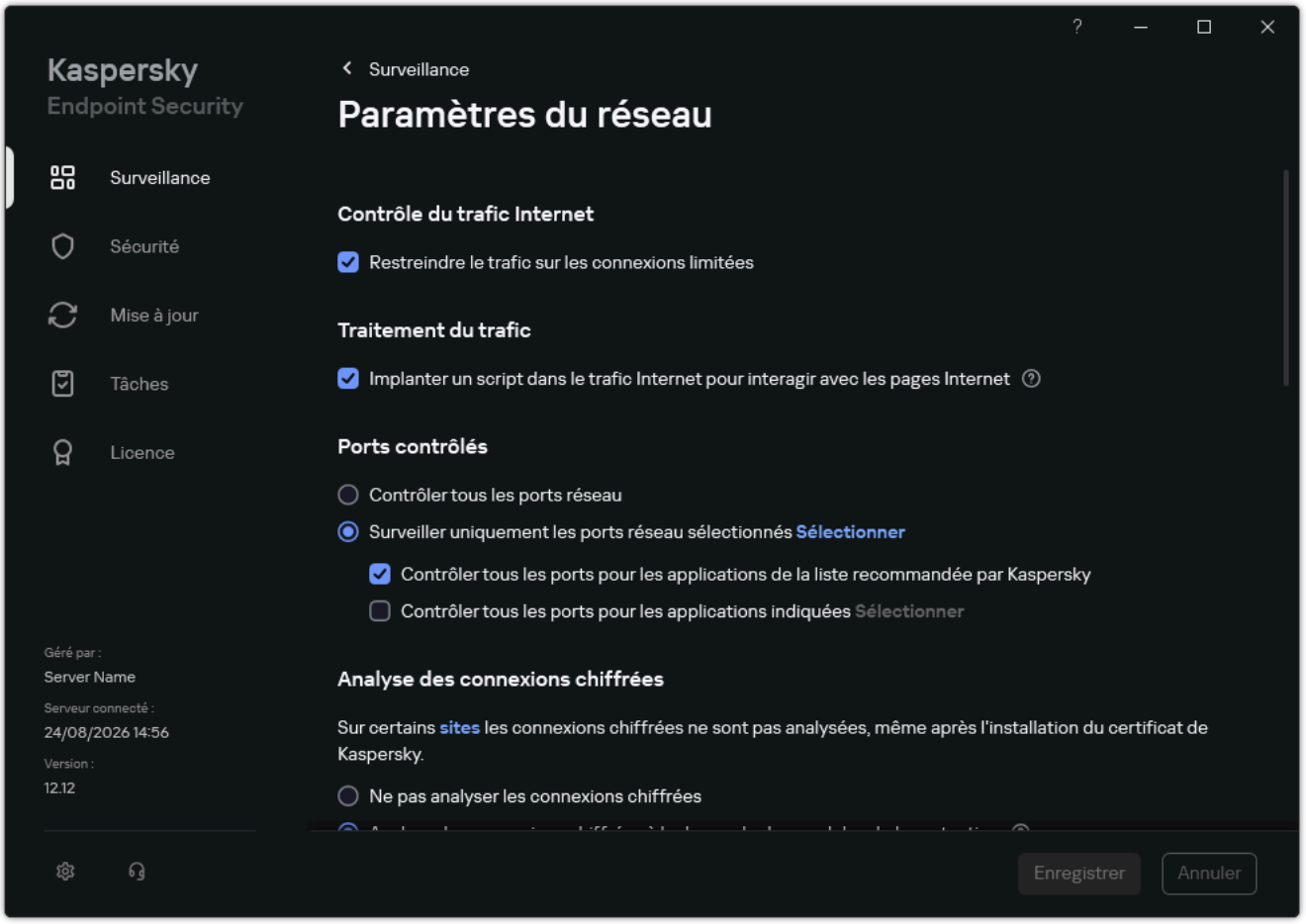
Pour garantir la sécurité de l'ordinateur, les modules Détection comportementale et Protection contre les Exploits contrôlent également les flux de données transitant par les ports du réseau. Les modules surveillent en permanence le trafic réseau à la recherche de processus individuels qui pourraient présenter une menace.

Activation du contrôle de tous les ports réseau

Pour activer le contrôle de tous les ports réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.



Paramètres du contrôle des ports 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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Surveiller uniquement les ports réseau sélectionnés**.
4. Cliquez sur **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 **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Surveiller 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 Acrobat 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 **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 **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. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez 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 **Surveiller uniquement les ports réseau sélectionnés**.
   b. Cliquez sur le lien **sélectionné X port**.

      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 **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. Enregistrez le fichier.

      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 **sélectionnée X application**.
   c. Dans la liste des applications, sélectionnez les applications que vous souhaitez exporter.
   d. Cliquez sur **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. Enregistrez le fichier.

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. Ouvrez le fichier.

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. Ouvrez le fichier.

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.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres du réseau**.

4. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Surveiller uniquement les ports réseau sélectionnés**.

5. Cliquez sur **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.

6. 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 **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. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste complète des ports réseau dans un fichier XML.

7. 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 **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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste complète des applications dans un fichier XML.

8. 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. Ouvrez le fichier.

      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.

9. 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. Ouvrez le fichier.

      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.

10. Enregistrez vos modifications.

Inspection des journaux

Ce module est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs. Ce module n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail.

L'inspection des journaux surveille l'intégrité de l'environnement protégé en fonction de l'analyse du journal des événements Windows. Lorsque l'application détecte des signes de comportement atypique dans le système, elle en informe l'administrateur, car ce comportement peut indiquer une tentative de cyberattaque.

Kaspersky Endpoint Security analyse les journaux d'événements Windows et détecte les violations conformément aux règles. Le module inclut des règles prédéfinies. Les règles prédéfinies sont alimentées par une analyse heuristique. Vous pouvez également ajouter vos propres règles (règles personnalisées). Lorsqu'une règle se déclenche, l'application crée un événement avec l'état *Critique* (voir la figure ci-dessous).

Si vous souhaitez utiliser l'inspection des journaux, assurez-vous que les paramètres de sécurité de la stratégie d'audit sont configurés et que le système enregistre les événements pertinents (pour en savoir plus, consultez le site du Support Technique Microsoft).

Notification d'inspection des journaux

Configuration des règles prédéfinies

Les règles prédéfinies incluent des modèles d'activité anormale sur l'ordinateur protégé. Une activité anormale peut signifier une tentative d'attaque. Les règles prédéfinies sont alimentées par une analyse heuristique. Sept règles prédéfinies sont disponibles pour l'inspection des journaux. Vous pouvez activer ou désactiver n'importe quelle règle. Les règles prédéfinies ne peuvent pas être supprimées.

Vous pouvez configurer les critères de déclenchement des règles qui surveillent les événements pour les opérations suivantes :

- Détection des attaques brute-force contre les mots de passe
- Traitement de la connexion au réseau

Comment configurer des règles prédéfinies dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Inspection des journaux**.
4. Assurez-vous que la case **Inspection des journaux** est cochée.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Règles prédéfinies**.
6. Cochez ou décochez les cases pour configurer des règles prédéfinies :
   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.

- **Certains comportements indiquent une possible violation du journal des événements Windows**.
- **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
- **Connexion inhabituelle utilisant des identifiants explicites**.
- **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.
- **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.

7. Si nécessaire ; configurez la règle **Certains comportements indiquent une possible attaque par force brute dans le système** :
   a. Cliquez sur le bouton **Paramètres** en dessous de la règle.
   b. Dans la fenêtre qui s'ouvre, indiquez le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle se déclenche.
   c. Cliquez sur le bouton **OK**.
8. Si vous avez sélectionné la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**, vous devez configurer ses paramètres :
   a. Cliquez sur le bouton **Paramètres** en dessous de la règle.
   b. Dans le groupe **Détection des connexions au réseau**, spécifiez le début et la fin de l'intervalle de temps.

      Kaspersky Endpoint Security considère les tentatives de connexion effectuées pendant l'intervalle défini comme une activité anormale.

      Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.
   c. Créez la liste des utilisateurs de confiance et des adresses IP de confiance (IPv4 et IPv6).

      Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Kaspersky Endpoint Security ne surveille pas les tentatives de connexion de ces utilisateurs et ordinateurs.
   d. Cliquez sur le bouton **OK**.
9. Enregistrez vos modifications.

Configuration des règles prédéfinies dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Contrôles de sécurité** → **Inspection des journaux**.

5. Assurez-vous que l'interrupteur **Inspection des journaux ACTIVÉE** est activé.

6. Dans le groupe **Règles prédéfinies**, activez ou désactivez les règles prédéfinies à l'aide des interrupteurs :

   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.
   - **Certains comportements indiquent une possible violation du journal des événements Windows**.
   - **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
   - **Connexion inhabituelle utilisant des identifiants explicites**.
   - **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.

   a. **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.

7. Si nécessaire ; configurez la règle **Certains comportements indiquent une possible attaque par force brute dans le système** :

   a. Cliquez sur **Paramètres** sous la règle.

   b. Dans la fenêtre qui s'ouvre, indiquez le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle se déclenche.

   c. Cliquez sur **OK**.

8. Si vous avez sélectionné la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**, vous devez configurer ses paramètres :

   a. Cliquez sur **Paramètres** sous la règle.

   b. Dans le groupe **Détection des connexions au réseau**, spécifiez le début et la fin de l'intervalle de temps.

      Kaspersky Endpoint Security considère les tentatives de connexion effectuées pendant l'intervalle défini comme une activité anormale.

      Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.

   c. Dans le groupe **Exclusions**, ajoutez des utilisateurs de confiance et des adresses IP de confiance (IPv4 et IPv6).

      Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Kaspersky Endpoint Security ne surveille pas les tentatives de connexion de ces utilisateurs et ordinateurs.

   d. Cliquez sur **OK**.

9. Enregistrez vos modifications.

Configuration des règles prédéfinies 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 **Contrôles de sécurité** → **Inspection des journaux**.
3. Assurez-vous que l'interrupteur **Inspection des journaux** est activé.
4. Cliquez sur le bouton **Configurer** dans le groupe **Règles prédéfinies**.
5. Cochez ou décochez les cases pour configurer des règles prédéfinies :
   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.
   - **Certains comportements indiquent une possible violation du journal des événements Windows**.
   - **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
   - **Connexion inhabituelle utilisant des identifiants explicites**.
   - **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.

   a. **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.
6. Si nécessaire ; configurez la règle **Certains comportements indiquent une possible attaque par force brute dans le système** :
   a. Cliquez sur **Paramètres** sous la règle.
   b. Dans la fenêtre qui s'ouvre, indiquez le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle se déclenche.
7. Si vous avez sélectionné la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**, vous devez configurer ses paramètres :
   a. Cliquez sur **Paramètres** sous la règle.
   b. Dans le groupe **Détection des connexions au réseau**, spécifiez le début et la fin de l'intervalle de temps.

      Kaspersky Endpoint Security considère les tentatives de connexion effectuées pendant l'intervalle défini comme une activité anormale.

      Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.

c. Dans le groupe **Exclusions**, ajoutez des utilisateurs de confiance et des adresses IP de confiance (IPv4 et IPv6).

   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Kaspersky Endpoint Security ne surveille pas les tentatives de connexion de ces utilisateurs et ordinateurs.

8. Enregistrez vos modifications.

Par conséquent, lorsque la règle se déclenche, Kaspersky Endpoint Security crée un *Événement critique*.

Ajout des règles personnalisées

Vous pouvez définir vos propres critères de déclenchement de règle d'inspection des journaux. Pour ce faire, vous devez entrer un ID d'événement et sélectionner une source d'événement. Vous pouvez rechercher l'ID d'événement sur le site du Support Technique de Microsoft. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Vous pouvez également spécifier le journal d'une application tierce. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal *Windows PowerShell*).

> L'application ne vérifie pas si le journal spécifié est bien présent dans le journal d'événements Windows. S'il y a une erreur dans le nom du journal, l'application ne surveille pas les événements de ce journal.

La liste des règles personnalisées comprend déjà trois règles créées par les experts de Kaspersky.

Ajout d'une règle personnalisée dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Inspection des journaux**.
4. Assurez-vous que la case **Inspection des journaux** est cochée.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Règles personnalisées**.
6. Dans la fenêtre qui s'ouvre, cochez les cases à côté des règles personnalisées que vous souhaitez activer.
7. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.
8. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :
   - **Nom de la règle**.
   - **Nom du journal**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.

- **Source**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal *Windows PowerShell*).

- **Identificateurs des événements**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

9. Enregistrez vos modifications.

Ajout d'une règle personnalisée dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Inspection des journaux**.

5. Assurez-vous que l'interrupteur **Inspection des journaux ACTIVÉE** est activé.

6. Dans le groupe **Règles personnalisées**, sélectionnez les règles personnalisées que vous souhaitez activer.

7. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.

8. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :

   - **Nom de la règle**.

   - **Nom personnalisé du journal**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.

   - **Provenance**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal *Windows PowerShell*).

   - **Identificateurs des événements**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

9. Enregistrez vos modifications.

Ajout d'une règle personnalisée 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 **Contrôles de sécurité** → **Inspection des journaux**.

3. Assurez-vous que l'interrupteur **Inspection des journaux** est activé.

4. Cliquez sur le bouton **Configurer** dans le groupe **Règles personnalisées**.

5. Dans la fenêtre qui s'ouvre, cochez les cases à côté des règles personnalisées que vous souhaitez activer.

6. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.

7. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :

- **Nom de la règle**.
- **Nom du journal**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.
- **Source**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal *Windows PowerShell*).
- **Identificateur des événements**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

8. Enregistrez vos modifications.

Par conséquent, lorsque la règle se déclenche, Kaspersky Endpoint Security crée un événement *Critique*.

Contrôle de l'intégrité du système

Ce module est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs. Ce module n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail.

À partir de la version 12.6, Kaspersky Endpoint Security for Windows inclut le module Contrôle de l'intégrité du système au lieu du module Contrôle de l'intégrité des fichiers. Le module Contrôle de l'intégrité du système inclut toutes les fonctionnalités du Contrôle de l'intégrité des fichiers et permet également de surveiller les modifications apportées au registre et la connexion d'appareils externes.

Le module Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Endpoint Security génère les événements correspondants et en informe l'administrateur. Le Contrôle de l'intégrité du système peut fonctionner en mode temps réel et peut également effectuer des vérifications de l'intégrité du système sur demande.

Contrôle de l'intégrité du système en temps réel

En mode temps réel, le Contrôle de l'intégrité du système suit les modifications apportées aux objets que vous avez inclus dans le champ d'application du module (la *zone de surveillance*). Le Contrôle de l'intégrité du système permet également de bloquer en temps réel l'accès non autorisé à ces objets.

Vérification de l'intégrité du système sur demande

La Vérification de l'intégrité du système sur demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Pour exécuter la tâche *Vérification de l'intégrité du système*, vous devez configurer la zone d'application du module (la *zone de surveillance*) et créer une référence. Une *référence* est un état enregistré des objets dans le système, que l'application utilise comme référence lors de la comparaison avec l'état actuel.

Migration des paramètres du Contrôle de l'intégrité des fichiers

Lorsque vous mettez à jour Kaspersky Endpoint Security vers la version 12.6, les paramètres du Contrôle de l'intégrité des fichiers sont migrés automatiquement. Dans le cadre de la migration, l'application déplace les règles de surveillance vers le Contrôle de l'intégrité du système. Les règles du Contrôle de l'intégrité des fichiers sont également migrées vers le Contrôle de l'intégrité du système lors d'une migration depuis KSWS vers KES.

> Pour garantir le bon fonctionnement du Contrôle de l'intégrité du système, l'application et le plug-in d'administration Kaspersky Endpoint Security doivent être mis à jour vers la version 12.6. Si une version antérieure du plug-in d'administration est installée, vous ne pouvez pas configurer le Contrôle de l'intégrité du système parce que le plug-in d'administration ne dispose pas de la section **Contrôle de l'intégrité du système**.

À propos des règles du Contrôle de l'intégrité du système

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une *règle du Contrôle de l'intégrité du système* est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers et au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers et dans le registre à l'intérieur de la *zone de surveillance* spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système.

Le Contrôle de l'intégrité du système permet de surveiller les objets suivants :

- Fichiers
- Registre
- Appareils externes

Considérations particulières liées à la surveillance des fichiers

Le Contrôle de l'intégrité du système surveille les modifications dans les fichiers et les dossiers, ainsi que les fichiers ajoutés ou supprimés de la zone de surveillance. Ces changements peuvent indiquer une faille de sécurité informatique. Il est conseillé d'ajouter des objets rarement modifiés ou des objets auxquels seul l'administrateur a accès. Cette mesure permettra de réduire le nombre d'événements du Contrôle de l'intégrité du système.

> Le Contrôle de l'intégrité du système ne contrôle pas les modifications apportées aux fichiers dans les dossiers partagés du serveur. Le Contrôle de l'intégrité du système peut être utilisé uniquement localement.

Kaspersky Endpoint Security surveille les modifications des fichiers et des dossiers uniquement sur les disques connectés au moment où le Contrôle de l'intégrité du système en temps réel a commencé à fonctionner. Si un disque n'était pas connecté lorsque le Contrôle de l'intégrité du système en temps réel a commencé à fonctionner, l'application ne surveille pas les modifications des fichiers et des dossiers sur ce disque même si les fichiers et les dossiers sont ajoutés à la zone de surveillance.

Considérations particulières liées à la surveillance du registre

Le Contrôle de l'intégrité du système surveille le registre. Ces changements peuvent indiquer une faille de sécurité informatique.

Le Contrôle de l'intégrité du système surveille les clés racine suivantes du registre :

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (disponible uniquement dans le Contrôle de l'intégrité du système en temps réel)
- `HKEY_CURRENT_USER` (disponible uniquement dans le Contrôle de l'intégrité du système en temps réel)

> La tâche *Vérification de l'intégrité du système* ne prend pas en charge la clé `HKEY_CURRENT_USER`. Vous pouvez spécifier une clé sous `HKEY_USERS` en tant que `HKEY_USERS\<user profile ID>\<key>`.

Considérations particulières liées à la surveillance des appareils externes

Le Contrôle de l'intégrité du système surveille la connexion et la déconnexion des appareils externes. Ceci est nécessaire afin de protéger l'ordinateur contre les menaces de sécurité pouvant résulter de l'échange de fichiers avec de tels appareils. Le Contrôle de l'intégrité du système ne surveille pas l'accès aux appareils externes et ne bloque pas l'échange de fichiers. Vous pouvez configurer l'accès aux appareils à l'aide d'un autre module d'application, à savoir le Contrôle des appareils.

> Lors de l'exécution de la tâche *Contrôle de l'intégrité du système par rapport à une référence*, l'application ignore la reconnexion des appareils externes si ceux-ci présentent la même lettre de lecteur dans le système d'exploitation. Pour être journalisés, les appareils reconnectés doivent avoir des lettres de lecteur différentes.

Le Contrôle de l'intégrité du système surveille la connexion des types d'appareils externes suivants :

- Disque amovible (y compris les clés USB)
- Disque dur
- Adaptateur réseau externe

- Disque CD/DVD/Blu-ray
- Scanner/caméra

Contrôle de l'intégrité du système en temps réel

Le Contrôle de l'intégrité du système permet de suivre en temps réel les modifications du système d'exploitation. Vous pouvez suivre les modifications susceptibles d'indiquer des atteintes à la sécurité sur l'ordinateur. Le module permet de bloquer ces modifications ou de consigner simplement les événements liés aux modifications.

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une *règle du Contrôle de l'intégrité du système* est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers et au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers et dans le registre à l'intérieur de la *zone de surveillance* spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système.

Modes du Contrôle de l'intégrité du système en temps réel

Pour s'assurer que les règles du Contrôle de l'intégrité du système ne bloquent aucune action liée à des ressources essentielles au bon fonctionnement du système d'exploitation ou d'autres services, il est conseillé d'activer le mode Test et d'analyser l'impact du module sur le système. Lorsque le mode Test est activé, Kaspersky Endpoint Security ne bloque pas l'activité de l'utilisateur interdite par les règles, mais génère à la place des événements *Avertissement* ⚠.

Le module Contrôle de l'intégrité du système en temps réel possède deux modes :

- Bloquer

  Dans ce mode, le Contrôle de l'intégrité du système suit les modifications dans le système et exécute une action conformément aux règles : **Autoriser** ou **Bloquer**. Le Contrôle de l'intégrité du système génère également un événement correspondant et modifie l'état de l'appareil dans la console de Kaspersky Security Center.

- Informer

  Dans ce mode, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance. Si les actions avec les fichiers ou le registre sont interdites, l'application génère un événement : *L'opération interdite a été autorisée en mode test*. Pour analyser l'impact des règles sur le système, vous pouvez consulter les rapports.

Activation du Contrôle de l'intégrité du système en temps réel

Comment activer le Contrôle de l'intégrité du système en temps réel dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

4. Cochez la case **Contrôle de l'intégrité du système**.

5. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour le Contrôle de l'intégrité du système en temps réel :

   - **Bloquer**. Dans ce mode, le Contrôle de l'intégrité du système bloque les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

   - **Informer**. Dans ce mode, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

6. Dans le groupe **Contrôle de l'intégrité du système en temps réel**, cochez la case **Contrôle de l'intégrité du système en temps réel**.

7. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif* ⓘ, *Avertissement* ⚠ ou *Critique* ⓘ.

   Le Contrôle de l'intégrité du système enregistre la connexion actuelle d'appareils externes. Après l'activation du module dans les paramètres de l'application, l'application commence à surveiller les connexions et les déconnexions d'appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant.

8. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Paramètres**.

      La liste des règles du Contrôle de l'intégrité du système s'ouvre.

   c. Cliquez sur **Ajouter**.

      Vous pouvez également importer des règles depuis une autre source.

   d. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment activer le Contrôle de l'intégrité du système en temps réel dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

5. Activez le commutateur **Contrôle de l'intégrité du système ACTIVÉ**.

6. Sélectionnez l'onglet **Windows**.

7. Sous **Contrôle de l'intégrité du système en temps réel**, sélectionnez un mode pour le Contrôle de l'intégrité du système en temps réel :

   - **Appliquer les règles**. Dans ce mode, le Contrôle de l'intégrité du système bloque les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

   - **Règles de test (informer)**. Dans ce mode, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

8. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Règles**.

   La liste des règles du Contrôle de l'intégrité du système s'ouvre.

   c. Cliquez sur **Ajouter**.

   Vous pouvez également importer des règles depuis une autre source.

   d. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

9. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif*, *Avertissement* ou *Critique*.

   Le Contrôle de l'intégrité du système enregistre la connexion actuelle d'appareils externes. Après l'activation du module dans les paramètres de l'application, l'application commence à surveiller les connexions et les déconnexions d'appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer le Contrôle de l'intégrité du système en temps réel 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 **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

3. Activez le commutateur **Contrôle de l'intégrité du système**.

4. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour le Contrôle de l'intégrité du système en temps réel :

   - **Bloquer**. Dans ce mode, le Contrôle de l'intégrité du système bloque les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

   - **Informer**. Dans ce mode, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.

5. Dans le groupe **Contrôle de l'intégrité du système en temps réel**, cochez la case **Contrôle de l'intégrité du système en temps réel**.

6. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif* ⓘ, *Avertissement* ⚠ ou *Critique* ⓘ.

   Le Contrôle de l'intégrité du système enregistre la connexion actuelle d'appareils externes. Après l'activation du module dans les paramètres de l'application, l'application commence à surveiller les connexions et les déconnexions d'appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant.

7. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Configurer**.

      La liste des règles du Contrôle de l'intégrité du système s'ouvre.

   c. Cliquez sur **Ajouter**.

      Vous pouvez également importer des règles depuis une autre source.

8. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

9. Enregistrez vos modifications.

Paramètres de la règle du Contrôle de l'intégrité du système en temps réel

Paramètre	Description
Nom de la règle	Nom de la règle du Contrôle de l'intégrité du système en temps réel
Opérations sur les fichiers et le registre	• **Autoriser**. Le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance. • **Bloquer**. Le comportement du Contrôle de l'intégrité du système dépend du mode sélectionné. Si vous avez sélectionné le *mode de protection du système*, le Contrôle de l'intégrité du système bloque les actions avec les fichiers et les clés de registre de la zone de surveillance, génère un événement correspondant et modifie l'état de l'appareil dans la console de Kaspersky Security Center. Si vous avez sélectionné le *mode Test*, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance.

Paramètre	Description
Niveau de gravité de l'événement	Kaspersky Endpoint Security enregistre les événements de modification de fichier chaque fois qu'un fichier ou une clé de registre de la zone de surveillance est modifié. Les niveaux de gravité d'événement suivants sont disponibles : *Informatif*, *Avertissement*, *Critique*.

Zone de surveillance	• **Fichier**. Liste des fichiers et des dossiers surveillés par le module. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
	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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
	• **Registre**. Liste des clés et des valeurs de registre surveillées par le module. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exclusions	• **Fichier**. Liste des exclusions de la zone de surveillance. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Par exemple, `C:\Folder\Application\*.log`. Les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.
	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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
	• **Registre**. Liste des exclusions de la zone de surveillance. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. Les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.

Utilisateurs et/ou groupes d'utilisateurs de confiance	Un *utilisateur de confiance* est un utilisateur qui est autorisé à exécuter des actions avec les fichiers et les clés de registre dans la zone de surveillance. Si Kaspersky Endpoint Security détecte une action effectuée par un utilisateur de confiance, le Contrôle de l'intégrité du système génère un événement *Informatif*. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.
Marqueurs d'opérations sur les fichiers/Opérations contrôlées	Marqueurs caractérisant l'action avec les fichiers ou les clés de registre que l'application va surveiller.
Hachage	Calcul du hachage d'un fichier lors de sa modification. Kaspersky Endpoint Security ajoute des informations relatives au hachage du fichier lorsqu'un événement est généré.

Vérification de l'intégrité du système sur demande

La Vérification de l'intégrité du système sur demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Lors de l'exécution de la tâche *Vérification de l'intégrité du système*, l'application compare l'état actuel des objets inclus dans la zone de surveillance avec leur état *de référence*. Contrairement au Contrôle de l'intégrité du système en temps réel, la tâche *Vérification de l'intégrité du système* aide à limiter le nombre d'événements et permet de générer un rapport global sur les modifications du système d'exploitation.

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une *règle du Contrôle de l'intégrité du système* est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers et au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers et dans le registre à l'intérieur de la *zone de surveillance* spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système. Vous pouvez configurer des règles qui seront partagées par le Contrôle de l'intégrité du système en temps réel et par la tâche *Vérification de l'intégrité du système* ou créer des règles distinctes pour la tâche. Pour créer une référence, Kaspersky Endpoint Security applique la zone de surveillance de la tâche *Vérification de l'intégrité du système* à la tâche *Mise à jour de la référence*.

Création et mise à jour d'une référence

La tâche *Vérification de l'intégrité du système* a besoin d'une référence pour fonctionner. Une *référence* est un état enregistré des objets dans le système, que l'application utilise comme référence lors de la comparaison avec l'état actuel. Si l'état actuel du système est différent de l'état du système enregistré dans la référence, Kaspersky Endpoint Security génère l'événement correspondant. Vous pouvez créer ou mettre à jour une référence à l'aide de la tâche *Mise à jour de la référence*.

Vous pouvez mettre à jour la référence dans les modes suivants :

- Mise à jour complète.

  L'application met à jour tous les objets dans la zone de surveillance.

- Mise à jour progressive.

  L'application détecte et met à jour les objets nouveaux ou modifiés uniquement.

Comment créer ou mettre à jour une référence dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Mise à jour de la référence**.

Étape 2. Sélection du mode de mise à jour de la référence

Sélectionnez un mode de mise à jour de la référence :

- **Mise à jour complète**. L'application met à jour tous les objets dans la zone de surveillance.
- **Mise à jour incrémentale**. L'application détecte et met à jour les objets nouveaux ou modifiés uniquement.

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 le nom de la tâche, par exemple *Référence 2024*.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment créer ou mettre à jour une référence dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Mise à jour de la référence**.

c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Référence 2024*.

d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Sélectionnez un mode de mise à jour de la référence :

   - **Mise à jour complète**. L'application met à jour tous les objets dans la zone de surveillance.

   - **Mise à jour incrémentale**. L'application détecte et met à jour les objets nouveaux ou modifiés uniquement.

10. Enregistrez vos modifications.

11. Cochez la case en regard de la tâche.

12. Cliquez sur **Démarrer**.

Configuration de la zone de surveillance pour la tâche Vérification de l'intégrité du système

Par défaut, la zone de surveillance de la tâche *Vérification de l'intégrité du système* est identique à la zone de surveillance du Contrôle de l'intégrité du système en temps réel. Vous pouvez configurer une autre zone de surveillance pour la tâche.

> Le Contrôle de l'intégrité du système ne prend pas en charge l'importation des clés `HKEY_CURRENT_USER` et `HKEY_CURRENT_CONFIG` pour la tâche *Vérification de l'intégrité du système*. Si la zone de surveillance de la tâche contient ces clés, l'application génère l'événement *La zone de surveillance inclut des objets incorrects*.

Comment configurer une autre zone de surveillance pour la tâche Vérification de l'intégrité du système dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

4. Cochez la case **Contrôle de l'intégrité du système**.

5. Sous **Vérification de l'intégrité du système**, sélectionnez le mode de configuration de la tâche : **Paramètres personnalisés**.

6. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif* ⓘ, *Avertissement* ⚠ ou *Critique* ⓘ.

   Le Contrôle de l'intégrité du système enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche *Vérification de l'intégrité du système*, l'application ne surveille pas la déconnexion des appareils externes.

7. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Paramètres**.

      La liste des règles du Contrôle de l'intégrité du système s'ouvre.

   c. Cliquez sur **Ajouter**.

      Vous pouvez également importer des règles depuis une autre source.

   d. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

8. Enregistrez vos modifications.

Comment configurer une autre zone de surveillance pour la tâche Vérification de l'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

5. Sélectionnez l'onglet **Windows**.

6. Activez le commutateur **Contrôle de l'intégrité du système ACTIVÉ**.

7. Sous **Vérification de l'intégrité du système**, sélectionnez le mode de configuration de la tâche : **Paramètres personnalisés**.

8. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif* ⓘ, *Avertissement* ⚠ ou *Critique* ⓘ.

Le Contrôle de l'intégrité du système enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche *Vérification de l'intégrité du système*, l'application ne surveille pas la déconnexion des appareils externes.

9. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Règles**.

      La liste des règles du Contrôle de l'intégrité du système s'ouvre.

   c. Cliquez sur **Ajouter**.

      Vous pouvez également importer des règles depuis une autre source.

   d. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

10. Enregistrez vos modifications.

Comment configurer une autre zone de surveillance pour la tâche Vérification de l'intégrité du système 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 **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

3. Activez le commutateur **Contrôle de l'intégrité du système**.

4. Sous **Vérification de l'intégrité du système**, sélectionnez le mode de configuration de la tâche : **Paramètres personnalisés**.

5. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif* ⓘ, *Avertissement* ⚠ ou *Critique* ⓘ.

   Le Contrôle de l'intégrité du système enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche *Vérification de l'intégrité du système*, l'application ne surveille pas la déconnexion des appareils externes.

6. Configurez la surveillance des fichiers et du registre :

   a. Cochez la case **Surveiller les fichiers et le registre**.

   b. Cliquez sur **Configurer**.

      La liste des règles du Contrôle de l'intégrité du système s'ouvre.

c. Cliquez sur **Ajouter**.

Vous pouvez également importer des règles depuis une autre source.

d. Configurez la règle du Contrôle de l'intégrité du système (voir le tableau ci-dessous).

7. Enregistrez vos modifications.

Paramètres d'une règle de la tâche Vérification de l'intégrité du système

Paramètre	Description
Nom de la règle	Nom de la règle de la tâche *Vérification de l'intégrité du système*.
Niveau de gravité de l'événement	Kaspersky Endpoint Security enregistre les événements de modification de fichier chaque fois qu'un fichier ou une clé de registre de la zone de surveillance est modifié. Les niveaux de gravité d'événement suivants sont disponibles : *Informatif*, *Avertissement*, *Critique*.

Zone de surveillance	• **Fichier**. Liste des fichiers et des dossiers surveillés par le module. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
	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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
	• **Registre**. Liste des clés et des valeurs de registre surveillées par le module. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Exclusions	• **Fichier**. Liste des exclusions de la zone de surveillance. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Par exemple, `C:\Folder\Application\*.log`. Les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.
	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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
	• **Registre**. Liste des exclusions de la zone de surveillance. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. Les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.

Lancement de la tâche Vérification de l'intégrité du système

La tâche *Vérification de l'intégrité du système* permet de vérifier si des fichiers ou des clés de registre ont été modifiés et de contrôler la connexion d'appareils externes. Pour vérifier si des fichiers ont été modifiés, vous pouvez exécuter la tâche *Vérification de l'intégrité du système* dans les modes suivants :

- Analyse rapide.

  Lors de la recherche de modifications dans les fichiers, les applications vérifient uniquement les attributs des fichiers. L'application ne vérifie pas le contenu des fichiers.

- Analyse complète.

  Lors de la recherche de modifications dans les fichiers, les applications vérifient tous les attributs des fichiers ainsi que le contenu des fichiers.

Le mode d'exécution de la tâche n'influence pas la vérification du registre ou des appareils externes.

Comment lancer la tâche Vérification de l'intégrité du système dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

3. Cliquez sur **Nouvelle tâche**.

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

4. Sélectionnez **Kaspersky Endpoint Security → Contrôle de l'intégrité du système par rapport à une référence**. Sélectionnez un mode de Contrôle de l'intégrité du système :

   - **Analyse complète**. Dans ce mode, l'application vérifie tous les attributs et tous les hachages des fichiers.

   - **Analyse rapide**. Dans ce mode, l'application vérifie uniquement les attributs des fichiers.

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

   - 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.

   - Indiquez la sélection d'appareils pour lesquels vous souhaitez exécuter la tâche.

   - 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.

6. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

7. Définissez une planification pour le lancement d'une tâche, par exemple, manuellement ou un jour particulier de la semaine.

8. Saisissez un nom pour la tâche.

9. Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment lancer une tâche Vérification de l'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Vérification de l'intégrité du système**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Contrôle hebdomadaire de l'intégrité du système*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Sélectionnez un mode de Vérification de l'intégrité du système :

   - **Analyse rapide**. L'application vérifie uniquement les attributs des fichiers. L'application ne vérifie pas le contenu des fichiers.

   - **Analyse complète**. L'application vérifie tous les attributs des fichiers ainsi que leur contenu.

10. Enregistrez vos modifications.

11. Cochez la case en regard de la tâche.

12. Cliquez sur **Démarrer**.

Pour que la tâche *Vérification de l'intégrité du système* puisse se terminer correctement, la zone de surveillance de la tâche *Vérification de l'intégrité du système* doit correspondre complètement à la référence. Si la zone de surveillance est différente, la tâche se termine sur une erreur. Pour synchroniser les zones de surveillance, exécutez la tâche *Mise à jour de la référence* avec une nouvelle zone de surveillance.

Exportation et importation des règles du Contrôle de l'intégrité du système

Vous pouvez exporter la liste des règles du Contrôle de l'intégrité du système vers un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'enregistrements du même type. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles du Contrôle de l'intégrité du système ou pour procéder à la migration de la liste vers un autre serveur.

Le Contrôle de l'intégrité du système ne prend pas en charge l'importation des clés `HKEY_CURRENT_USER` et `HKEY_CURRENT_CONFIG` pour la tâche *Vérification de l'intégrité du système*. Si la zone de surveillance de la tâche contient ces clés, l'application génère l'événement *La zone de surveillance inclut des objets incorrects*.

Comment exporter et importer une liste de règles du Contrôle de l'intégrité du système dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.
4. Pour exporter ou importer des règles du *Contrôle de l'intégrité du système en temps réel*, procédez comme suit :
   a. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle de l'intégrité du système en temps réel**.
   b. Pour exporter une liste des règles du Contrôle de l'intégrité du système en temps réel, procédez comme suit :
      1. 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.
      2. Cliquez sur le lien **Exporter**.
      3. 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.
      4. Enregistrez le fichier.

         Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.

c. Pour importer une liste des règles du Contrôle de l'intégrité du système en temps réel, procédez comme suit :

1. 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.

2. Ouvrez le fichier.

   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.

5. Pour exporter ou importer des règles de la *Vérification de l'intégrité du système*, procédez comme suit :

a. Dans le groupe **Vérification de l'intégrité du système**, sélectionnez l'option **Paramètres personnalisés**.

b. Cliquez sur **Paramètres**.

c. Pour exporter la liste des règles de la Vérification de l'intégrité du système, procédez comme suit :

1. 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.

2. Cliquez sur le lien **Exporter**.

3. 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.

4. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.

d. Pour importer une liste des règles de la Vérification de l'intégrité du système, procédez comme suit :

1. 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.

2. Ouvrez le fichier.

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.

6. Enregistrez vos modifications.

Comment exporter et importer une liste du Contrôle de l'intégrité du système dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Contrôles de sécurité** → **Contrôle de l'intégrité du système**.

5. Sélectionnez l'onglet **Windows**.

6. Pour exporter ou importer des règles du *Contrôle de l'intégrité du système en temps réel*, procédez comme suit :

   a. Dans le groupe **Contrôle de l'intégrité du système en temps réel**, cliquez sur le lien **Règles**.

   b. Pour exporter une liste des règles du Contrôle de l'intégrité du système en temps réel, procédez comme suit :

      1. Sélectionnez les règles que vous souhaitez exporter.

      2. Appuyez sur le bouton → **Exporter**.

         Kaspersky Endpoint Security exporte la liste des règles dans un fichier JSON dans le dossier des téléchargements par défaut.

   c. Pour importer une liste des règles du Contrôle de l'intégrité du système en temps réel, procédez comme suit :

      1. Appuyez sur le bouton → **Importer**.

         Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des adresses de confiance.

      2. Ouvrez le fichier.

         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 JSON.

7. Pour exporter ou importer des règles de la *Vérification de l'intégrité du système*, procédez comme suit :

   a. Dans le groupe **Vérification de l'intégrité du système sur demande**, sélectionnez l'option **Paramètres personnalisés**.

   b. Cliquez sur le lien **Règles**.

   c. Pour exporter la liste des règles de la Vérification de l'intégrité du système, procédez comme suit :

      1. Sélectionnez les règles que vous souhaitez exporter.

      2. Appuyez sur le bouton → **Exporter**.

         Kaspersky Endpoint Security exporte la liste des règles dans un fichier JSON dans le dossier des téléchargements par défaut.

   d. Pour importer une liste des règles de la Vérification de l'intégrité du système, procédez comme suit :

      1. Appuyez sur le bouton → **Importer**.

         Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des adresses de confiance.

2. Ouvrez le fichier.

   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 JSON.

8. Enregistrez vos modifications.

Affichage des rapports du Contrôle de l'intégrité du système

Pour analyser les performances des règles du Contrôle de l'intégrité du système, vous pouvez consulter les rapports et les événements générés par l'application. Kaspersky Endpoint Security génère les rapports suivants concernant le module :

- Dans l'interface de l'application :
  - Rapport du Contrôle de l'intégrité du système
  - Rapport de la Vérification de l'intégrité du système
  - Rapport de la Mise à jour de la référence

  Les rapports contiennent des événements du Contrôle de l'intégrité du système.

- Dans Kaspersky Security Center Console :
  - Rapport sur les ordinateurs sur lesquels les règles de surveillance ont été appliquées le plus grand nombre de fois
  - Rapport sur les règles de surveillance les plus fréquemment appliquées

  Par défaut, un rapport est créé pour les 30 jours précédents, en incluant la date de création du rapport.

  Comment consulter les rapports du Contrôle de l'intégrité du système dans la Console d'administration (MMC)

  1. Ouvrez la Console d'administration de Kaspersky Security Center.
  2. Dans le nœud **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
  3. Cliquez sur **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 de rapport**, sélectionnez un rapport du Contrôle de l'intégrité du système (la section **Autres**) :
     - **Top 10 des appareils dont les règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système sont le plus souvent déclenchées**.
     - **Top 10 des règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système qui ont été le plus souvent déclenchées sur les appareils**.

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.

Comment consulter les rapports du Contrôle de l'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Surveillance** → **Rapports**.

2. Cliquez sur **Ajouter**.

   L'Assistant de création du modèle du rapport démarre.

3. Sous **Type de modèle**, dans la section **Autre**, sélectionnez un rapport du Contrôle de l'intégrité du système :

   - **Top 10 des appareils dont les règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système sont le plus souvent déclenchées**.

   - **Top 10 des règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système qui ont été le plus souvent déclenchées sur les appareils**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau.

4. Sélectionnez et exécutez le rapport.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Pour consulter les événements générés par l'application, vous pouvez également utiliser les sélections d'événements dans la console de Kaspersky Security Center.

Réinitialisation de l'état de l'intégrité du système

Les ordinateurs dans la console de Kaspersky Security Center présentent un des états suivants : *OK*, *Avertissement* ou *Critique*. Si le Contrôle de l'intégrité du système détecte une modification de fichiers ou de clés de registre dans la zone de surveillance, l'état de l'ordinateur passe à *Avertissement* ou *Critique*. L'état attribué par le Contrôle de l'intégrité du système est appelé *état d'intégrité du système*. Vous pouvez réinitialiser l'état d'intégrité du système, par exemple, si l'analyse vous a permis de déterminer que la modification détectée des objets n'affecte pas la sécurité de l'ordinateur.

Comment réinitialiser l'état d'intégrité du système dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Réinitialisation de l'état d'intégrité du système**.

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

Configurez la planification de la tâche, par exemple, manuellement.

Étape 4. Définition du nom de la tâche

Saisissez le nom de la tâche, par exemple, *Réinitialisation de l'état après la modification de la zone de surveillance*.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment réinitialiser l'état d'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Réinitialisation de l'état d'intégrité du système**.

   c. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple, *Réinitialisation de l'état après la modification de la zone de surveillance*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Endpoint Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cochez la case en regard de la tâche.

8. Cliquez sur **Démarrer**.

Par conséquent, si l'état de l'ordinateur est passé à *Avertissement* ou *Critique* en raison des événements du Contrôle de l'intégrité du système, l'état de l'ordinateur est réinitialisé sur *OK*. Si l'état de l'ordinateur a également été modifié en raison d'autres événements, l'état de l'ordinateur reste inchangé.

Cloud Discovery

Cloud Discovery gère l'accès des utilisateurs aux services cloud. Les services cloud comprennent, par exemple, Microsoft Teams, Salesforce et Microsoft Office 365. Les services cloud sont regroupés en catégories, par exemple, *Stockage de fichiers*, *Clients de messagerie* ou *Email*. Les experts de Kaspersky mettent régulièrement à jour les catégories de Cloud Discovery et les services cloud classés dans les catégories. Kaspersky Endpoint Security met à jour l'ensemble des catégories et des services cloud avec les bases de données des applications. Cela signifie que Cloud Discovery n'utilise pas Kaspersky Security Network pour catégoriser les services cloud.

Cloud Discovery offre les fonctionnalités suivantes :

- Surveillance de l'utilisation des services cloud
- Blocage de l'accès des utilisateurs aux services cloud

Configuration requise

Cloud Discovery est disponible si les conditions suivantes sont remplies :

- L'application est installée sur un ordinateur fonctionnant sous Windows pour les postes de travail.

  Le module n'est pas disponible pour les serveurs.

- Kaspersky Security Center version 15.1 ou toute version ultérieure.

  Le module n'est pas disponible dans la Console d'administration (MMC). Vous pouvez configurer Cloud Discovery dans Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console.

- Licence Kaspersky Next.

Activez la fonctionnalité de l'application requise par le module Cloud Discovery :

1. **Analyser les connexions chiffrées**. Cette action est nécessaire pour assurer la surveillance du trafic HTTPS. Vous pouvez gérer cette fonctionnalité dans la section **Paramètres du réseau**.

2. **Implanter un script dans le trafic Internet pour interagir avec les pages Internet**. Le script permet l'enregistrement des événements de Cloud Discovery. Le script fournit également un blocage complet de l'accès aux services cloud. Sans le script, l'application bloque l'accès uniquement par les domaines de services cloud. Vous pouvez gérer cette fonctionnalité dans la section **Paramètres du réseau**.

Vous pouvez également activer la fonctionnalité **Enregistrer les données relatives aux visites des pages autorisées dans le journal**. La fonctionnalité comprend le regroupement d'événements lorsqu'un utilisateur visite des pages Internet appartenant au même domaine. Ainsi, lorsqu'un utilisateur utilise un service cloud, Cloud Discovery ne consigne qu'un seul événement au lieu de plusieurs événements pour chaque page Internet. Vous pouvez gérer cette fonctionnalité dans la section **Contrôle Internet**.

Surveillance des services cloud

Lorsqu'un utilisateur commence à utiliser un service cloud, Kaspersky Endpoint Security enregistre cet événement et crée une entrée dans le rapport. Cloud Discovery contrôle l'utilisation des services cloud dans le navigateur ainsi que dans les applications correspondantes. Cloud Discovery contrôle l'utilisation des services cloud via HTTP et HTTPS.

Comment activer la surveillance des services cloud dans Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Cloud Discovery**.

5. Activez le commutateur **Cloud Discovery ACTIVÉ**.

6. Enregistrez vos modifications.

L'application transmet alors à Kaspersky Security Center des informations sur les services cloud utilisés. Vous pouvez consulter les informations relatives à l'utilisation des services cloud dans des rapports. Si nécessaire, vous pouvez bloquer l'accès aux services cloud.

Blocage de l'accès aux services cloud

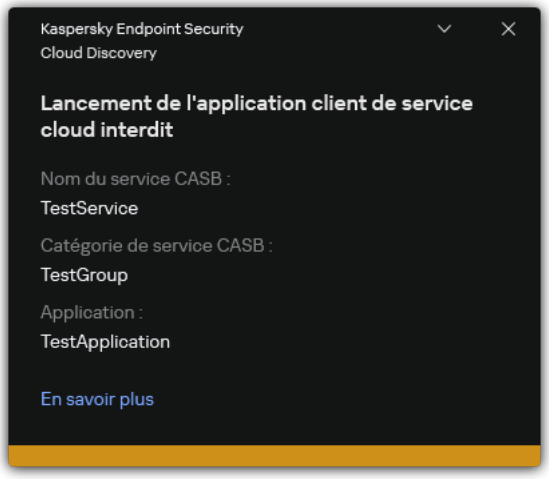
Le blocage de l'accès aux services cloud n'est disponible que pour la licence Kaspersky Next EDR Optimum et XDR Expert. Cette fonctionnalité n'est pas disponible pour la licence Kaspersky Next EDR Foundations. Comparaison des fonctionnalités de l'application en fonction du type de licence de Kaspersky Next, voir l'aide de Kaspersky Next.

L'administrateur peut restreindre l'accès des utilisateurs à des catégories de Cloud Discovery ou à des services cloud individuels. Ainsi, l'administrateur peut autoriser uniquement les services cloud sécurisés et éviter les fuites de données. Les *informations relatives au niveau de risque* sont affichées pour chaque service cloud dans Cloud Discovery. Le niveau de risque permet de détecter les services qui ne répondent pas aux exigences de sécurité de l'organisation.

Le niveau de risque est une estimation et n'implique aucune déclaration sur la qualité du service cloud ni de son fournisseur. Le niveau de risque est simplement une recommandation des experts de Kaspersky.

Les niveaux de risque des services cloud sont affichés dans la section **Cloud Discovery** de la stratégie dans la liste de tous les services cloud contrôlés.

D'autres modules de Kaspersky Endpoint Security assurent la protection contre les menaces et le suivi des activités suspectes des utilisateurs lors de l'utilisation de services cloud.



Notification de Cloud Discovery

Cloud Discovery ne bloque pas les applications cloud qui ont été lancées avant Kaspersky Endpoint Security.

Comment bloquer l'accès à des services cloud dans Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Communication et protection Internet** → **Cloud Discovery**.

5. Activez le commutateur **Cloud Discovery ACTIVÉ**.

   Une liste de tous les services cloud s'affiche. Les services cloud sont regroupés en catégories, par exemple, *Stockage de fichiers*, *Clients de messagerie* ou *Email*. Les experts de Kaspersky mettent régulièrement à jour les catégories de Cloud Discovery et les services cloud classés dans les catégories. Kaspersky Endpoint Security met à jour l'ensemble des catégories et des services cloud avec les bases de données des applications.

6. Utilisez le commutateur dans la colonne **Accès** pour configurer l'accès aux services cloud.

7. Enregistrez vos modifications.

En conséquence, l'application contrôle l'utilisation des services cloud dans le navigateur ainsi que dans les applications correspondantes.

Exclusions de l'analyse pour l'application

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, en tenant compte des propriétés des objets gérés et des 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.

À partir de Kaspersky Endpoint Security 12.5 for Windows, vous pouvez ajouter la télémétrie EDR à la zone de confiance. Cette option permet d'optimiser les données que l'application envoie au serveur de collecte de données télémétriques pour la solution Kaspersky Anti Targeted Attack Platform (EDR).

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware.

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 un ordinateur et aux données de l'utilisateur. De telles applications n'ont pas nécessairement de finalité malveillante, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que des individus malintentionnés peuvent utiliser pour compromettre l'ordinateur ou les données de l'utilisateur, consultez le site de l'Encyclopédie 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.
- Tâche *Analyse des logiciels malveillants*

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 l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Exclusions de l'analyse et applications de confiance** → **Exclusions de l'analyse**.

   Une fenêtre reprenant la liste des exclusions s'ouvre.
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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des exclusions d'analyse dans l'interface utilisateur de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

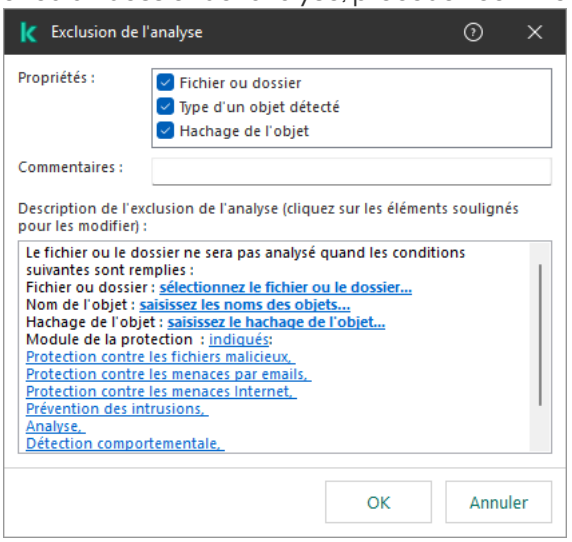
- **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

- **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

- **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

- **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle exclusion d'analyse à une catégorie en particulier, sélectionnez une catégorie.

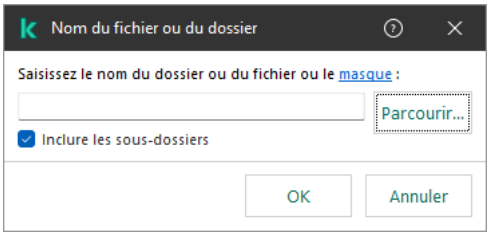
9. Si vous souhaitez exclure un fichier ou un dossier de l'analyse, procédez comme suit :



Paramètres d'exclusion

a. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.

b. Cliquez sur le lien dans le groupe ci-dessous **Nom du fichier ou du dossier** pour ouvrir la fenêtre.



Sélectionnez un fichier ou un dossier

a. 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

Kaspersky Endpoint Security prend en charge les variables d'environnement

Vous pouvez exclure des dossiers réseau. Pour ce faire, saisissez manuellement le chemin d'accès au dossier réseau (par exemple, `\\Network Share\*`).

> Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'exclusions à l'aide de 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.

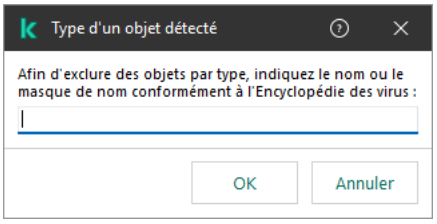
b. Si nécessaire, désactivez la fonctionnalité **Inclure les sous-dossiers**. Si cette fonctionnalité est activée, l'application n'analyse pas les fichiers dans les sous-dossiers. Si cette fonctionnalité est désactivée, l'application exclut uniquement le dossier sélectionné de la zone d'analyse. Cette option est activée par défaut.

c. Enregistrez vos modifications.

10. Si vous voulez exclure de l'analyse des objets portant un nom précis, procédez comme suit :

    a. Dans le groupe **Propriétés**, cochez la case **Type d'un objet détecté**.

    b. Cliquez sur le lien dans le groupe ci-dessous **Type d'un objet détecté** pour ouvrir la fenêtre.



Sélectionnez un objet

    a. Saisissez le nom du type d'objet en fonction de 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.

    b. Enregistrez vos modifications.

11. 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 dans le groupe ci-dessous **Hachage de l'objet** pour ouvrir la fenêtre.

Sélectionnez un fichier

    a. Saisissez le hachage du fichier ou sélectionnez le fichier en cliquant sur le bouton **Parcourir**.

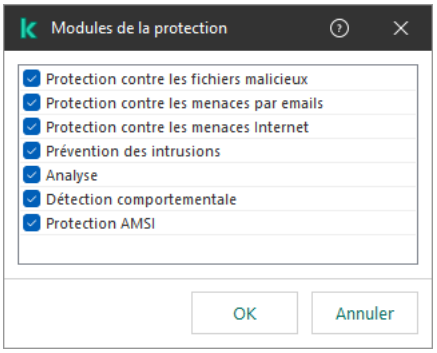
    Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

    b. Enregistrez vos modifications.

12. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

13. Définissez les modules de Kaspersky Endpoint Security qui doivent appliquer l'exclusion de l'analyse :

    a. Cliquez sur le lien dans le groupe ci-dessous **Modules de la protection** pour ouvrir la fenêtre.



Sélectionner les modules de la protection

    a. Cochez les cases en regard modules auxquels s'appliqueront les exclusions de l'analyse.

    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.

14. Cliquez sur **OK**.

    La nouvelle exclusion sera ajoutée à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case à côté de l'objet.

15. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment créer une exclusion d'analyse dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zone de confiance**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Exclusions de l'analyse des logiciels malveillants**.

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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des exclusions d'analyse dans l'interface utilisateur de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

   Pour ajouter une nouvelle exclusion de l'analyse à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

9. Sélectionnez la manière dont vous souhaitez ajouter l'exclusion : **Chemin d'accès au fichier ou au dossier**, **Type d'objet** ou **Hachage de l'objet**.

10. Pour exclure un fichier ou un dossier de l'analyse, entrez 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 :

    - 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

      Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

      Vous pouvez exclure des dossiers réseau. Pour ce faire, saisissez manuellement le chemin d'accès au dossier réseau (par exemple, `\\Network Share\*`).

11. Si vous souhaitez exclure un type particulier d'objet des analyses, saisissez, dans le champ **Type d'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 de l'objet**.

    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 **Appliquer l'exclusion à**, 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. Cliquez sur le bouton **OK**.

    La nouvelle exclusion sera ajoutée à la liste. Vous pouvez utiliser le commutateur pour mettre fin à une exclusion à tout moment.

16. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

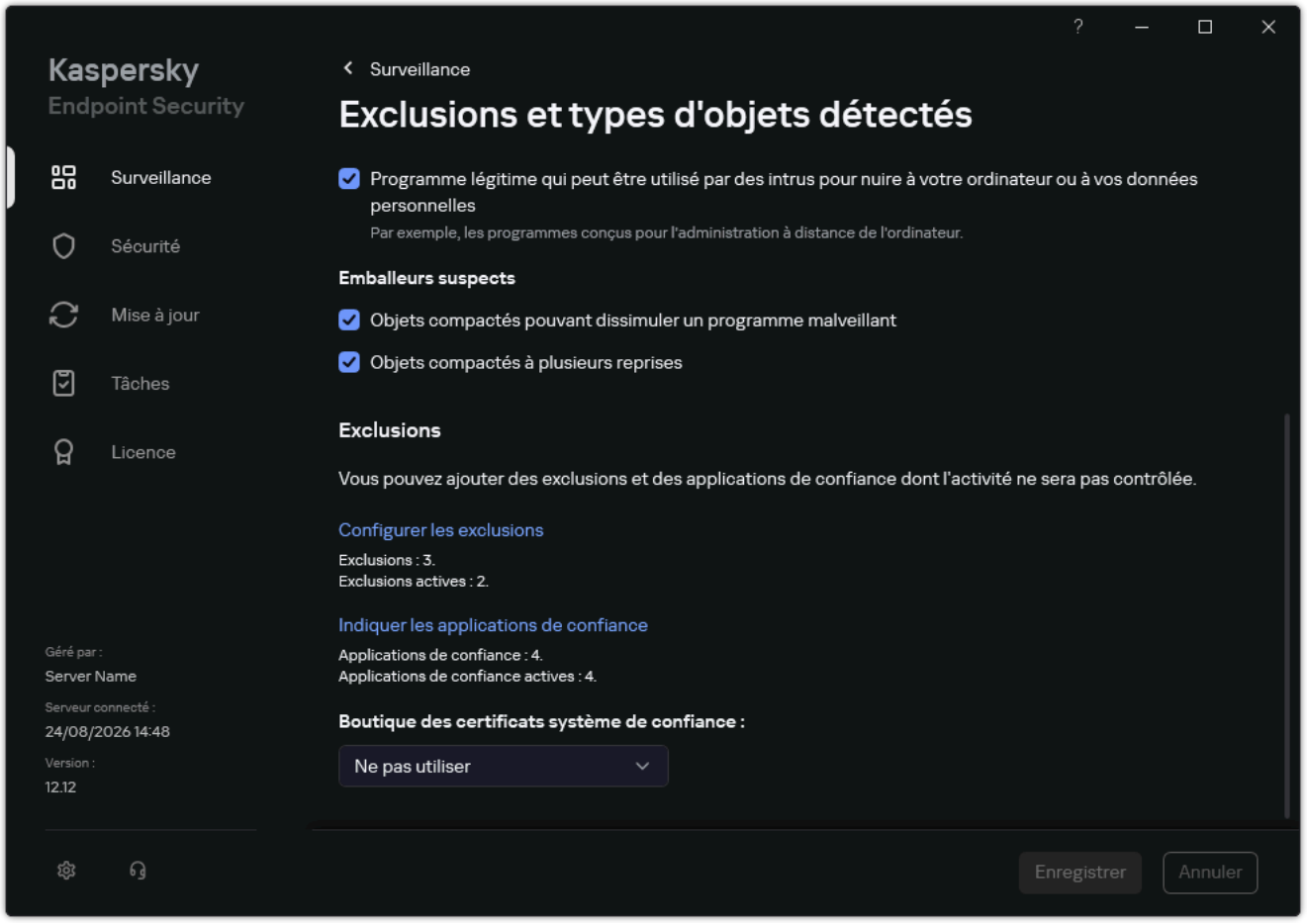
Création d'une exclusion d'analyse dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

Kaspersky Endpoint Security masque la liste des exclusions d'analyse dans l'interface utilisateur de l'application si la configuration des exclusions d'analyse est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les exclusions d'analyse locales sont interdites (la case **Autoriser l'utilisation des exclusions locales** est décochée).



Paramètres des exclusions

4. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner l'exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

   Pour ajouter une nouvelle exclusion de l'analyse à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

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 variables d'environnement ainsi que 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

  Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

  Vous pouvez exclure des dossiers réseau. Pour ce faire, saisissez manuellement le chemin d'accès au dossier réseau (par exemple, `\\Network Share\*`).

6. Si vous souhaitez exclure un type particulier d'objet des analyses, saisissez, dans le champ **Type d'un objet détecté**, 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 de l'objet**.

   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.

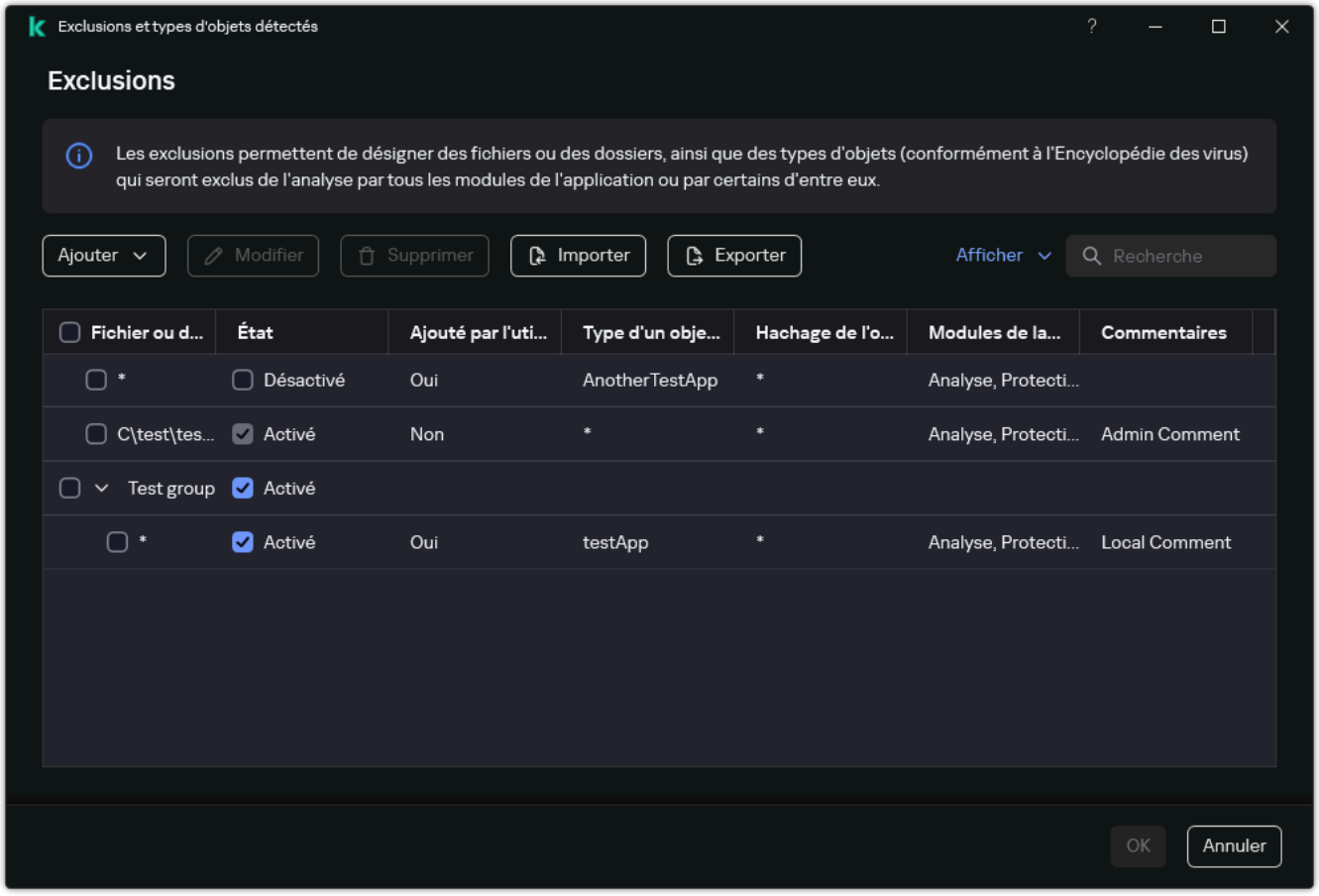
9. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaire**.

10. Sélectionnez l'état **Actif** pour l'exclusion.

11. Cliquez sur **Ajouter**.

    La nouvelle exclusion sera ajoutée à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case dans la colonne **État**.

12. Enregistrez vos modifications.



Liste des exclusions

Exemples de masque de chemin d'accès :

Nous recommandons d'utiliser des chemins relatifs plutôt que des chemins absolus. Cela permet d'exclure non seulement les objets du système de fichiers, mais aussi les objets sans fichier. Par exemple, `*\Program Files (x86)\Folder\Subfolder`.

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 `example*` 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 dans le 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\`, y compris les sous-dossiers.
- Le masque `C:\dir\` reprend tous les chemins d'accès aux fichiers du dossier `C:\dir\`, y compris les sous-dossiers.
- 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\`.
- Le masque `C:\dir1\*\dir3\` inclura tous les chemins d'accès aux fichiers des sous-dossiers dir3 d'un niveau dans le dossier `C:\dir1\`.
- Le masque `C:\dir1\**\dirN\` inclura tous les chemins d'accès aux fichiers dans les sous-dossiers dirN du dossier `C:\dir1\` à n'importe quel niveau.

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.

Création d'une exclusion par type d'objets détectés

Kaspersky Endpoint Security classe les objets détectés comme suit :

- **Virus et vers**

  Sous-catégorie : virus et vers (Viruses_and_Worms)

  Niveau de danger : 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 *Overwriting* remplacent le code du fichier infecté par leur propre code, effaçant ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *Parasitic* modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les virus *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-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	Name	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.
IM-Worm	Vers de client 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-Worm	Vers de chats	Ils se diffusent via les canaux Internet Relay Chats, des systèmes qui permettent de discuter en temps réel avec d'autres personnes. 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.
Net-Worm	Vers de réseau (vers de réseaux informatiques)	Ils se diffusent via les réseaux informatiques. 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.
P2P-Worm	Vers de réseau d'échange de fichiers	Ils se propagent via les réseaux d'échange de fichiers pair à pair. 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. 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.

Type	Name	Description
Ver	Autres vers	Parmi ces autres vers, citons : • 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 (y compris les ransomwares)**

  Sous-catégories : chevaux de Troie (Trojan_programs)

  Niveau de danger : 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	Name	Description
Trojan-ArcBomb	Chevaux de Troie (bombes dans les archives)	Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur. 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.
Backdoor	Chevaux de Troie pour l'administration à distance	Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs. 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.
Trojan	Chevaux de Troie	Cette catégorie reprend les programmes malveillants suivants : • **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	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.

Type	Name	Description
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 : • 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-PSW	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 « attaquant » 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	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	Name	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". 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. Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploites de type Nuker sont des paquets réseau qui mettent l'ordinateur hors service.
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.
Spoofer	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.

Type	Name	Description
IM-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.

- **Logiciel publicitaire**

  Sous-catégorie : Logiciels publicitaires (Adware)

  Niveau de danger : Moyen

  Les logiciels 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 : numéroteurs automatiques.

  Niveau de danger : Moyen

  Les numéroteurs automatiques peuvent établir subrepticement des connexions téléphoniques à l'aide d'un modem.

- **Programme légitime qui peut être utilisé par des intrus 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	Name	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.
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).

Type	Name	Description
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.

- **Objets compactés pouvant dissimuler un programme malveillant**

  Sous-catégorie : fichiers compressés susceptibles de causer des dommages.

  Niveau de danger : Moyen.

  Le fichier est compressé à l'aide d'un outil de compression spécial utilisé pour contenir des programmes malveillants : virus, vers, chevaux de Troie. Kaspersky Endpoint Security analyse le module de décompression dans les archives autoextractibles SFX.

  Pour dissimuler les programmes malveillants afin qu'ils ne soient pas détectés par un antivirus, les pirates informatiques les compressent à l'aide d'empaqueteurs spéciaux. Les experts de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

- **Objets compactés à plusieurs reprises**

  Sous-catégorie : fichiers compressés à plusieurs reprises.

  Niveau de danger : Moyen.

  Le fichier est emballé par un ou plusieurs empaqueteurs trois fois ou plus.

  Pour dissimuler un programme malveillant afin qu'il ne soit pas détecté par un antivirus, les pirates informatiques peuvent compresser un fichier plusieurs fois. Kaspersky Endpoint Security analyse les fichiers compressés.

Par défaut, Kaspersky Endpoint Security détecte tous les types d'objets. Nous vous recommandons de laisser la détection de tous les types d'objets activée afin d'améliorer la sécurité de l'ordinateur. Si vous utilisez des utilitaires en interne que l'application détecte comme malveillants, ajoutez ces utilitaires à une liste d'exclusion, mais ne désactivez pas la détection de l'ensemble du type d'objets.

Comment sélectionner les types d'objets détectés dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Types d'objets détectés**.
6. Dans la fenêtre qui s'ouvre, cochez les cases pour les types d'objets que Kaspersky Endpoint Security doit détecter.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner les types d'objets détectables dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

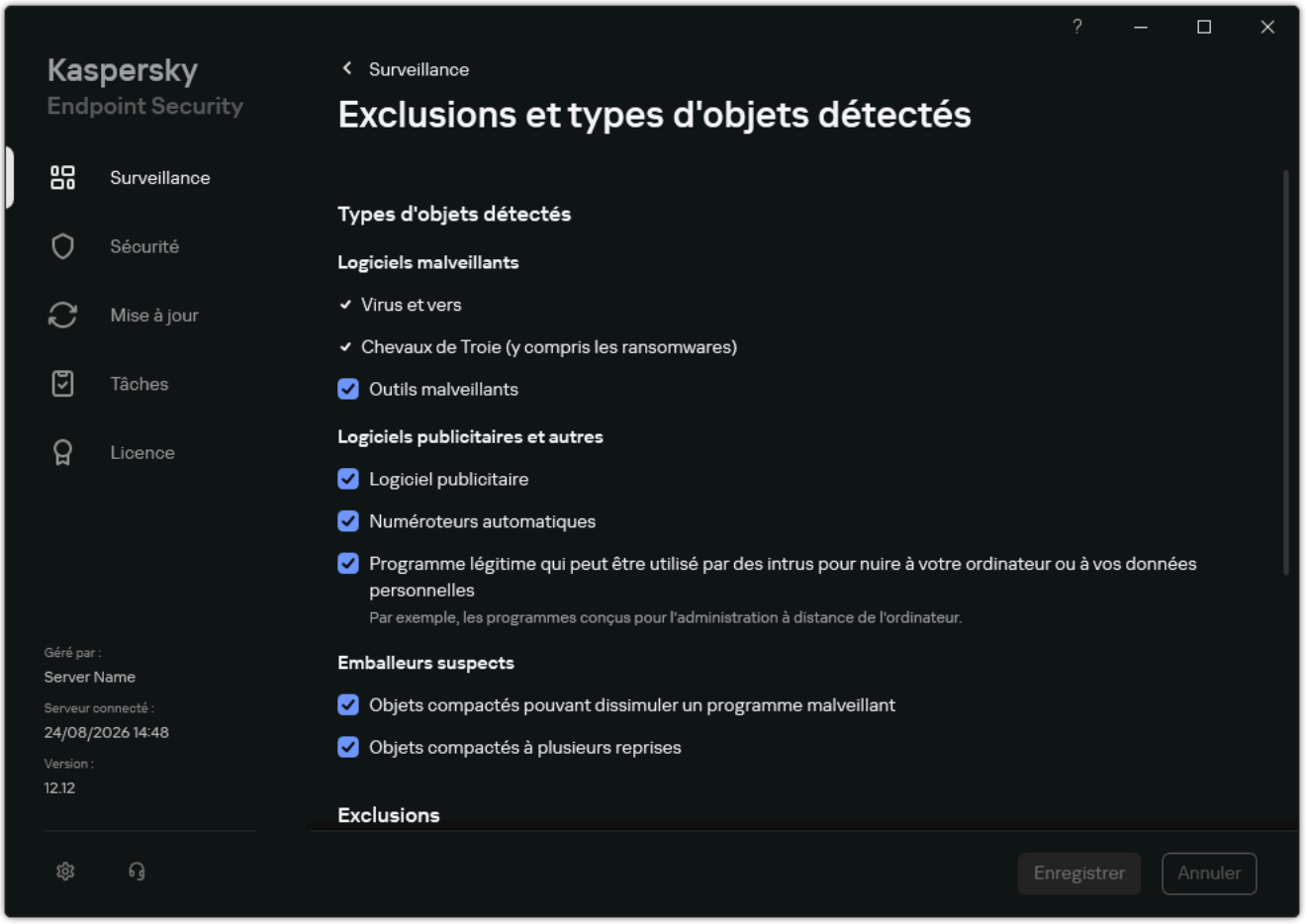
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de détection**.
5. Dans le groupe **Détection d'autres types d'objets**, cochez les cases pour les types d'objets que Kaspersky Endpoint Security doit détecter.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment sélectionner les types d'objets détectables dans la Console d'administration (MMC)

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.

3. Dans le groupe **Types d'objets détectés**, cochez les cases pour les types d'objets que Kaspersky Endpoint Security doit détecter.

4. Enregistrez vos modifications.



Types d'objets à détecter

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 surveille 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. Après l'ajout d'une application à la liste des applications de confiance, Kaspersky Endpoint Security cesse de surveiller l'activité de l'application.

La différence entre les exclusions d'analyse et les applications de confiance est que pour les exclusions, Kaspersky Endpoint Security n'analyse pas les fichiers, tandis que pour les applications de confiance, il ne contrôle pas les processus lancés. Si une application de confiance crée un fichier malveillant dans un dossier qui n'est pas inclus dans les exclusions d'analyse, Kaspersky Endpoint Security détectera le fichier et éliminera la menace. Si le dossier est ajouté aux exclusions, Kaspersky Endpoint Security ignorera ce fichier.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance afin que les objets utilisés par cette application ne soient pas surveillés. Cela augmentera les performances de l'ordinateur, ce qui est particulièrement important lors de l'utilisation d'applications serveur.

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.

Les applications de confiance permettent d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, le problème de la double analyse du trafic réseau d'un ordinateur tiers par Kaspersky Endpoint Security et par une autre application antivirus).

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre 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 l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Exclusions de l'analyse et applications de confiance** → **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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des applications de confiance dans l'interface utilisateur de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle application de confiance à la racine de la liste.

- **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *applications de confiance prédéfinies*. Des applications de confiance prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des applications de confiance prédéfinies conformément à la fonction du serveur protégé.

- **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle application de confiance à une catégorie en particulier, sélectionnez une catégorie.

9. Sélectionnez les critères de confiance :

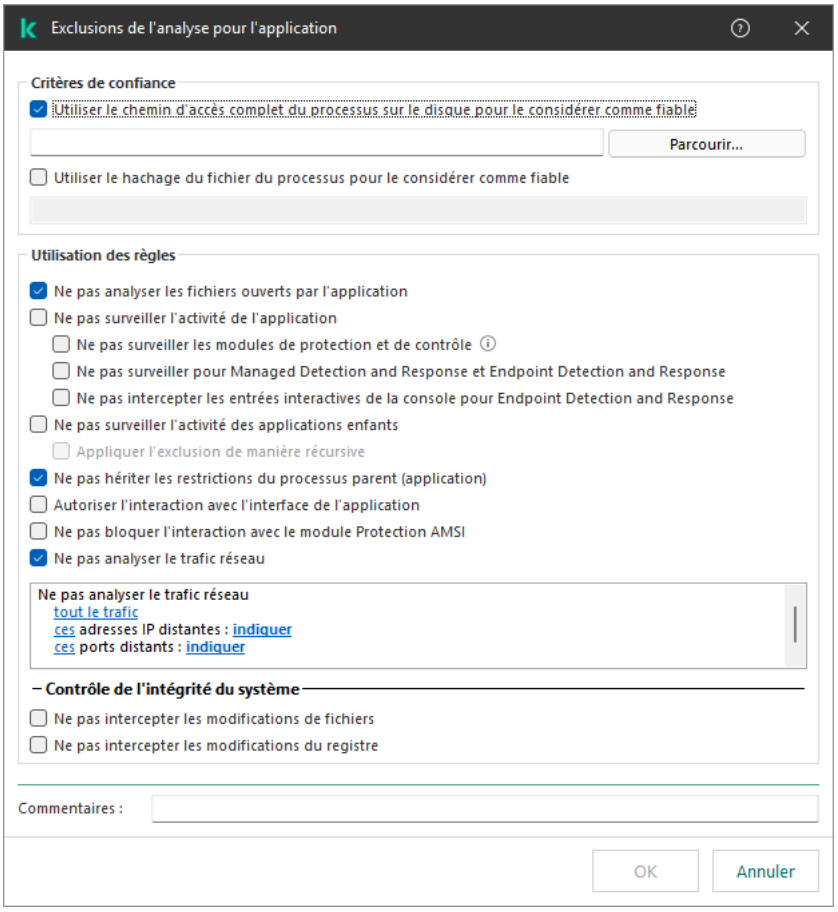
- **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**. Indiquez le chemin d'accès au fichier exécutable de l'application de confiance.

  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 considère le nom de fichier d'une application de confiance comme étant sensible à la casse. Si le nom de fichier saisi ne respecte pas la casse, Kaspersky Endpoint Security ne reconnaîtra pas l'application de confiance.

- **Utiliser le hachage du fichier du processus pour le considérer comme fiable**.

> Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'applications de confiance dans 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.



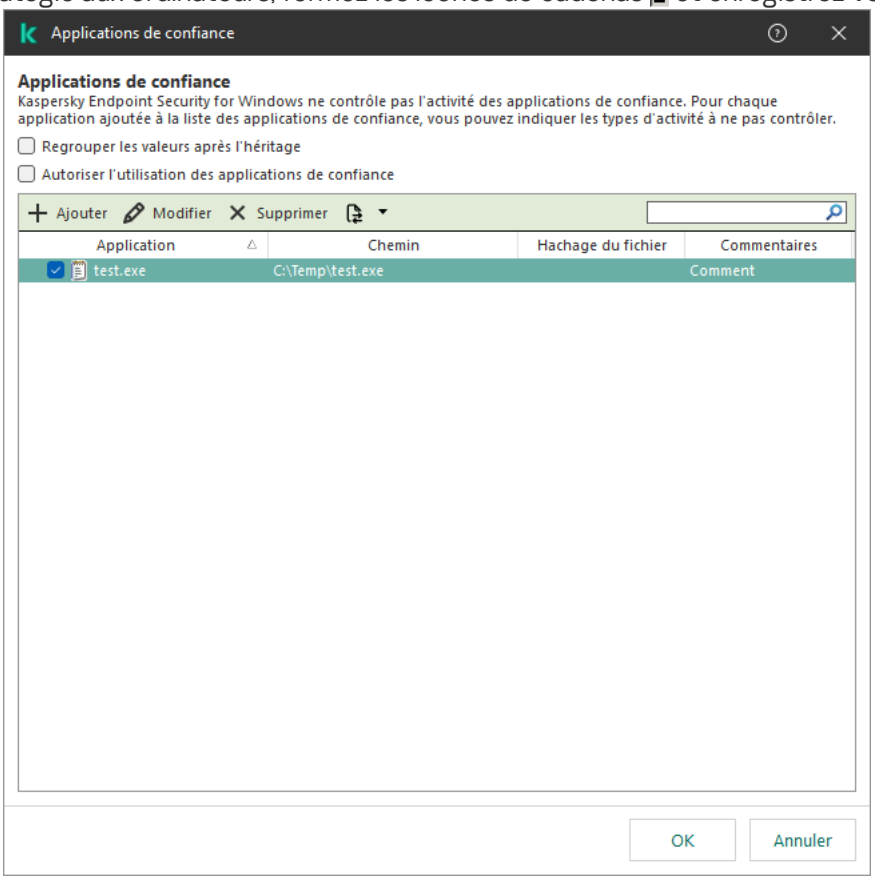
Paramètres des applications de confiance

10. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).

11. Cliquez sur **OK**.

    La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case à côté de l'objet.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Liste des applications de confiance

Comment ajouter une application à la liste de confiance dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zone de confiance**.

5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Applications**.

   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 exclusions locales** 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. De plus, si la case est décochée, Kaspersky Endpoint Security masque la liste consolidée des applications de confiance dans l'interface utilisateur de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle application de confiance à la racine de la liste.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *applications de confiance prédéfinies*. Des applications de confiance prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des applications de confiance prédéfinies conformément à la fonction du serveur protégé.

   Pour ajouter une nouvelle application de confiance à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

9. Sélectionnez les critères de confiance :

   - **Chemin d'accès au fichier ou au dossier**. 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 considère le nom de fichier d'une application de confiance comme étant sensible à la casse. Si le nom de fichier saisi ne respecte pas la casse, Kaspersky Endpoint Security ne reconnaîtra pas l'application de confiance.

   - **Hachage de l'application**.

   > Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement %userprofile% lors de la génération d'une liste d'applications de confiance dans la console de 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. Cliquez sur **OK**.

    La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case dans la colonne **État**.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

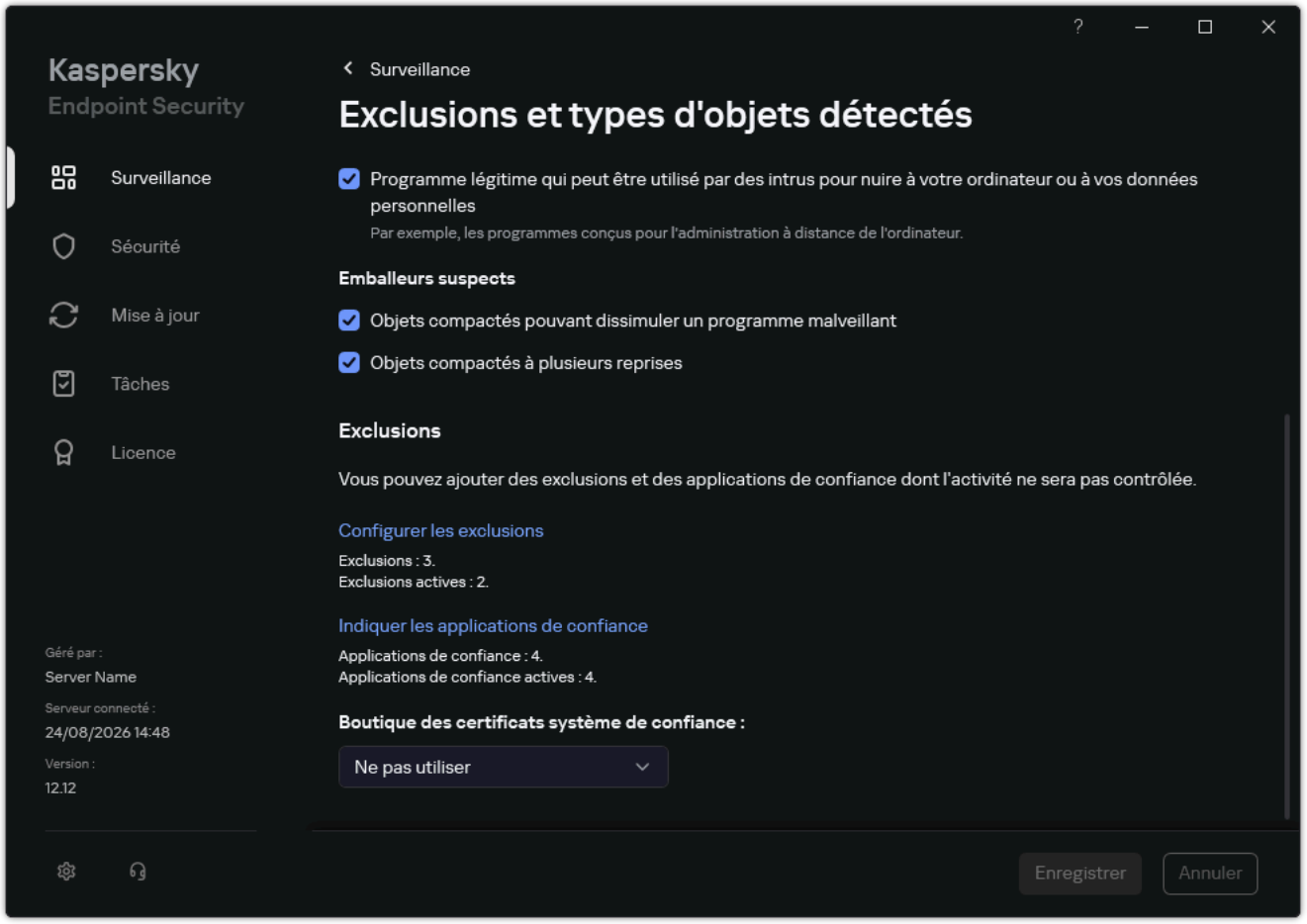
Comment ajouter une application à la liste des applications de confiance dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.

Kaspersky Endpoint Security masque la liste consolidée des applications de confiance dans l'interface utilisateur de l'application si la configuration des applications de confiance est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les applications de confiance locales sont interdites (la case **Autoriser l'utilisation des applications de confiance** est décochée).



Paramètres des exclusions

4. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle application de confiance à la racine de la liste.

   - **Sélectionner l'exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *applications de confiance prédéfinies*. Des applications de confiance prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des applications de confiance prédéfinies conformément à la fonction du serveur protégé.

   Pour ajouter une nouvelle application de confiance à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

5. Sélectionnez les critères de confiance :

   - **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme fiable**. 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 considère le nom de fichier d'une application de confiance comme étant sensible à la casse. Si le nom de fichier saisi ne respecte pas la casse, Kaspersky Endpoint Security ne reconnaîtra pas l'application de confiance.

   - **Utiliser le hachage du fichier du processus pour le considérer comme fiable**.

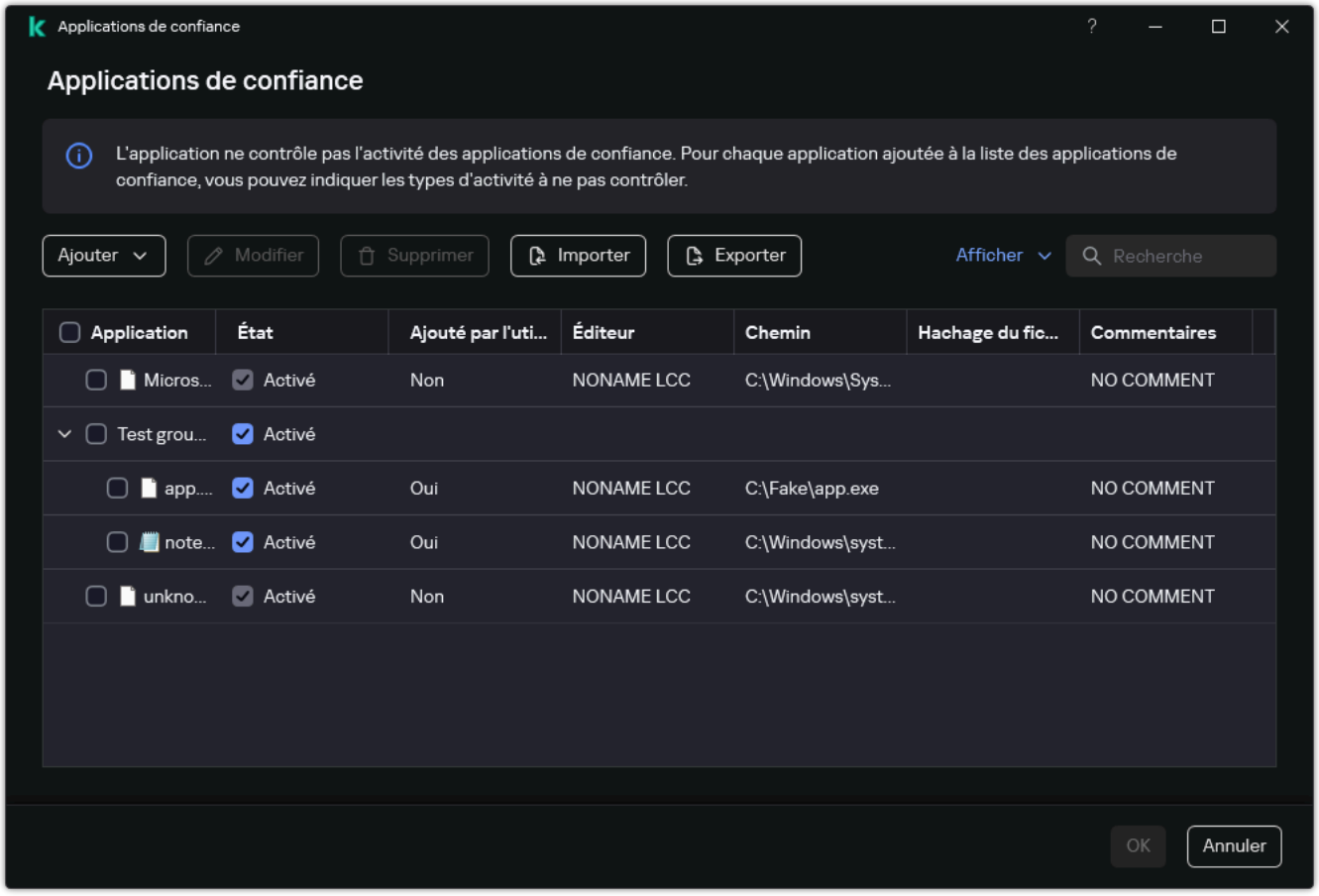
   > Kaspersky Endpoint Security prend en charge les variables d'environnement et convertit le chemin dans l'interface locale de l'application. Autrement dit, si vous saisissez le chemin d'accès au fichier `%userprofile%\Documents\File.exe`, une entrée `C:\Users\Fred123\Documents\File.exe` est ajoutéedans 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.

7. Cliquez sur **OK**.

   La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case dans la colonne **État**.

8. Enregistrez vos modifications.



Liste des applications de confiance

Paramètres des applications de confiance

Paramètre	Description
Ne pas analyser les fichiers ouverts par l'application	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. Vous pouvez configurer le contrôle de l'activité des applications pour différents modules de Kaspersky Endpoint Security : • **Ne pas surveiller les modules de protection et de contrôle**. 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 surveiller pour Managed Detection and Response et Endpoint Detection and Response**. L'activité de l'application est surveillée par l'agent MDR intégré et l'agent EDR (KATA) intégré. • **Ne pas intercepter les entrées interactives de la console pour Endpoint Detection and Response**. Kaspersky Endpoint Security n'envoie pas de données télémétriques sur la gestion de l'application dans la console. Les données de télémétrie sont utilisées par Kaspersky Anti Targeted Attack Platform (EDR).
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. Vous pouvez appliquer l'exclusion de manière récursive. Ainsi, l'application ne surveille pas l'activité de toute la chaîne d'applications enfants.
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 applications enfants	Kaspersky Endpoint Security ne surveille pas l'activité des fichiers ni du réseau des applications qui sont lancées par cette application. Vous pouvez appliquer l'exclusion de manière récursive. Ainsi, l'application ne surveille pas l'activité de toute la chaîne d'applications enfants.
Autoriser l'interaction avec l'interface de l'application	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	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.

Paramètre	Description
Ne pas analyser le trafic réseau	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. Kaspersky Endpoint Security version 14.0 ou antérieure ne permet pas d'exclure le trafic réseau si un hachage est spécifié pour une application de confiance à la place d'un chemin d'accès.
Ne pas intercepter les modifications de fichiers *(disponible uniquement dans Kaspersky Security Center Console)*	Kaspersky Endpoint Security ne surveille pas les modifications apportées aux fichiers dans la zone de surveillance du Contrôle de l'intégrité du système. L'application applique l'exclusion à tous les modes de Contrôle de l'intégrité du système : Contrôle de l'intégrité du système en temps réel et Vérification de l'intégrité du système sur demande.
Ne pas intercepter les modifications du registre *(disponible uniquement dans Kaspersky Security Center Console)*	Kaspersky Endpoint Security ne surveille pas les modifications apportées aux clés de registre dans la zone de surveillance du Contrôle de l'intégrité du système. L'application applique l'exclusion à tous les modes de Contrôle de l'intégrité du système : Contrôle de l'intégrité du système en temps réel et Vérification de l'intégrité du système sur demande.
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 : • 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.

Création d'une zone de confiance locale

L'utilisateur peut désormais créer sa propre zone de confiance locale pour un ordinateur spécifique. De cette façon, l'utilisateur peut créer ses propres listes locales d'exclusions d'analyse 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 dans les paramètres de stratégie. Pour ce faire, utilisez les cases **Autoriser l'utilisation des exclusions locales** et **Autoriser l'utilisation des applications de confiance** dans la section **Exclusions** de la stratégie.

Si la création d'une zone de confiance locale est autorisée par un administrateur, l'utilisateur peut ajouter ses propres exclusions d'analyse et applications de confiance dans l'interface utilisateur de l'application. Dans le même temps, l'utilisateur ne dispose pas des autorisations nécessaires pour modifier ou supprimer des objets de la zone de confiance configurée dans la stratégie. L'administrateur peut également afficher, ajouter, modifier ou supprimer des éléments de liste dans la console Kaspersky Security Center si des exclusions doivent être ajoutées pour un ordinateur individuel.

Kaspersky Endpoint Security masque les listes des exclusions d'analyse et des applications de confiance dans l'interface utilisateur de l'application si la configuration de la zone de confiance est bloquée par l'administrateur dans la console (symbole « cadenas fermé »), et si les exclusions d'analyse et les applications de confiance locales sont interdites.

Comment ajouter un objet à la zone de confiance locale 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. Ouvrez les propriétés de l'ordinateur d'un double clic.

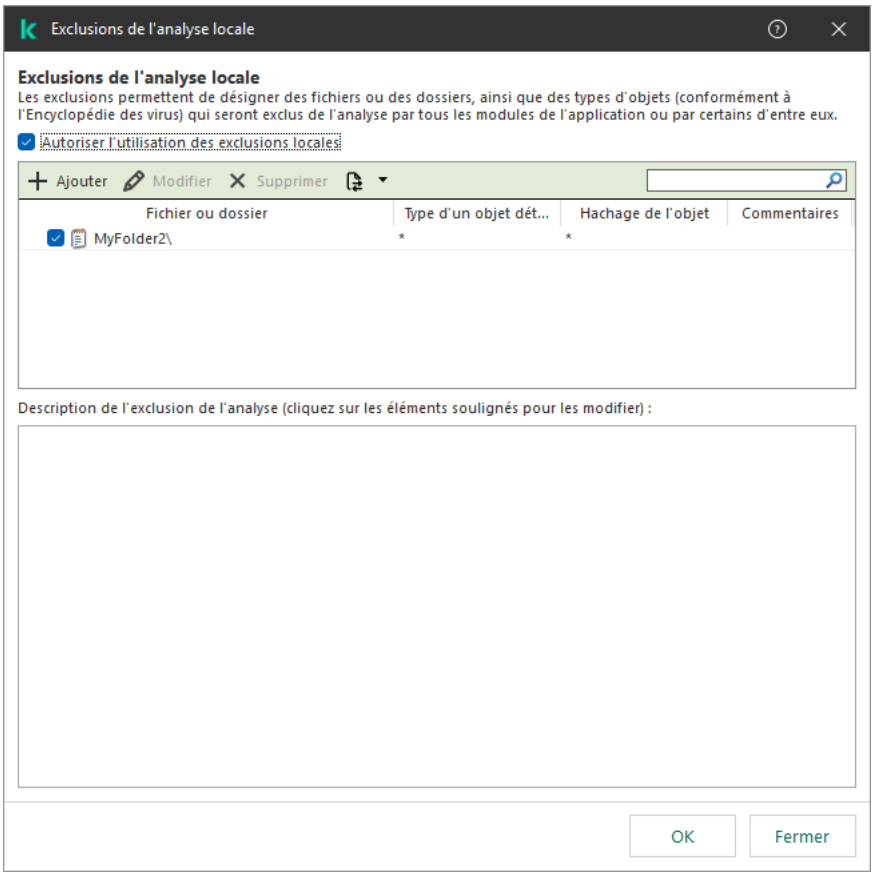
5. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.

6. Dans la liste des applications de Kaspersky installées sur l'ordinateur, choisissez **Kaspersky Endpoint Security for Windows (14.2)**, puis ouvrez les propriétés de l'application d'un double-clic.

7. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

8. Cliquez sur le bouton **Paramètres** dans le groupe **Exclusions de l'analyse et applications de confiance** → **Exclusions de l'analyse locale**.

   Une fenêtre reprenant la liste des exclusions locales s'ouvre.



Paramètres des zones de confiance

9. Dressez une liste des exclusions de l'analyse locale.

   Les règles de création d'exclusions d'analyse locale sont les mêmes que pour les exclusions générales. 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 **Paramètres** dans le groupe **Exclusions de l'analyse et applications de confiance** → **Applications de confiance locales**.

    Une fenêtre reprenant la liste des applications locales de confiance s'ouvre.

11. Dressez une liste des applications locales de confiance.

    Les règles d'ajout d'applications à la liste des applications locales de confiance sont les mêmes que les règles d'ajout à la liste générale. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.

12. Enregistrez vos modifications.

Comment ajouter un objet à la zone de confiance locale dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez permettre à un utilisateur d'effectuer une action bloquée.
3. Sélectionnez l'onglet **Applications**.
4. Cliquez sur **Kaspersky Endpoint Security for Windows**.

   La fenêtre des paramètres locaux de l'application s'ouvre.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.
7. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le lien **Exclusions de l'analyse locale**.
8. Dressez une liste des exclusions de l'analyse locale.

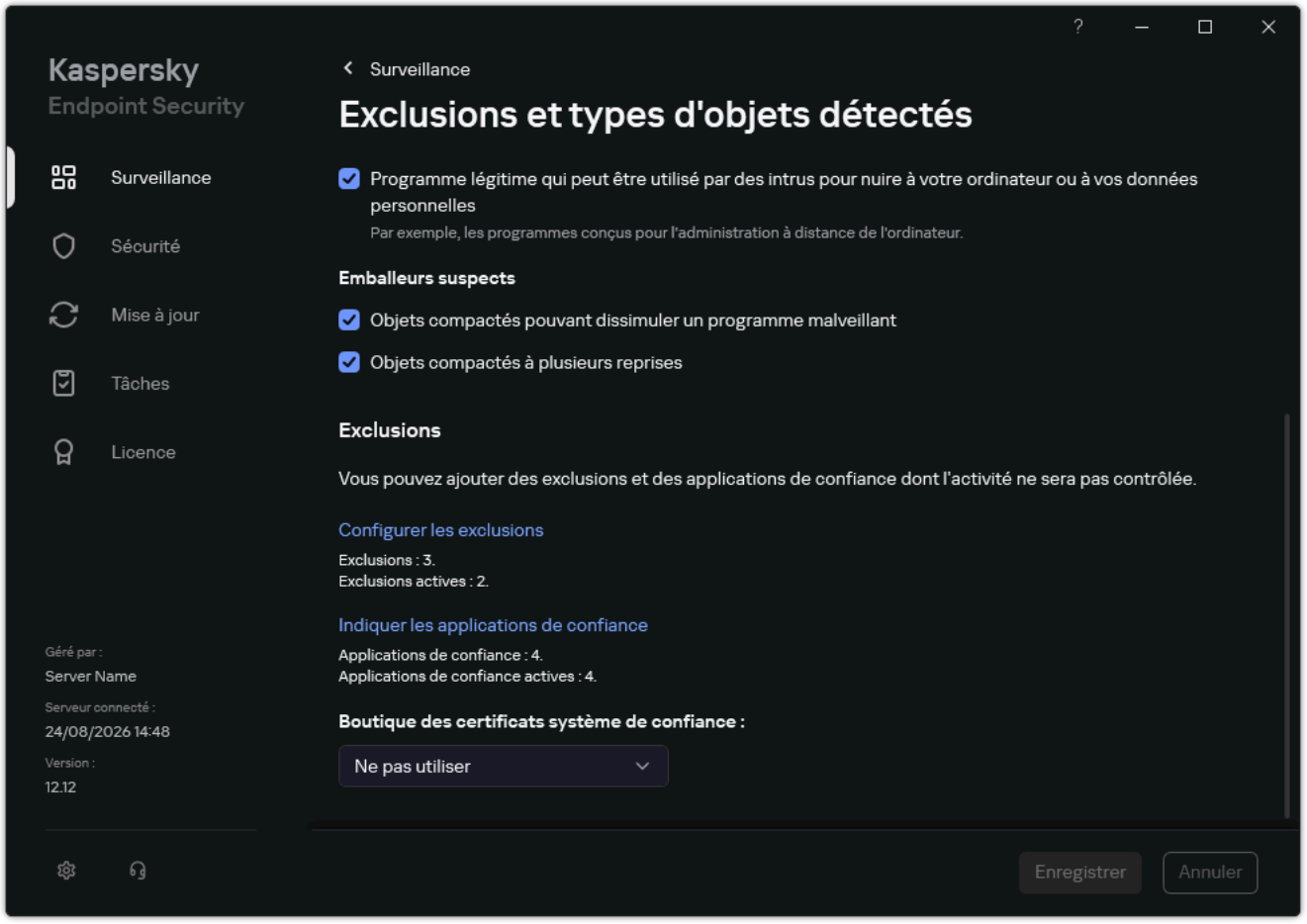
   Les règles de création d'exclusions locales sont les mêmes que les règles de création d'exclusions générales. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
9. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le lien **Applications de confiance locales**.
10. Dressez une liste des applications locales de confiance.

    Les règles d'ajout d'applications à la liste des applications locales de confiance sont les mêmes que les règles d'ajout à la liste générale. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
11. Enregistrez vos modifications.

Comment créer une exclusion d'analyse locale 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** → **Exclusions et types d'objets détectés**.
3. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

Kaspersky Endpoint Security masque la liste des exclusions d'analyse dans l'interface utilisateur de l'application si la configuration des exclusions d'analyse est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les exclusions d'analyse locales sont interdites (la case **Autoriser l'utilisation des exclusions locales** est décochée).



Paramètres des exclusions

4. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner l'exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *exclusions d'analyse prédéfinies*. Des exclusions d'analyse prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des exclusions de l'analyse prédéfinies conformément à la fonction du serveur protégé.

   Pour ajouter une nouvelle exclusion de l'analyse à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

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 variables d'environnement ainsi que 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

  Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

  Vous pouvez exclure des dossiers réseau. Pour ce faire, saisissez manuellement le chemin d'accès au dossier réseau (par exemple, `\\Network Share\*`).

6. Si vous souhaitez exclure un type particulier d'objet des analyses, saisissez, dans le champ **Type d'un objet détecté**, 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 de l'objet**.

   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.

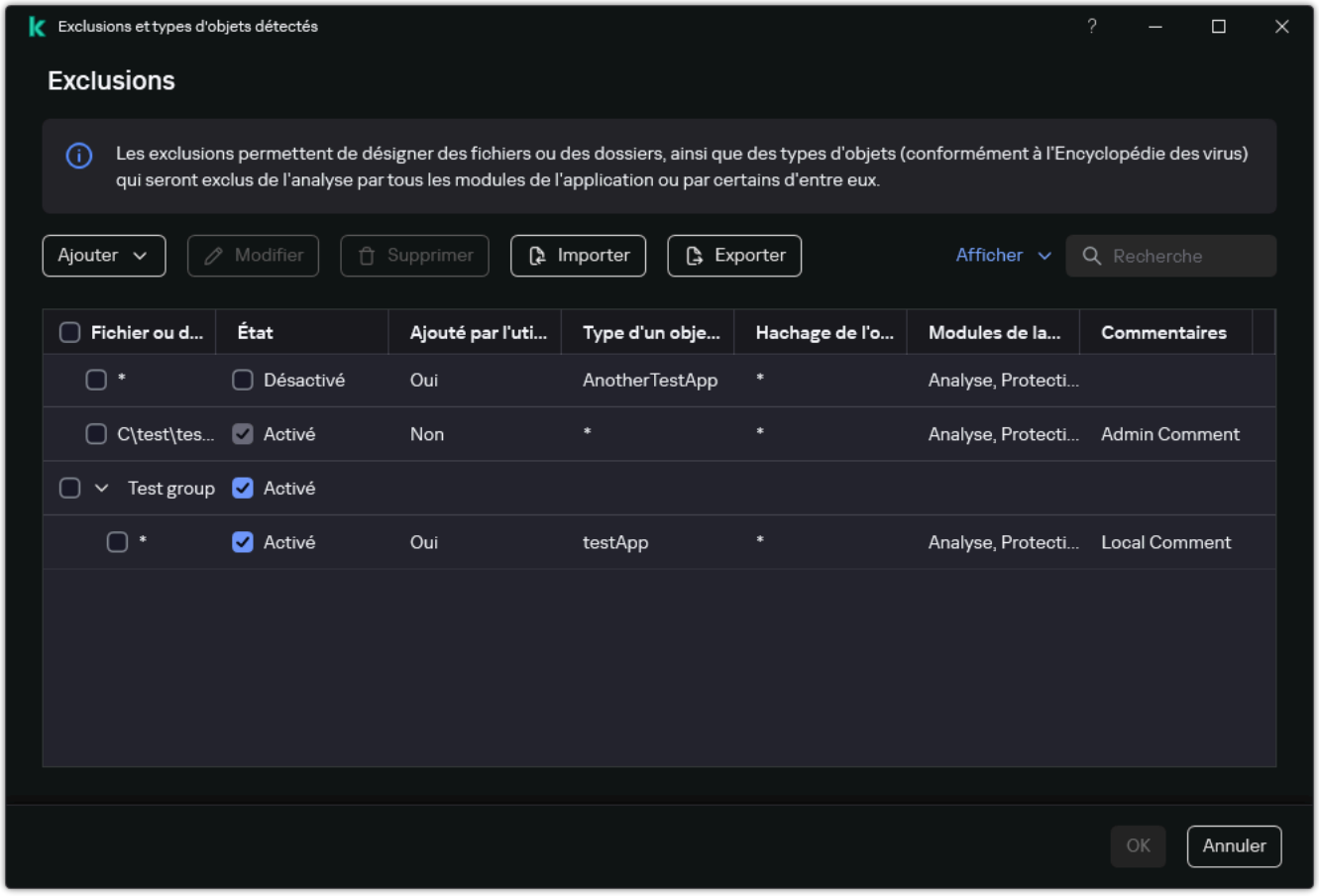
9. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaire**.

10. Sélectionnez l'état **Actif** pour l'exclusion.

11. Cliquez sur **Ajouter**.

    La nouvelle exclusion sera ajoutée à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case dans la colonne **État**.

12. Enregistrez vos modifications.



Liste des exclusions

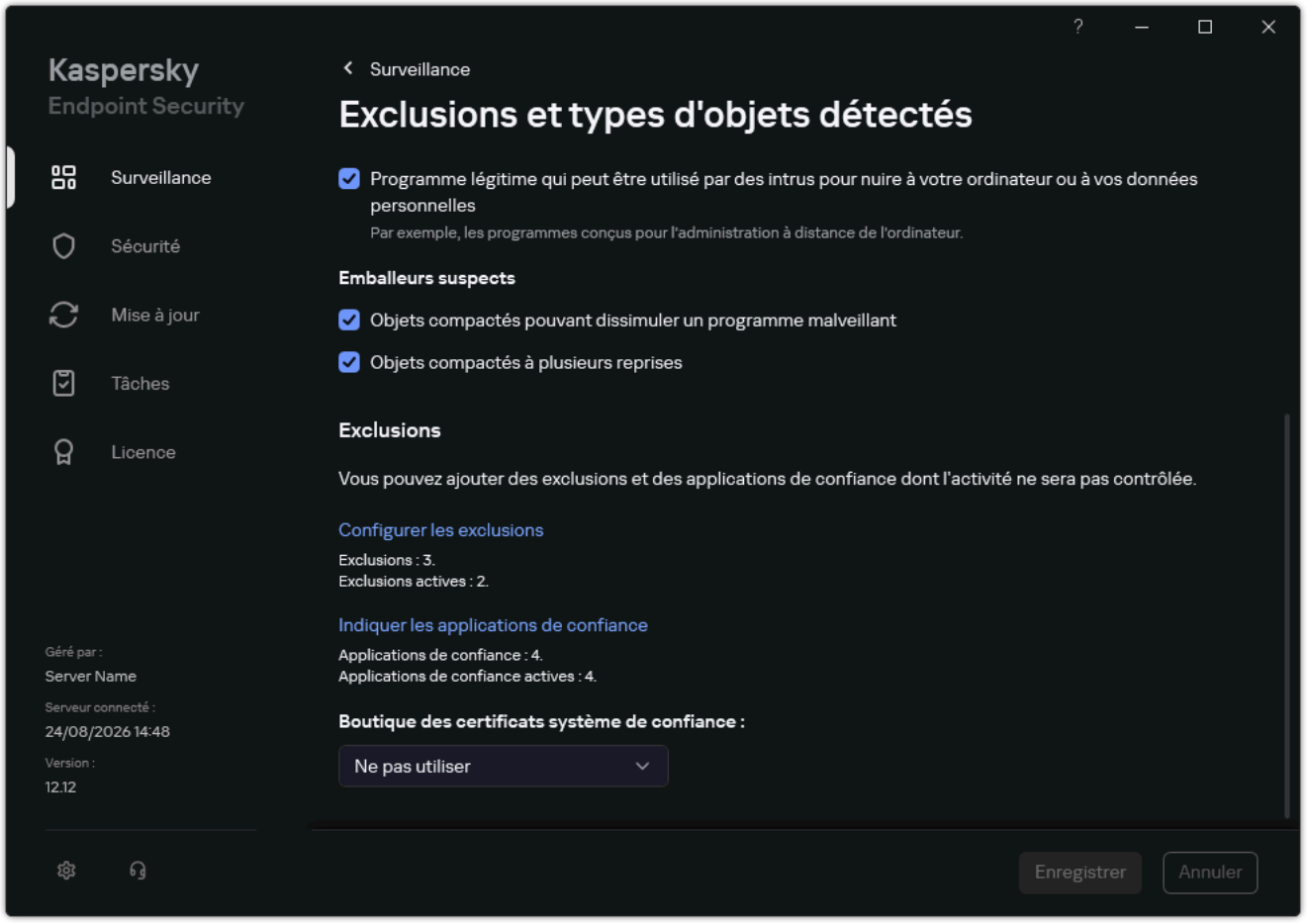
Comment ajouter une application à la liste des applications locales de confiance dans l'interface de l'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.

3. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.

Kaspersky Endpoint Security masque la liste consolidée des applications de confiance dans l'interface utilisateur de l'application si la configuration des applications de confiance est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les applications de confiance locales sont interdites (la case **Autoriser l'utilisation des applications de confiance** est décochée).



Paramètres des exclusions

4. Cliquez sur **Ajouter** et sélectionnez une action :

- **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.

- **Nouvelle exclusion**. Kaspersky Endpoint Security ajoute une nouvelle application de confiance à la racine de la liste.

- **Sélectionner l'exclusion dans la liste**. Pour configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager, l'application comprend des *applications de confiance prédéfinies*. Des applications de confiance prédéfinies ont également été ajoutées pour prendre en charge la configuration de l'application dans les environnements virtuels Citrix et VMware. Vous devez sélectionner des applications de confiance prédéfinies conformément à la fonction du serveur protégé.

Pour ajouter une nouvelle application de confiance à une catégorie en particulier, cochez la case en regard de cette catégorie et sélectionnez l'option **Nouvelle exclusion**.

5. Sélectionnez les critères de confiance :

- **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme fiable**. 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 considère le nom de fichier d'une application de confiance comme étant sensible à la casse. Si le nom de fichier saisi ne respecte pas la casse, Kaspersky Endpoint Security ne reconnaîtra pas l'application de confiance.

- **Utiliser le hachage du fichier du processus pour le considérer comme fiable**.

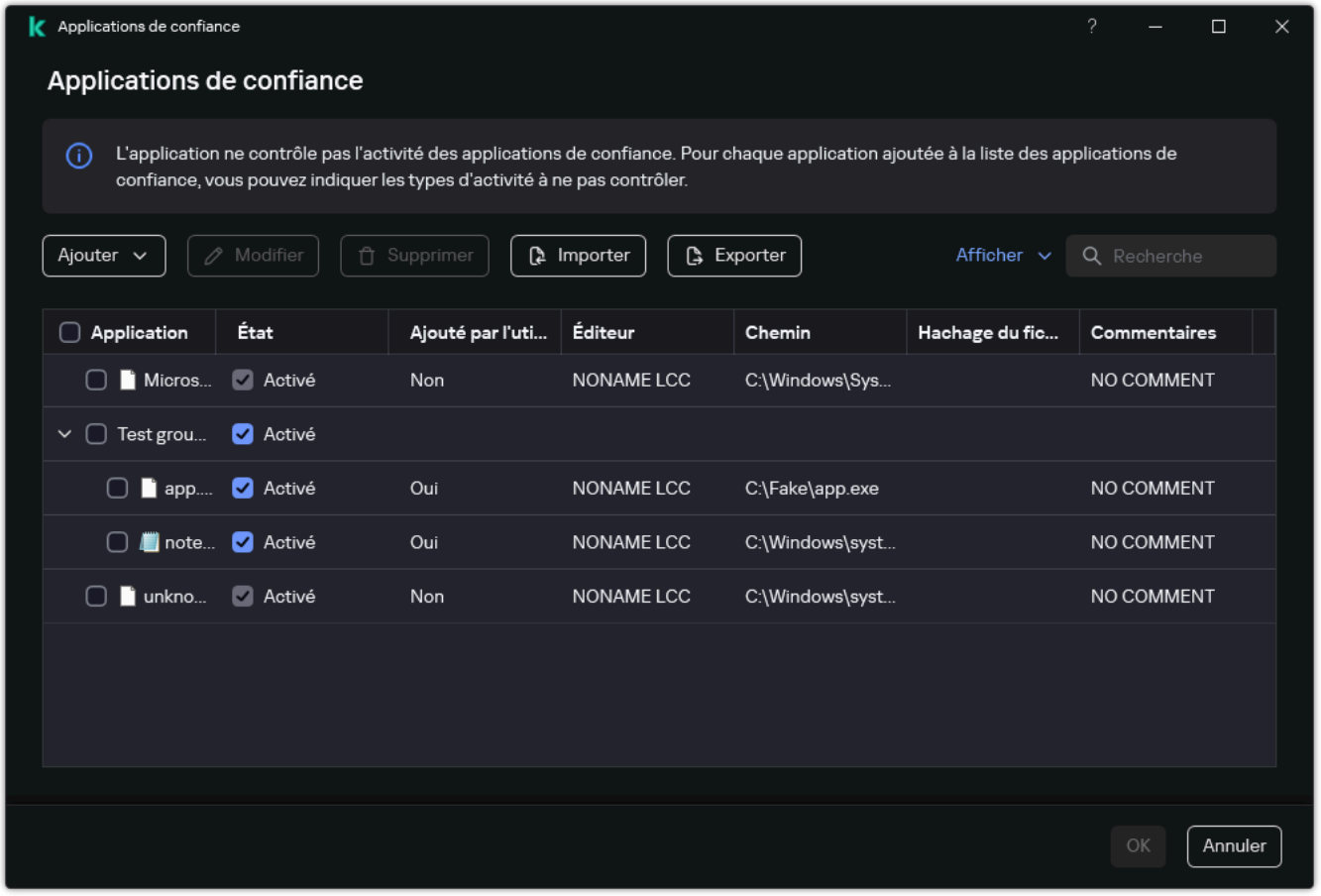
> Kaspersky Endpoint Security prend en charge les variables d'environnement et convertit le chemin dans l'interface locale de l'application. Autrement dit, si vous saisissez le chemin d'accès au fichier `%userprofile%\Documents\File.exe`, une entrée `C:\Users\Fred123\Documents\File.exe` est ajoutéedans 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.

7. Cliquez sur **OK**.

   La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case dans la colonne **État**.

8. Enregistrez vos modifications.



Liste des applications de confiance

Exportation et importation de la 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. La zone de confiance est constituée des listes suivantes : *exclusions d'analyse* et *applications de confiance*. Vous pouvez exporter ces listes vers des fichiers XML et d'autres formats. 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 et la liste des applications de confiance ou pour procéder à la migration de la liste vers un autre serveur.

L'application utilise les formats suivants pour exporter et importer la *liste des exclusions* :

- XML est disponible dans la Console d'administration (MMC), Web Console et Console Cloud.
- DAT est disponible uniquement pour l'importation dans la Console d'administration (MMC). L'objectif de ce format est de maintenir la compatibilité avec les anciennes versions de l'application. Vous pouvez convertir un fichier DAT en XML dans la Console d'administration (MMC) pour migrer les listes d'exclusion vers Web Console.
- Le format CSV n'est disponible que dans l'interface locale de l'application.

Kaspersky Endpoint Security utilise le format XML pour exporter et importer la *liste des applications de confiance*.

Comment exporter et importer la zone de confiance dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.
4. Sous **Exclusions de l'analyse et applications de confiance**, sélectionnez le module de la zone de confiance que vous souhaitez exporter ou importer : **Exclusions de l'analyse** ou **Applications de confiance**.
5. Cliquez sur **Paramètres**.
6. 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**.

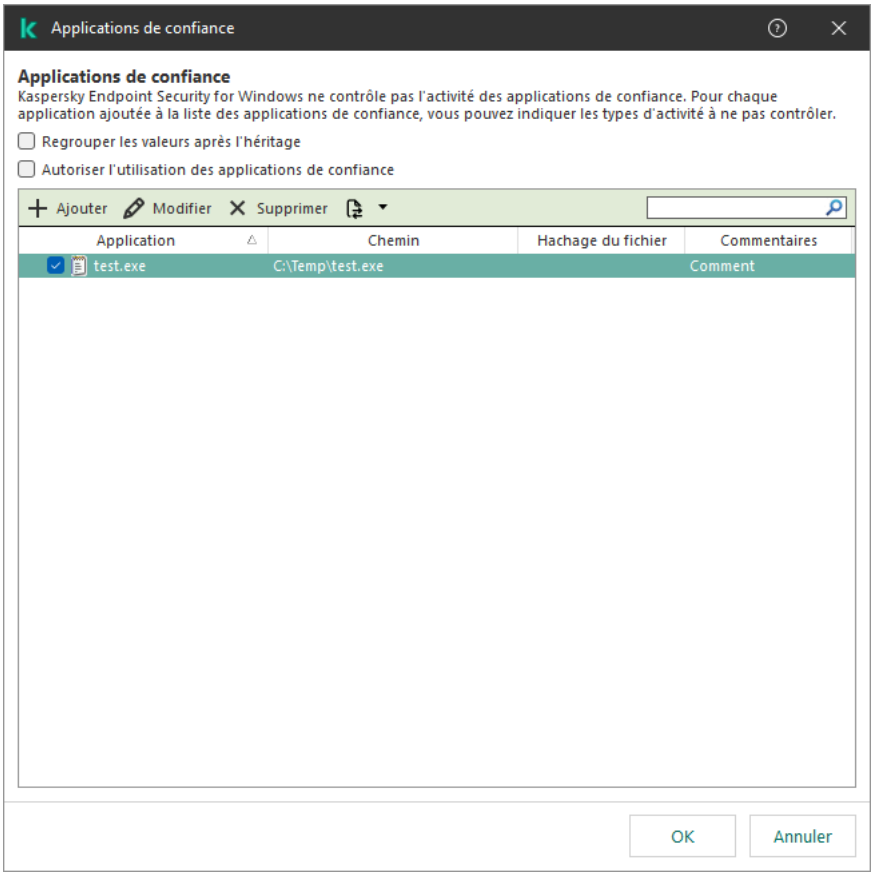
      Si vous n'avez sélectionné aucune exclusion, Kaspersky Endpoint Security exportera toutes les exclusions.

   b. Appuyez 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML. Kaspersky Endpoint Security prend également en charge l'exportation de la liste des exclusions vers un fichier DAT.



Liste des applications de confiance

7. Pour importer la liste des exclusions, procédez comme suit :

   a. Appuyez 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. Ouvrez le fichier.

      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. Kaspersky Endpoint Security prend également en charge l'importation d'une liste d'exclusions à partir d'un fichier DAT.

8. Enregistrez vos modifications.

Comment exporter ou importer la zone de confiance dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Zone de confiance**.

5. Pour exporter la liste des règles, procédez comme suit :

   a. Cliquez sur le lien **Exclusions de l'analyse des logiciels malveillants**.

   b. Sélectionnez les exclusions que vous souhaitez exporter.

   c. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des exclusions dans un fichier JSON dans le dossier des téléchargements par défaut.

6. Pour exporter la liste des applications de confiance :

   a. Sélectionnez les applications de confiance que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

      Kaspersky Endpoint Security exporte la liste des applications de confiance dans un fichier JSON dans le dossier des téléchargements par défaut.

7. Pour importer la liste des exclusions, procédez comme suit :

   a. Cliquez sur le lien **Exclusions de l'analyse des logiciels malveillants**.

   b. Appuyez sur le bouton → **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des exclusions.

c. Ouvrez le fichier.

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 JSON.

8. Pour importer une liste d'applications de confiance :

a. Cliquez sur le lien **Applications**.

b. Appuyez sur le bouton → **Importer**.

Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des applications de confiance.

c. Ouvrez le fichier.

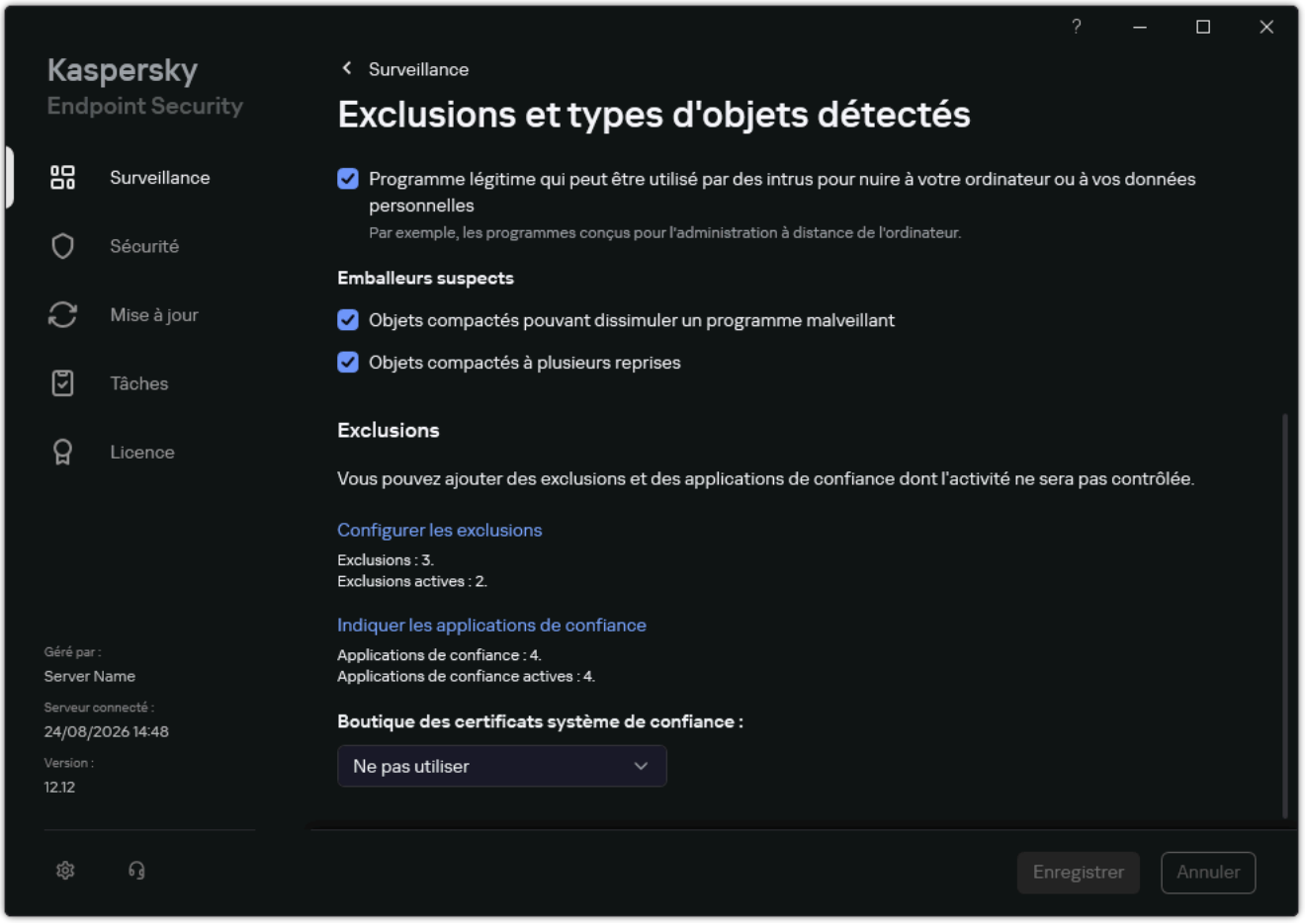
Si l'ordinateur dispose déjà d'une liste d'applications de confiance, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier JSON.

9. Enregistrez vos modifications.

Comment exporter ou importer la zone de confiance 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** → **Exclusions et types d'objets détectés**.



Paramètres des exclusions

3. Pour exporter la liste des règles, procédez comme suit :

   a. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

   b. Sélectionnez les exclusions que vous souhaitez exporter.

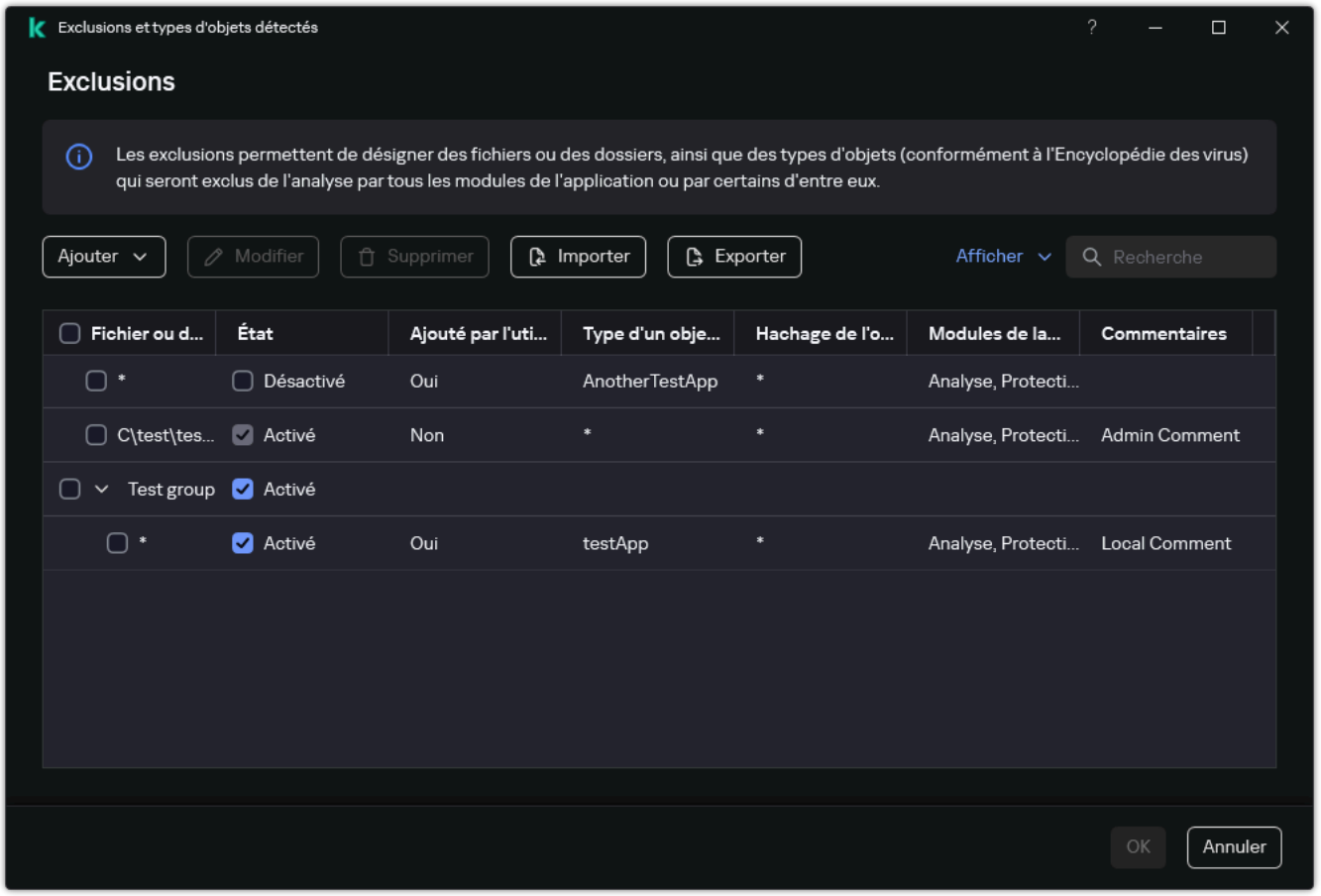
   c. Cliquez sur **Exporter**.

   d. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.

   e. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format CSV dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   f. Enregistrez le fichier.

   Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier CSV.



Liste des exclusions

4. Pour exporter la liste des applications de confiance :

   a. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.

   b. Sélectionnez les applications de confiance que vous souhaitez exporter.

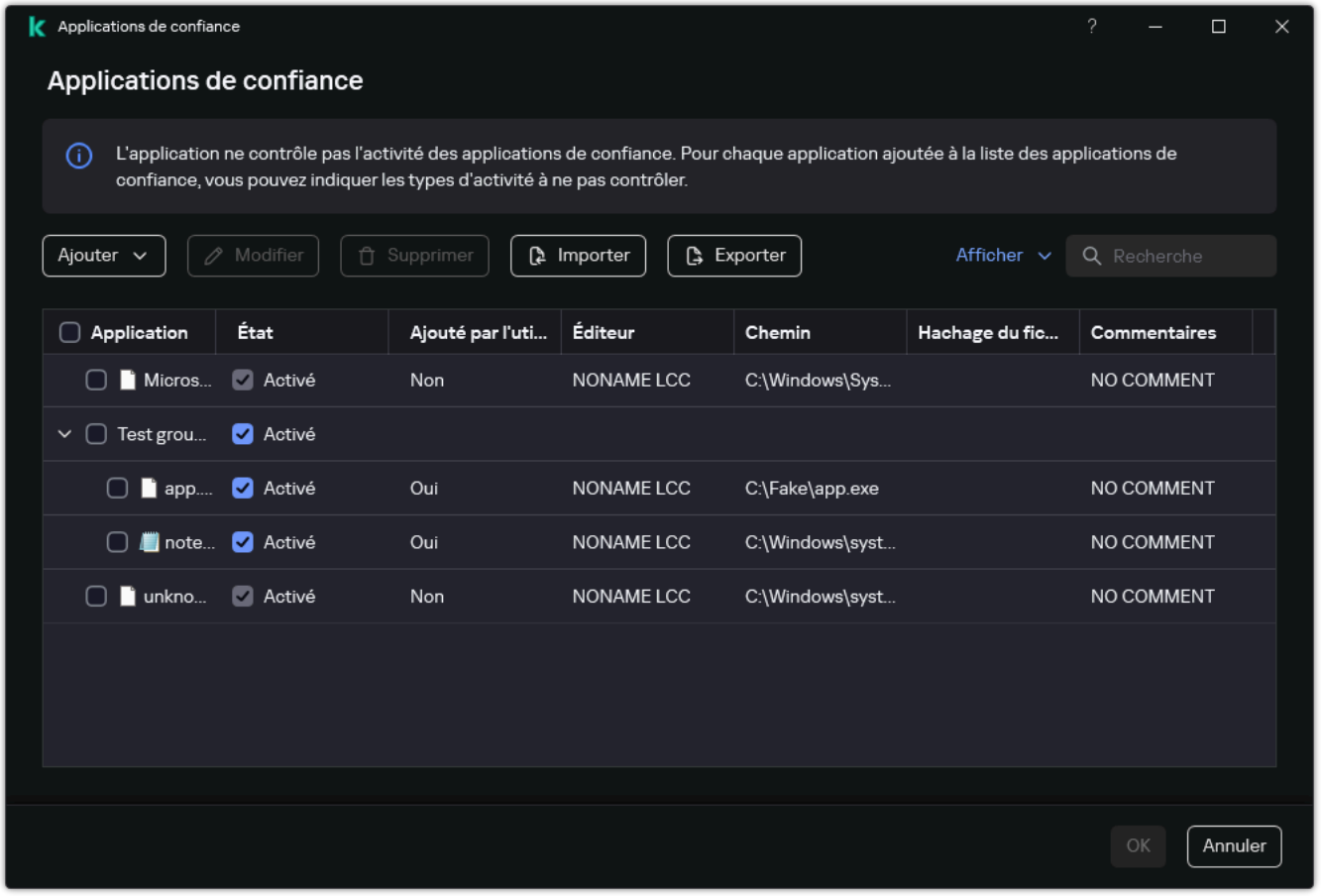
   c. Cliquez sur **Exporter**.

   d. Confirmez que vous souhaitez exporter uniquement les applications de confiance sélectionnées ou exporter la liste entière.

e. Une fenêtre s'ouvre. Dans cette fenêtre, saisissez le nom du fichier XML vers lequel vous souhaitez exporter la liste des applications de confiance et sélectionnez le dossier dans lequel vous souhaitez enregistrer ce fichier.

f. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste complète des applications de confiance dans un fichier XML.



Liste des applications de confiance

5. Pour importer la liste des exclusions, procédez comme suit :

a. Dans le groupe **Exclusions**, cliquez sur le lien **Configurer les exclusions**.

b. Cliquez sur **Importer**.

c. Dans la fenêtre qui s'ouvre, sélectionnez le fichier CSV à partir duquel vous souhaitez importer la liste des exclusions.

d. Ouvrez le fichier.

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 CSV.

6. Pour importer une liste d'applications de confiance :

a. Dans le groupe **Exclusions**, cliquez sur le lien **Indiquer les applications de confiance**.

b. Cliquez sur **Importer**.

c. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications de confiance.

d. Ouvrez le fichier.

Si l'ordinateur dispose déjà d'une liste d'applications de confiance, Kaspersky Endpoint Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

7. Enregistrez vos modifications.

Gestion des applications dotées d'une signature numérique de confiance

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*.

Comment démarrer l'utilisation d'un stockage des certificats du système de confiance dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.
4. Dans le groupe **Boutique des certificats système de confiance**, cochez la case **Utiliser la boutique des certificats système de confiance**.
5. Dans la liste déroulante, choisissez le stockage système que Kaspersky Endpoint Security devra considérer comme sécurisé.
6. Enregistrez vos modifications.

Comment démarrer l'utilisation d'un stockage des certificats du système de confiance dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Zone de confiance**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Certificats racine**.
6. Dans la fenêtre qui s'ouvre, cochez la case **Utiliser la boutique des certificats système de confiance**.
7. Sélectionnez le stockage système que Kaspersky Endpoint Security devra considérer comme sécurisé.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Comment démarrer l'utilisation d'un stockage des certificats du système de confiance 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** → **Exclusions et types d'objets détectés**.
3. Dans la liste déroulante **Boutique des certificats système de confiance**, choisissez le stockage système que Kaspersky Endpoint Security devra considérer comme sécurisé.
4. Enregistrez vos modifications.

Application. Exclusions d'analyse prédéfinies et applications de confiance

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware.

Vous pouvez sélectionner des exclusions prédéfinies et des applications de confiance comme suit :

- Installation de l'application.
  - Installation locale de l'application à l'aide de l'Assistant
  - Propriétés du paquet d'installation
- Configuration de la stratégie.
  - Assistant de création d'une stratégie
  - Propriétés de la stratégie : exclusions de l'analyse et applications de confiance.

Microsoft SQL Server

Lors de l'installation de Kaspersky Endpoint Security sur un serveur SQL, vous devez créer une zone de confiance à partir des exclusions prédéfinies et des applications de confiance pour vous assurer que le fonctionnement du serveur n'est pas entravé.

Exclusions d'analyse prédéfinies

Chemin d'accès	Version de SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Serveur Microsoft Exchange

Lors de l'installation de Kaspersky Endpoint Security sur un serveur Microsoft Exchange, vous devez créer une zone de confiance à partir des exclusions prédéfinies et des applications de confiance pour vous assurer que le fonctionnement du serveur n'est pas perturbé.

Exclusions d'analyse prédéfinies

Chemin d'accès	Version de Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Chemin d'accès	Version de Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Applications de confiance prédéfinies

Chemin d'accès	Version de Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Si Microsoft System Center Configuration Manager est installé dans le système d'exploitation de l'ordinateur protégé, vous devez ajouter une exclusion prédéfinie à la liste des exclusions de l'analyse afin de garantir la stabilité du fonctionnement de la solution.

Exclusions d'analyse prédéfinies

Chemin d'accès	Version de System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Lors de l'installation de Kaspersky Endpoint Security dans l'environnement virtuel Citrix, vous devez créer une zone de confiance à partir des exclusions prédéfinies et des applications de confiance pour vous assurer que le fonctionnement du serveur n'est pas perturbé.

Exclusions d'analyse prédéfinies

Chemin d'accès
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf

Chemin d'accès
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Applications de confiance prédéfinies

Chemin d'accès	Solution
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Applicatio bureaux vi
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Applicatio bureaux vi

Chemin d'accès	Solution
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Applicatio bureaux vi
%SystemRoot%\System32\drivers\CVhdFilter.sys	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Applicatio bureaux vi
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Applicatio bureaux vi
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Applicat d'espace de

Chemin d'accès	Solution C
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Applicat d'espace de
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Applicat d'espace de
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Approvision
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Approvision
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Approvision
%SystemRoot%\System32\drivers\bnistack6.sys	Approvision
%SystemRoot%\System32\drivers\CfsDep2.sys	Approvision
%SystemRoot%\System32\drivers\cnicteam.sys	Approvision
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Approvision
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Approvision
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Approvision
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Approvision
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Approvision
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFr
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFr

VMware

Lors de l'installation de Kaspersky Endpoint Security dans l'environnement virtuel Citrix, vous devez créer une zone de confiance à partir des applications de confiance prédéfinies pour vous assurer que le fonctionnement du serveur n'est pas perturbé.

Applications de confiance prédéfinies

Chemin d'accès	Solution VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon

Chemin d'accès	Solution VMware
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Déduplication des données dans Microsoft Windows Server

Si la déduplication des données est activée dans le système d'exploitation Microsoft Windows Server sur lequel Kaspersky Endpoint Security est installé, vous devez ajouter une application de confiance prédéfinie à la liste des applications de confiance afin d'optimiser Kaspersky Endpoint Security et de réduire la charge du processeur.

Chemin d'accès	Version de Microsoft Windows Server
`%SystemRoot%\system32\fsdmhost.exe`	Toutes les versions prises en charge

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.14.2\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.

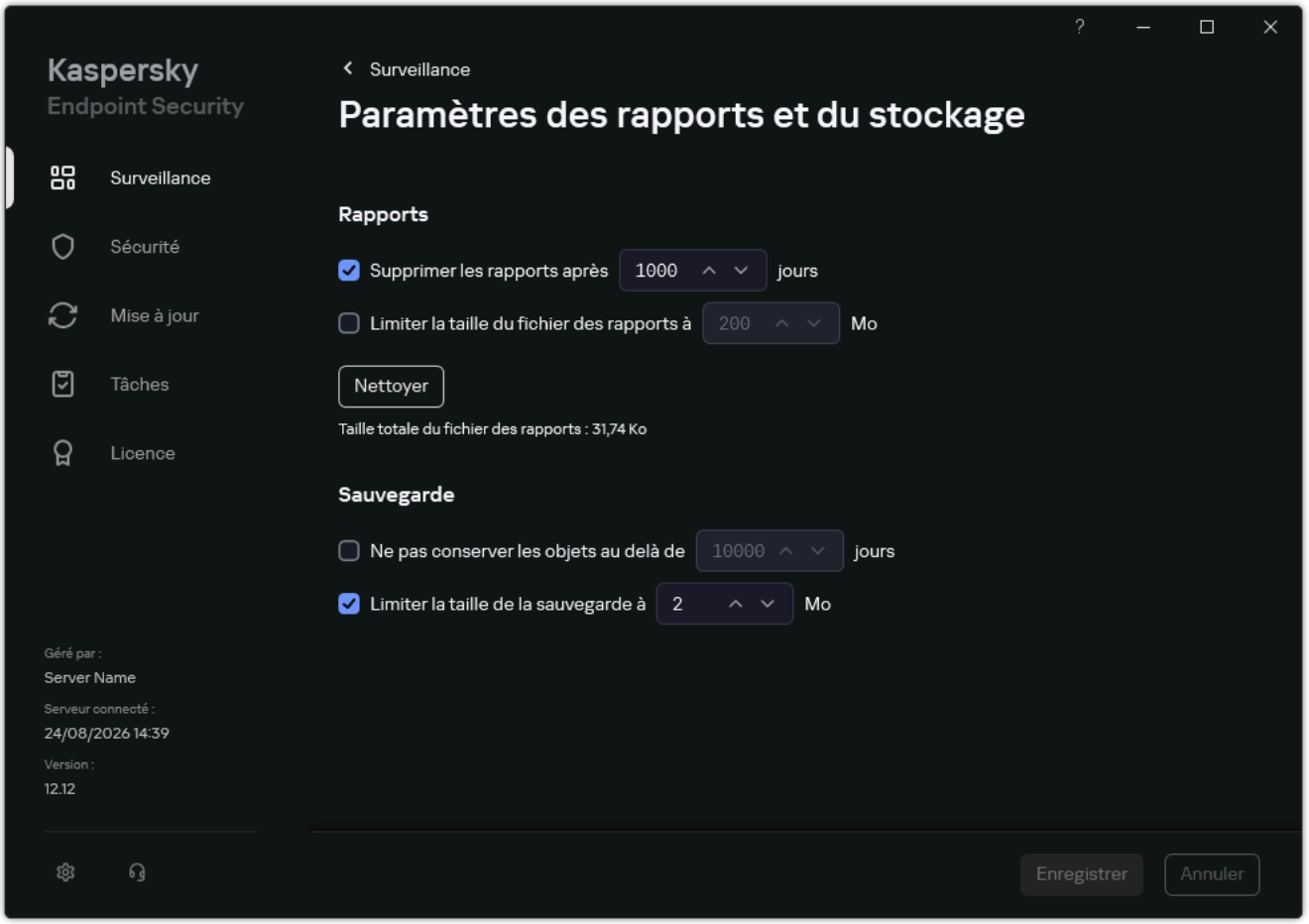
Configuration de la durée de conservation maximale des fichiers dans la sauvegarde

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sous **Paramètres généraux**, cliquez sur le lien **Rapports et stockage**.



Paramètres de sauvegarde

3. Si vous souhaitez limiter la durée de conservation des copies de fichiers dans le dossier de sauvegarde, cochez la case **Ne pas conserver les objets au delà de X jours** dans le groupe **Sauvegarde**. Indiquez la durée maximale de conservation des copies de fichiers dans le dossier de sauvegarde.

4. Enregistrez vos modifications.

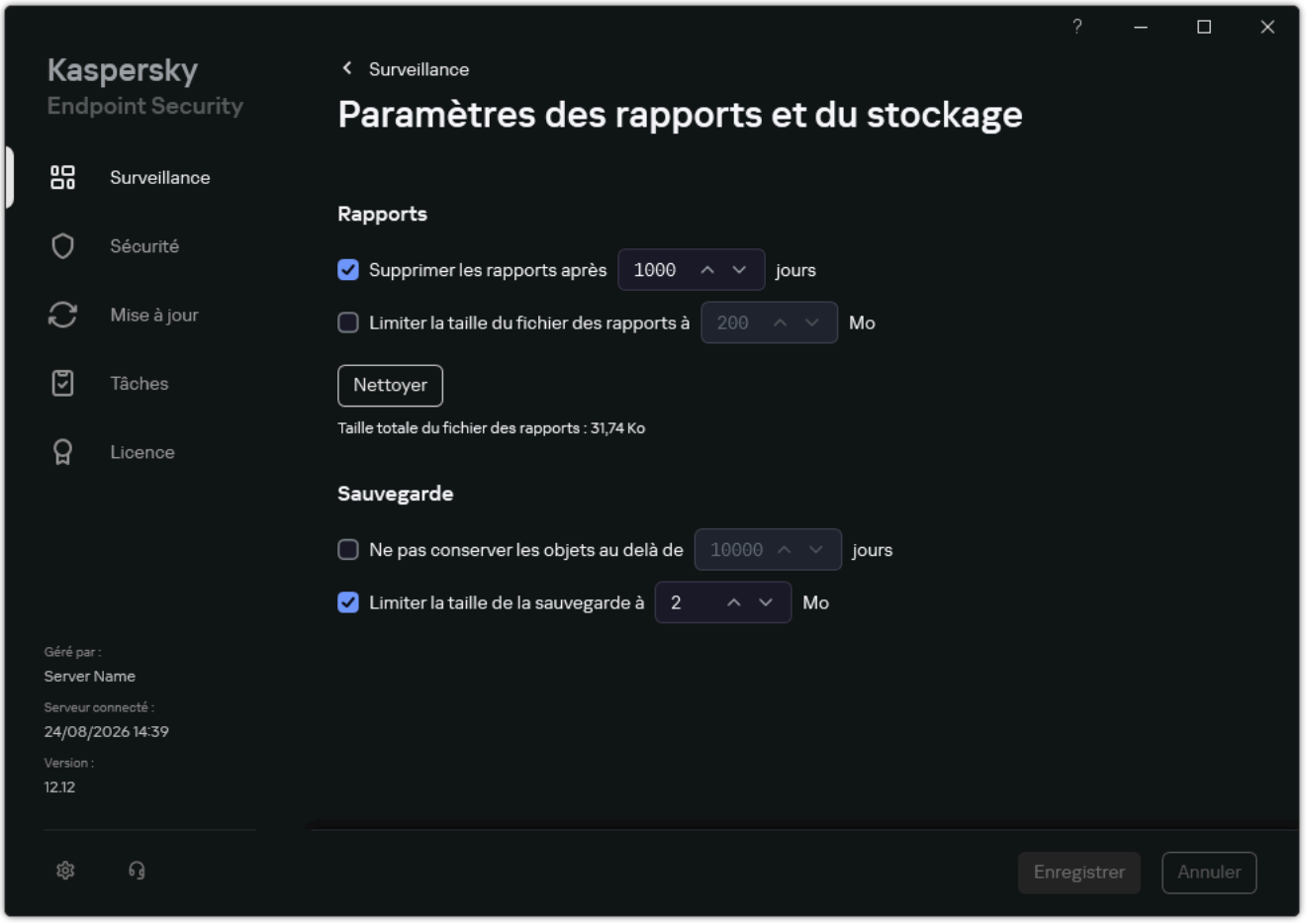
Configuration de la taille maximale de la Sauvegarde

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.

Pour configurer la taille maximale du dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sous **Paramètres généraux**, cliquez sur le lien **Rapports et stockage**.



Paramètres de sauvegarde

3. Dans le groupe **Sauvegarde**, cochez la case **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 1 024 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.

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 *Non désinfecté* 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 *Désinfecté*. 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 présentant l'état *Sera supprimé lors du redémarrage* ne peuvent 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'application de Windows Store, vous pouvez utiliser les outils du système d'exploitation (pour en savoir plus sur la restauration d'une application de Windows Store, lisez l'Aide de Microsoft Windows).

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.

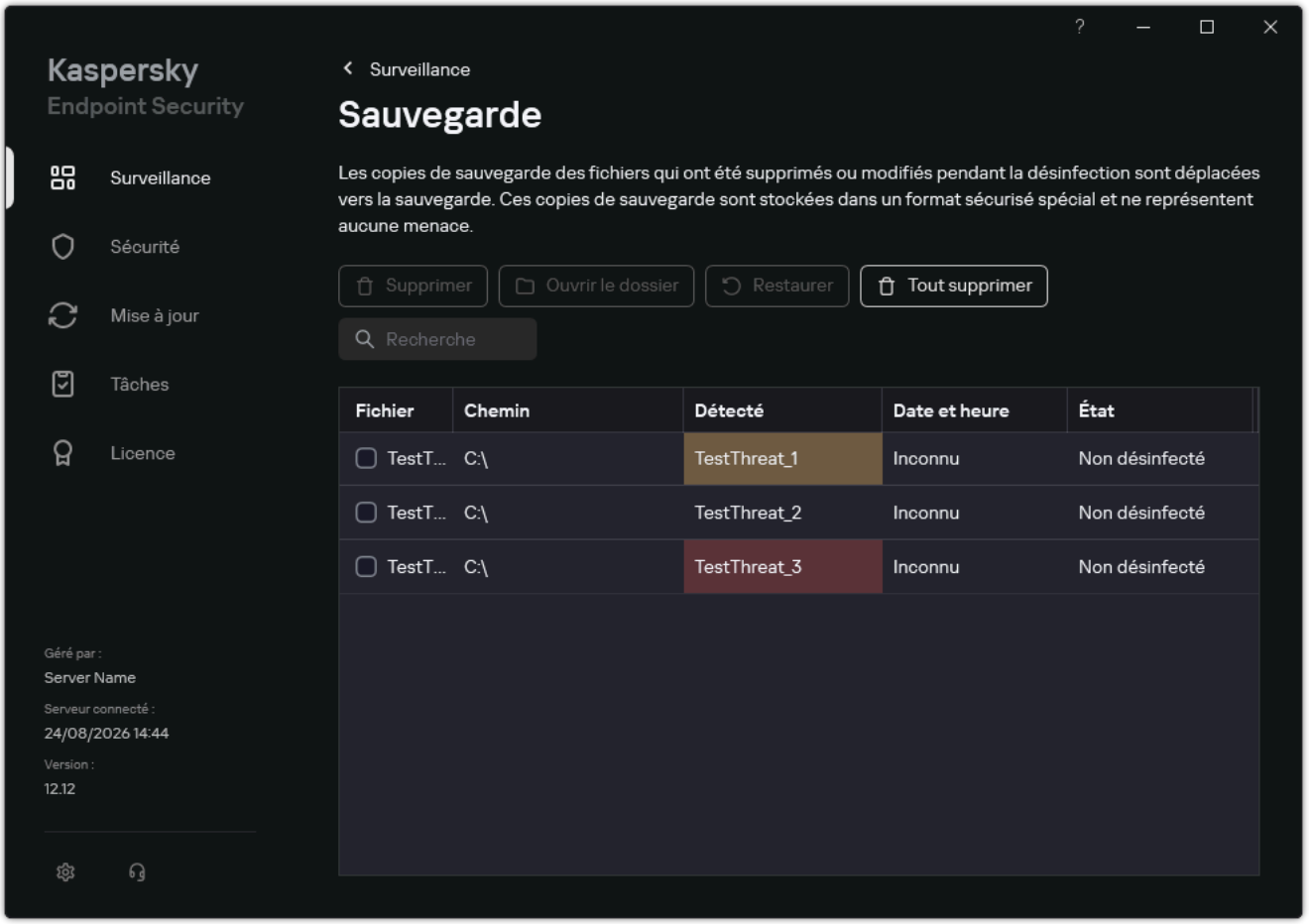
Si la Sauvegarde contient plusieurs fichiers portant le même nom, mais de contenu différent placés dans le même dossier, seul le fichier placé en dernier dans la Sauvegarde peut être restauré.

Pour restaurer des fichiers depuis le dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, dans la section **Surveillance**, cliquez sur la mosaïque **Sauvegarde**.

2. La liste des fichiers présents dans la sauvegarde s'ouvre. Dans cette liste, sélectionnez les fichiers que vous voulez restaurer et cliquez sur **Restaurer**.

Kaspersky Endpoint Security restaure tous les fichiers sélectionnés depuis le dossier de sauvegarde vers leurs dossiers d'origine.



Sauvegarde

Suppression des copies de sauvegarde des fichiers depuis le dossier de sauvegarde

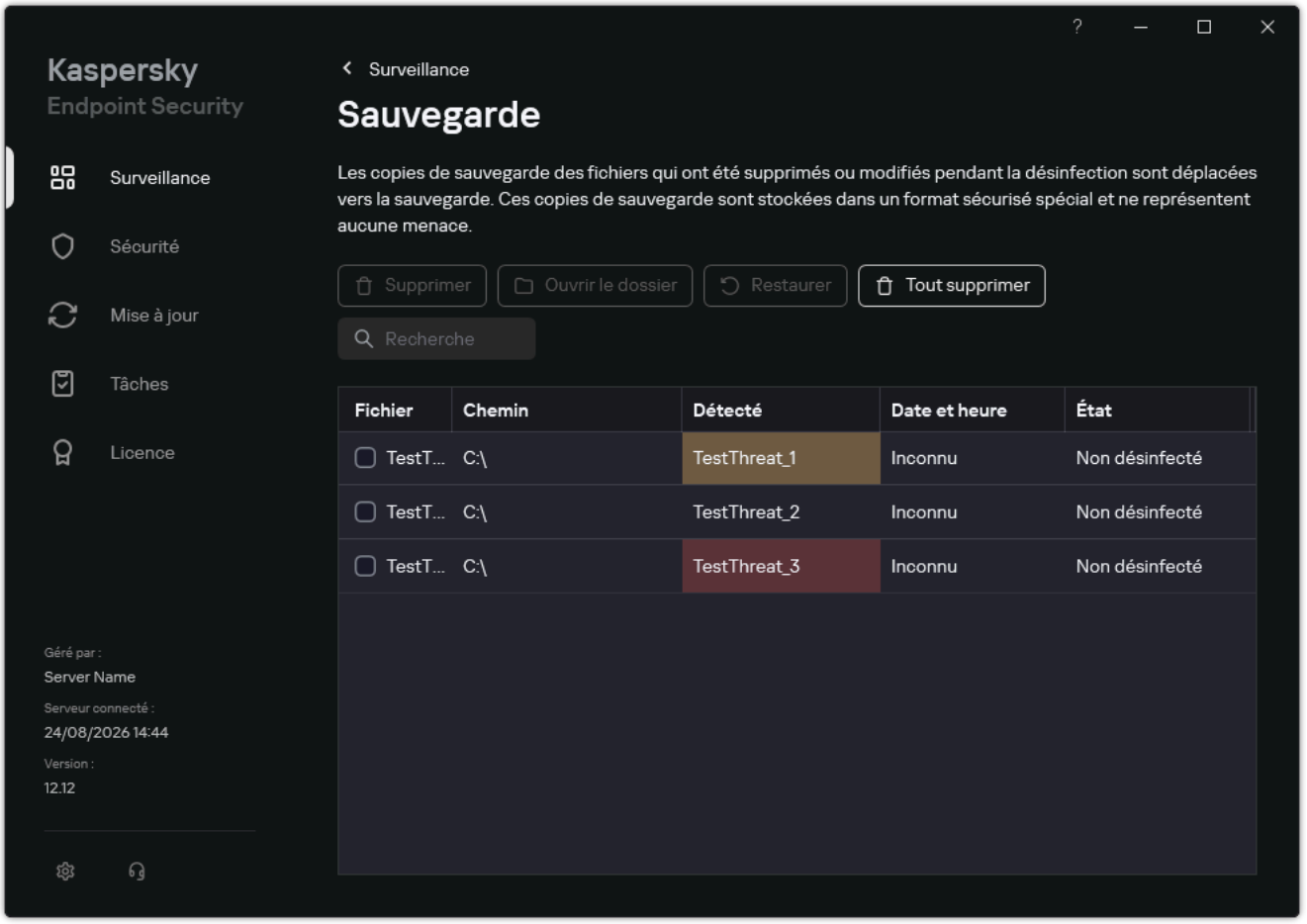
Kaspersky Endpoint Security supprime les copies de sauvegarde des fichiers de n'importe quel état automatiquement à l'issue de la période définie dans les paramètres de l'application. Vous pouvez aussi supprimer vous-même n'importe quelle copie de fichier dans la sauvegarde.

Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, dans la section **Surveillance**, cliquez sur la mosaïque **Sauvegarde**.

2. La liste des fichiers présents dans la sauvegarde s'ouvre. Dans cette liste, sélectionnez les fichiers que vous voulez supprimer de la sauvegarde et cliquez sur **Supprimer**.

Kaspersky Endpoint Security supprimera les copies de sauvegarde sélectionnées des fichiers de la sauvegarde.



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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.
3. Cliquez sur le bouton **Configurer les notifications** dans le groupe **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 de l'application. 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 chaîne `Application`.

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.

3. Cliquez sur le bouton **Configurer les notifications** dans le groupe **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 sur 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 **OK**.

8. Si vous avez activé les notifications par email, configurez les paramètres de livraison par email :

   a. Cliquez sur **Configurer les 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 **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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.

3. Dans le groupe **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.

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 le nœud **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 **Requêtes des utilisateurs** dans la liste déroulante **Sélections d'événements**.

4. Choisissez le message pour l'administrateur.

5. Cliquez sur le bouton **Ouvrir la fenêtre des propriétés des événements** dans la partie droite de l'espace de travail de la Console d'administration.

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.14.2\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 **Audit du système**. 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 Kaspersky Endpoint Security.

⊘ **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.

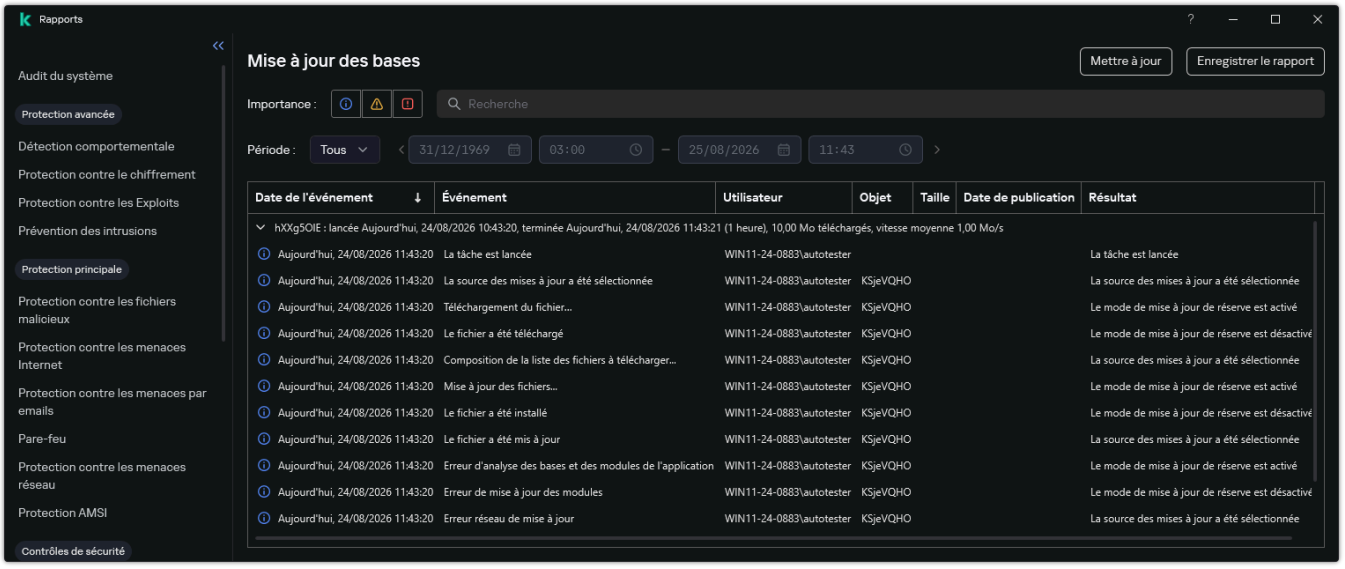
Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les informations relatives aux événements peuvent être transmises au Serveur d'administration de Kaspersky Security Center (pour en savoir plus, consultez l'aide de Kaspersky Security Center).

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, dans la section **Surveillance**, cliquez sur la mosaïque **Rapports**.



Rapports

2. Sélectionnez un module ou une tâche dans la liste des modules et des tâches.

   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.

3. Si vous souhaitez consulter des informations détaillées sur un événement, sélectionnez l'événement souhaité dans le rapport.

Un groupe reprenant des informations de synthèse sur l'événement s'affiche dans la partie inférieure de la fenêtre.

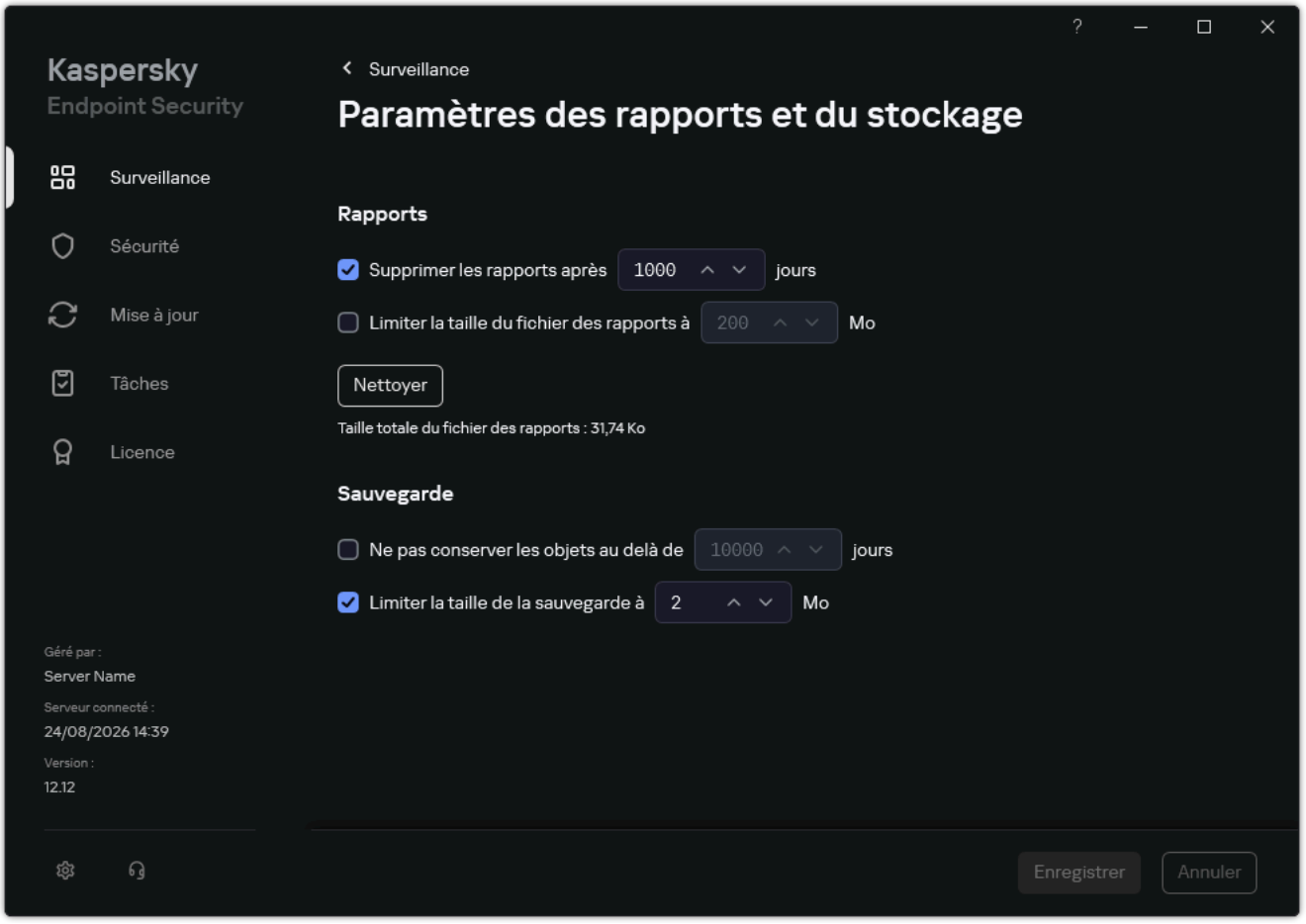
Configuration de la durée maximale de conservation des rapports

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sous **Paramètres généraux**, cliquez sur le lien **Rapports et stockage**.



Paramètres du rapport

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.

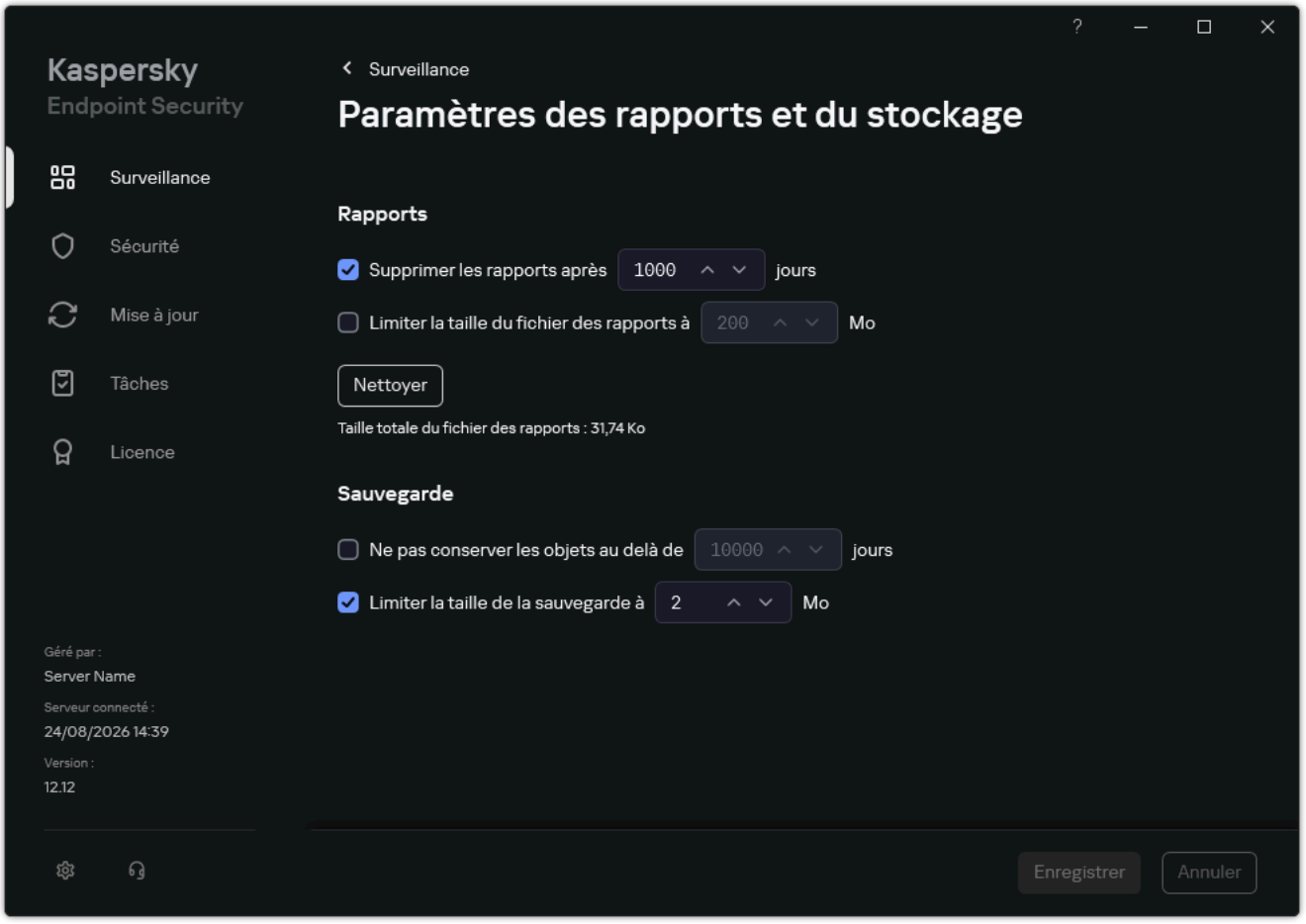
Configuration de la taille maximale du fichier de rapport

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sous **Paramètres généraux**, cliquez sur le lien **Rapports et stockage**.



Paramètres du rapport

3. Dans le groupe **Rapports**, cochez la case **Limiter la taille du fichier des 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

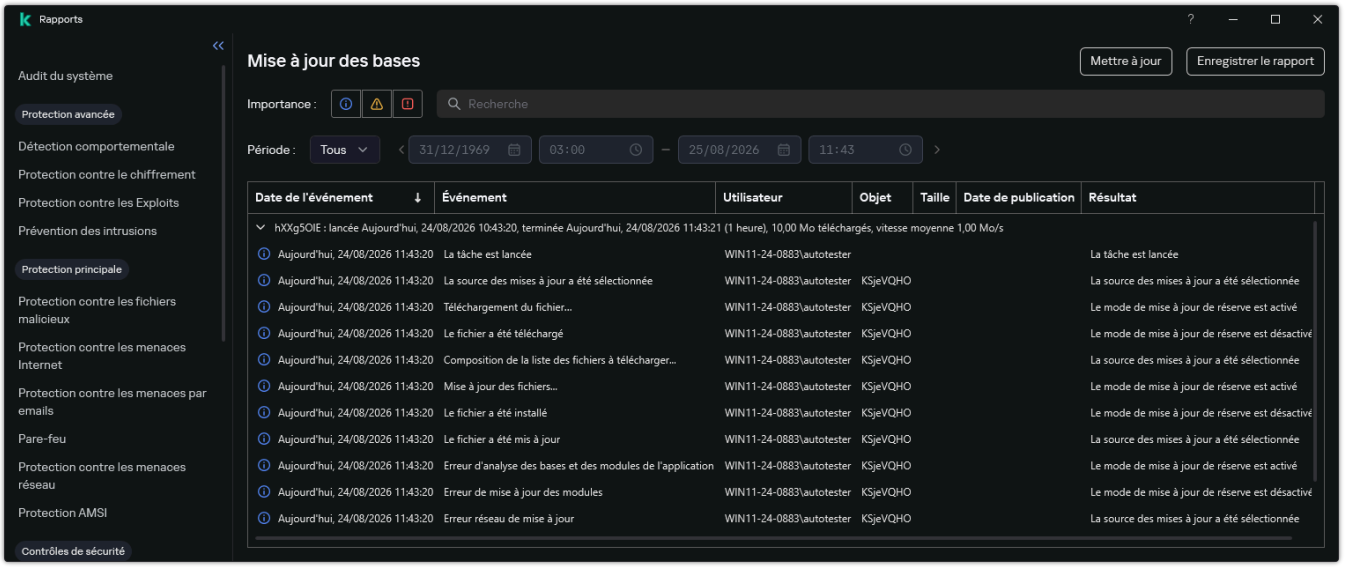
L'utilisateur est seul responsable de la sécurité des informations du rapport enregistré dans le fichier et, plus particulièrement, du contrôle et de la restriction de l'accès à ces informations.

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, dans la section **Surveillance**, cliquez sur la mosaïque **Rapports**.



Rapports

2. Une fenêtre s'ouvre. Dans cette fenêtre, 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 de rapport.

7. Sélectionnez le format du fichier de rapport nécessaire : TXT ou CSV.

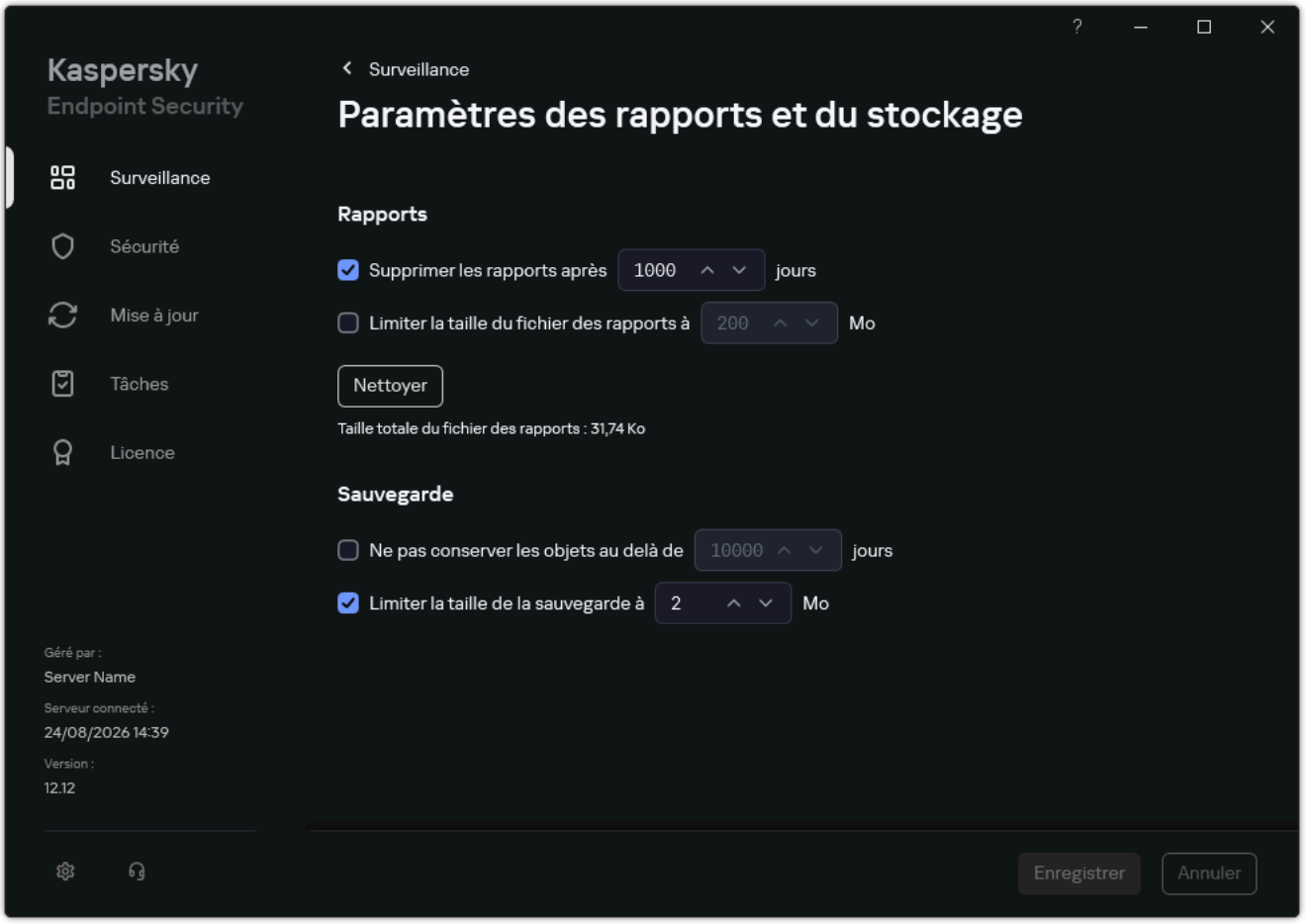
8. Enregistrez vos modifications.

Suppression des informations des rapports

Pour supprimer les informations des rapports, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.

2. Dans la fenêtre des paramètres de l'application, sous **Paramètres généraux**, cliquez sur le lien **Rapports et stockage**.



Paramètres du rapport

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 de l'autorisation requise.

Kaspersky Endpoint Security supprimera tous les rapports pour tous les modules et tâches de l'application.

Autodéfense de Kaspersky Endpoint Security

L'Autodéfense empêche d'autres applications d'effectuer des actions susceptibles d'interférer avec le fonctionnement de Kaspersky Endpoint Security et, par exemple, de supprimer Kaspersky Endpoint Security 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). L'Autodéfense inclut également la Protection par mot de passe et la Protection de la connexion au Serveur d'administration.

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).

La *Protection de la connexion au Serveur d'administration* empêche la reconnexion non autorisée de l'ordinateur à un serveur non fiable.

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 : • Fichiers du dossier d'installation de Kaspersky Endpoint Security et autres fichiers de l'application ; • Clés de registre avec des enregistrements appartenant à l'application ; • Processus 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. La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019.	✓	✓
Mécanisme de protection contre l'administration externe	Cette technologie empêche toute autre application (par exemple, TeamViewer ou RemotelyAnywhere) d'accéder à Kaspersky Endpoint Security.	✓	– (sauf pour Windows 7)

Activation et désactivation du mécanisme de l'autodéfense

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.

Cette technologie bloque l'accès aux modules d'application suivants :

- Fichiers du dossier d'installation de Kaspersky Endpoint Security et autres fichiers de l'application ;
- Clés de registre avec des enregistrements appartenant à l'application ;
- Processus que l'application exécute.

Les mécanismes d'autodéfense ne s'appliquent pas aux processus de Kaspersky Endpoint Security lancés par des processus parents non fiables.

Par défaut, le mécanisme de l'autodéfense de Kaspersky Endpoint Security est activé.

Comment activer ou désactiver l'Autodéfense dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Utilisez la case **Activer l'Autodéfense** pour activer ou désactiver le mécanisme d'autodéfense.
5. Enregistrez vos modifications.

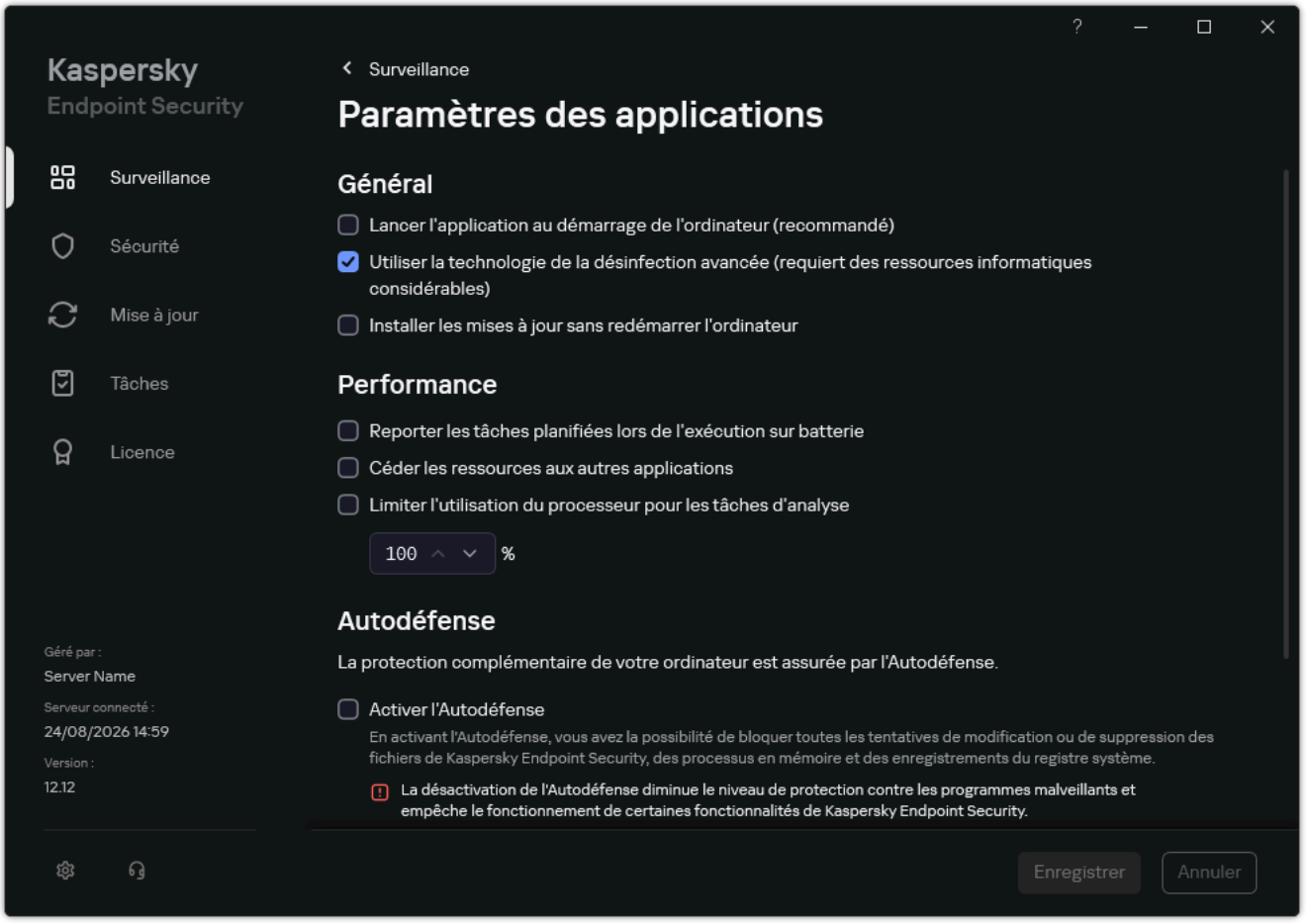
Comment activer ou désactiver l'Autodéfense dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Autodéfense**.
5. Utilisez le commutateur **Autodéfense ACTIVÉE** pour activer ou désactiver le mécanisme d'autodéfense.
6. Enregistrez vos modifications.

Comment activer ou désactiver l'Autodéfense 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

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.

Utilisez la technologie AM-PPL en permanence. Le module AM-PPL est un module important de la protection du système d'exploitation. La désactivation de la prise en charge de la technologie AM-PPL peut entraîner le dysfonctionnement de certaines fonctionnalités de Kaspersky Endpoint Security (par exemple, l'intégration de l'application avec Windows Security Center). La désactivation de la prise en charge de la technologie AM-PPL est autorisée uniquement dans un environnement de test distinct à des fins de dépannage.

La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes 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.

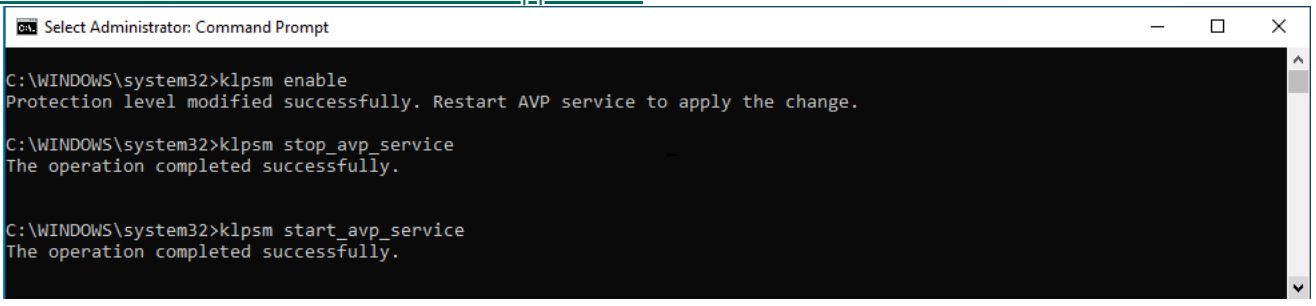
   Vous pouvez ajouter le chemin du fichier exécutable à la variable système %PATH% pendant la mise en place d'applications.

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.



Activation de la prise en charge de la technologie AM-PPL

Protection des services d'application contre l'administration externe

La protection des services d'application contre l'administration externe bloque les tentatives des utilisateurs et d'autres applications d'arrêter les services de Kaspersky Endpoint Security. La protection assure l'exploitation des services suivants :

- Kaspersky Endpoint Security Service (AVP.KES.14.2)
- Service Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

Pour quitter l'application à partir de la ligne de commande, désactivez la protection des services de Kaspersky Endpoint Security contre l'administration externe.

Vous pouvez autoriser l'administration externe des services de l'application sur les ordinateurs qui ne prennent pas en charge la technologie AM-PPL ou sur les ordinateurs sur lesquels la technologie désactivée.

Comment activer ou désactiver la Protection des services d'application contre l'administration externe dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Utilisez la case **Bloquer la gestion externe des services de l'application** pour activer ou désactiver la protection des services de Kaspersky Endpoint Security contre l'administration externe.
5. Enregistrez vos modifications.

Comment activer ou désactiver la Protection des services d'application contre l'administration externe dans Web Console et Cloud Console

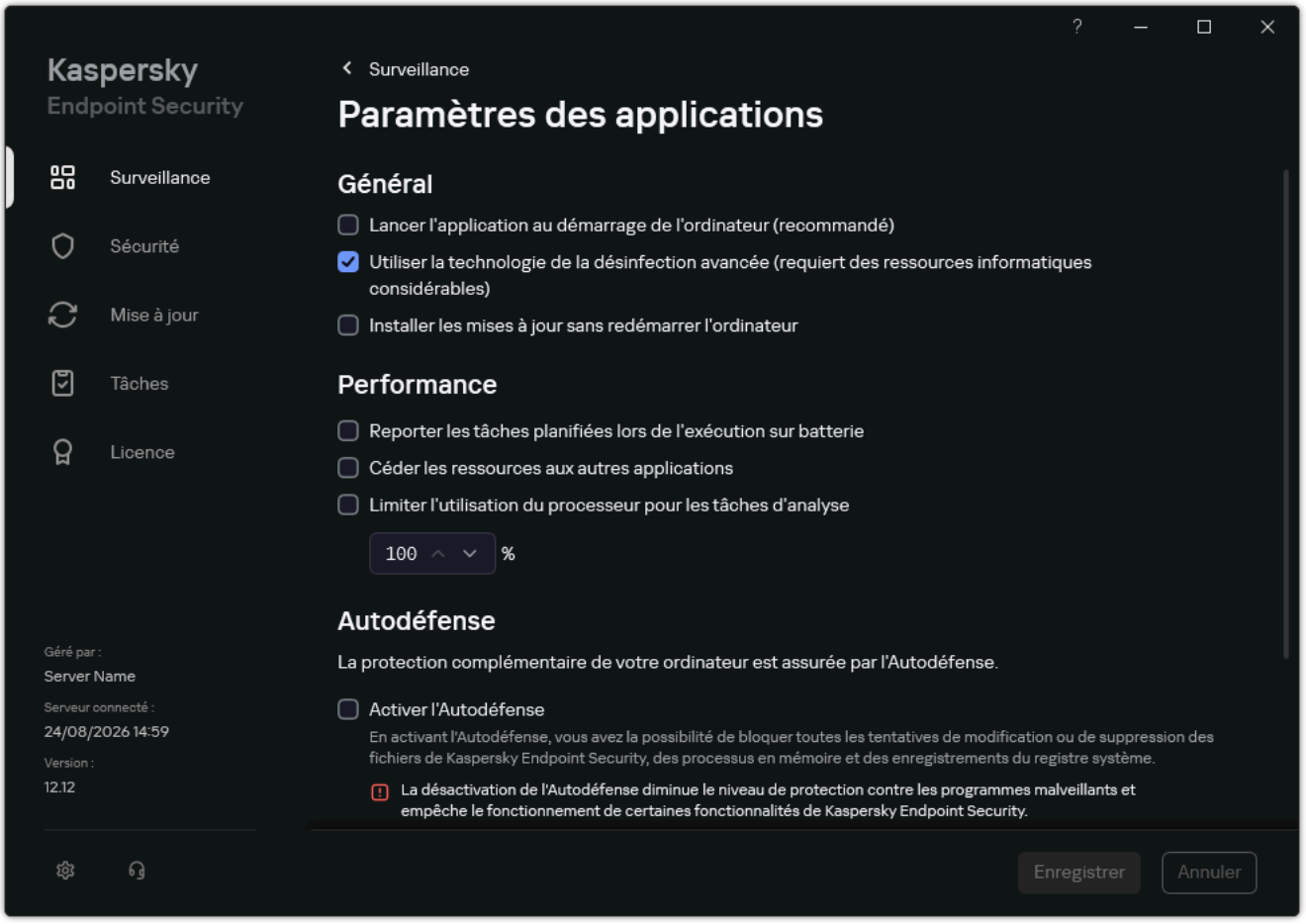
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Autodéfense**.
5. Utilisez la case **Bloquer la gestion externe des services d'applications** pour activer ou désactiver la protection des services de Kaspersky Endpoint Security contre l'administration externe.
6. Enregistrez vos modifications.

Comment activer ou désactiver la Protection des services d'application contre l'administration externe 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** → **Paramètres des applications**.

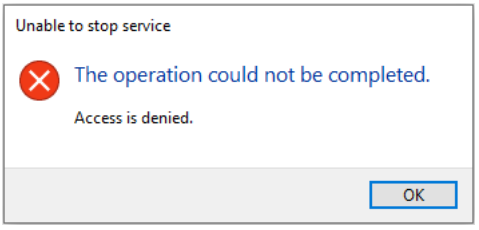


Paramètres de Kaspersky Endpoint Security for Windows

3. Utilisez la case **Bloquer la gestion externe des services de l'application** pour activer ou désactiver la protection des services de Kaspersky Endpoint Security contre l'administration externe.

4. Enregistrez vos modifications.

Par conséquent, lorsqu'un utilisateur tente d'arrêter les services d'application, une fenêtre système contenant un message d'erreur apparaît. L'utilisateur ne peut gérer les services d'application qu'à partir de l'interface de Kaspersky Endpoint Security.



Erreur d'accès aux services de l'application

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. Dans la fenêtre principale de l'application, cliquez sur le bouton ⚙.
2. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets détectés**.
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 **Autoriser l'interaction avec l'interface de Kaspersky Endpoint Security**.
7. Enregistrez vos modifications.

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 un compte utilisateur KLAdmin ou un compte ajouté manuellement.

- Saisie d'un mot de passe temporaire.

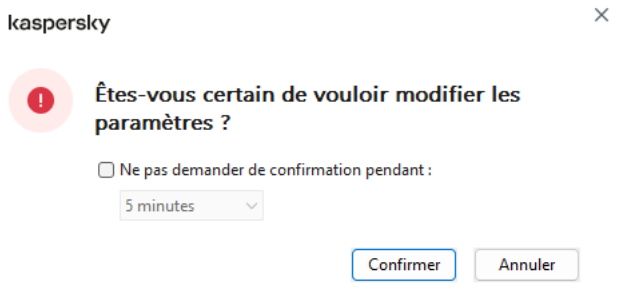
  Cette méthode est pratique quand l'utilisateur se trouve en-dehors du réseau de l'entreprise et doit absolument obtenir un accès temporaire pour pouvoir réaliser une action interdite (par exemple, quitter l'application). À l'issue de la validité du mot de passe temporaire ou à la fin de la session, l'application rétablit les valeurs antérieures des paramètres de Kaspersky Endpoint Security.

- Jeton.

  Cette méthode convient aux utilisateurs privilégiés (tels que le personnel du support technique). L'authentification par jeton permet d'utiliser le mode d'ouverture de session par carte à puce dans Active Directory. Cela améliore la sécurité de l'infrastructure de l'organisation.

Si l'utilisateur tente d'exécuter une action protégée par un mot de passe, Kaspersky Endpoint Security l'invite à saisir un nom d'utilisateur et un mot de passe, un mot de passe de jeton ou un mot de passe temporaire (voir l'illustration ci-dessous).

Dans la fenêtre de saisie du mot de passe, vous pouvez changer de langue uniquement en appuyant sur les touches **ALT+SHIFT**. L'utilisation d'autres raccourcis, même s'ils sont configurés dans le système d'exploitation, ne fonctionne pas pour le changement de langue.



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 saisir les identifiants du compte. 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.

- **Compte ajouté manuellement**. Un compte en dehors du domaine Active Directory. Vous pouvez utiliser ce compte de service au lieu du compte KLAdmin si vous ne souhaitez pas partager le mot de passe de l'administrateur. Vous pouvez définir n'importe quel nom d'utilisateur et mot de passe et configurer des autorisations individuelles.

- **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 pour la session actuelle**). 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.

Jeton

Pour accéder aux fonctionnalités de Kaspersky Endpoint Security, vous devez sélectionner le certificat utilisateur approprié dans la liste des certificats stockés sur le jeton connecté et saisir votre code PIN. L'authentification par jeton est disponible uniquement pour les utilisateurs du domaine Active Directory. L'administrateur peut configurer les autorisations pour un utilisateur individuel ou un groupe. Pour que l'authentification par jeton fonctionne, vous devez déployer une infrastructure PKI de confiance et installer un logiciel dédié à la gestion du jeton.

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).

Activation de la protection par mot de passe dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection par mot de passe**.

   Cette action ouvre une fenêtre avec les paramètres de protection par mot de passe.

5. Utilisez la case **Activer la protection par mot de passe** pour activer ou désactiver le module.

6. Sous **Autorisations**, sélectionnez le compte KLAdmin.

7. Cette action ouvre une fenêtre ; dans cette fenêtre, cliquez sur **Mot de passe** et définissez un mot de passe pour le compte KLAdmin.

   Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe.

   > Si vous avez oublié le mot de passe de votre compte KLAdmin, vous pouvez le réinitialiser dans les propriétés de la stratégie.

8. Retournez à la liste des comptes.

9. Définissez les autorisations pour tous les utilisateurs du réseau de l'entreprise.

   a. Sous **Autorisations**, sélectionnez le groupe « Tout le monde ».

      Le *groupe "Tous"* est un groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise.

   b. Dans la fenêtre qui s'est ouverte, cochez les cases en regard des actions que les utilisateurs pourront exécuter sans saisir de 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 **Fermer 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.

10. Enregistrez vos modifications.

Activation de la protection par mot de passe dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Autodéfense**.

5. Sous **Protection par mot de passe**, utilisez le commutateur **Protection par mot de passe ACTIVÉE** pour activer ou désactiver le module.

6. 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 vous avez oublié le mot de passe de votre compte KLAdmin, vous pouvez le réinitialiser dans les propriétés de la stratégie.

7. Retournez à la liste des comptes.

8. Définissez les autorisations pour tous les utilisateurs du réseau de l'entreprise.

   a. Dans le tableau des comptes, sélectionnez le groupe « Tout le monde ».

      Le *groupe "Tous"* est un groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise.

   b. Dans la fenêtre qui s'est ouverte, cochez les cases en regard des actions que les utilisateurs pourront exécuter sans saisir de 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 **Fermer 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.

9. Enregistrez vos modifications.

Activation de la protection par mot de passe 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** → **Interface**.

3. Utilisez le commutateur **Protection par mot de passe** pour activer ou désactiver le module.

4. 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.

5. Définissez les autorisations pour tous les utilisateurs du réseau de l'entreprise.

   a. Dans le tableau des comptes, 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.

6. 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

La Protection par mot de passe permet d'accorder à Kaspersky Endpoint Security l'accès à des comptes utilisateurs individuels d'Active Directory et à des comptes utilisateurs ajoutés manuellement.

Comptes utilisateurs Active Directory

Vous pouvez accorder l'accès à Kaspersky Endpoint Security à des utilisateurs individuels ou à des groupes au sein du domaine Active Directory. 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.

Comptes utilisateurs ajoutés manuellement

Vous pouvez créer un compte utilisateur qui n'est pas présent dans Active Directory et lui attribuer des autorisations individuelles. Autrement dit, vous pouvez créer un *compte utilisateur de service* et l'utiliser à la place de KLAdmin. Vous n'avez donc pas besoin de partager votre mot de passe KLAdmin avec d'autres utilisateurs ni de créer différents comptes utilisateurs Active Directory. Vous pouvez définir n'importe quel nom d'utilisateur et n'importe quel mot de passe. Par exemple, vous pouvez accorder l'autorisation **Consulter les rapports** au compte utilisateur de service. Par conséquent, si la consultation des rapports est interdite au groupe « Tous », vous pouvez ouvrir les rapports à l'aide du compte utilisateur de service ou du compte utilisateur KLAdmin.

Octroi d'autorisations à des utilisateurs ou des groupes distincts

Comment accorder des autorisations à des utilisateurs individuels ou à des groupes dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection par mot de passe**.

   Cette action ouvre une fenêtre avec les paramètres de protection par mot de passe.
5. Dans le tableau des comptes, cliquez sur **Ajouter**.
6. Sélectionnez le type de compte utilisateur que vous souhaitez ajouter :

   - **Sélectionner un utilisateur/un groupe à partir d'Active Directory** : comptes utilisateurs d'Active Directory.

     Pour sélectionner un compte utilisateur, cliquez sur **Sélectionner**. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.

   - **Ajouter un utilisateur/un groupe d'utilisateurs manuellement** pour un compte d'utilisateur de service ajouté manuellement.

     Pour ajouter un compte utilisateur de service, saisissez un nom d'utilisateur et un mot de passe (par exemple, SecureAdmin).

     > Vous pouvez réinitialiser le mot de passe d'un compte utilisateur de service dans les paramètres de la stratégie. Le mot de passe du compte utilisateur de service doit être réinitialisé de la même manière que le mot de passe du compte KLAdmin. Si la modification des paramètres de protection par mot de passe est autorisée (le « cadenas » est ouvert) ou si aucune stratégie n'est appliquée sur l'ordinateur, vous pouvez réinitialiser le mot de passe du compte de l'utilisateur de service dans l'interface de l'application. Pour ce faire, confirmez les modifications des informations relatives au compte utilisateur de service en utilisant le mot de passe KLAdmin.
7. 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 **Fermer 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.
8. Enregistrez vos modifications.

Comment accorder des autorisations à des utilisateurs individuels ou à des groupes dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Autodéfense**.
5. Dans le groupe **Protection par mot de passe**, cliquez sur le lien **Autorisations utilisateur**.

   Le formulaire permettant d'accorder les autorisations pour l'activation du mot de passe s'ouvre.
6. Cliquez sur **Ajouter**.
7. Sélectionnez le type de compte utilisateur que vous souhaitez ajouter :
   - **Sélectionner dans Active Directory** : comptes utilisateurs d'Active Directory.

     Pour sélectionner un compte utilisateur, cliquez sur **Modifier**. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.
   - **Ajouter manuellement** pour un compte d'utilisateur de service ajouté manuellement.

     Pour ajouter un compte utilisateur de service, saisissez un nom d'utilisateur et un mot de passe (par exemple, SecureAdmin).

     > Vous pouvez réinitialiser le mot de passe d'un compte utilisateur de service dans les paramètres de la stratégie. Le mot de passe du compte utilisateur de service doit être réinitialisé de la même manière que le mot de passe du compte KLAdmin. Si la modification des paramètres de protection par mot de passe est autorisée (le « cadenas » est ouvert) ou si aucune stratégie n'est appliquée sur l'ordinateur, vous pouvez réinitialiser le mot de passe du compte de l'utilisateur de service dans l'interface de l'application. Pour ce faire, confirmez les modifications des informations relatives au compte utilisateur de service en utilisant le mot de passe KLAdmin.
8. 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 **Fermer 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.
9. Cliquez sur **Ajouter**.
10. Enregistrez vos modifications.

Comment accorder des autorisations à des utilisateurs individuels ou à des groupes dans l'interface utilisateur 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** → **Interface**.

3. Dans le tableau des comptes, cliquez sur **Ajouter**.

4. Sélectionnez le type de compte utilisateur que vous souhaitez ajouter :

   - **Sélectionner un utilisateur/un groupe à partir d'Active Directory** : comptes utilisateurs d'Active Directory.

     Pour sélectionner un compte utilisateur, cliquez sur **Sélectionnez un utilisateur ou un groupe**. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.

   - **Ajouter un utilisateur manuellement** pour un compte d'utilisateur de service ajouté manuellement.

     Pour ajouter un compte utilisateur de service, saisissez un nom d'utilisateur et un mot de passe (par exemple, SecureAdmin).

     > Vous pouvez réinitialiser le mot de passe d'un compte utilisateur de service dans les paramètres de la stratégie. Le mot de passe du compte utilisateur de service doit être réinitialisé de la même manière que le mot de passe du compte KLAdmin. Si la modification des paramètres de protection par mot de passe est autorisée (le « cadenas » est ouvert) ou si aucune stratégie n'est appliquée sur l'ordinateur, vous pouvez réinitialiser le mot de passe du compte de l'utilisateur de service dans l'interface de l'application. Pour ce faire, confirmez les modifications des informations relatives au compte utilisateur de service en utilisant le mot de passe KLAdmin.

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.

Comment permettre à un utilisateur d'effectuer une action bloquée à l'aide d'un mot de passe temporaire 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 **Applications**.
6. Dans la liste des applications de Kaspersky installées sur l'ordinateur, choisissez **Kaspersky Endpoint Security for Windows (14.2)**, puis ouvrez les propriétés de l'application d'un double-clic.
7. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.
8. Cliquez sur le bouton **Paramètres** dans le groupe **Protection par mot de passe**.
9. Dans la fenêtre qui s'ouvre, dans le groupe **Mot de passe temporaire**, cliquez sur le bouton **Liste des mots de passe temporaires**.

   La fenêtre Gestion des mots de passe temporaires s'ouvre.
10. Cliquez sur **Ajouter**.
11. Dans le champ **Date d'expiration**, définissez la durée de validité du mot de passe temporaire.
12. 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.
13. Cliquez sur **Générer**.

    La fenêtre du mot de passe temporaire s'ouvre (cf. ill. ci-dessous).
14. Copiez et transmettez celui-ci à l'utilisateur.

Comment permettre à un utilisateur d'effectuer une action bloquée à l'aide d'un mot de passe temporaire via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez permettre à un utilisateur d'effectuer une action bloquée.
3. Sélectionnez l'onglet **Applications**.
4. Cliquez sur **Kaspersky Endpoint Security for Windows**.

   La fenêtre des paramètres locaux de l'application s'ouvre.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.
7. Cliquez sur le bouton **Ajouter** dans le groupe **Mots de passe temporaires**.

8. Dans le champ **Date d'expiration**, définissez la durée de validité du mot de passe temporaire.

9. 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.

10. Cliquez sur **Générer**.

    Une fenêtre contenant le mot de passe temporaire s'ouvre.

11. Copiez et transmettez celui-ci à l'utilisateur.

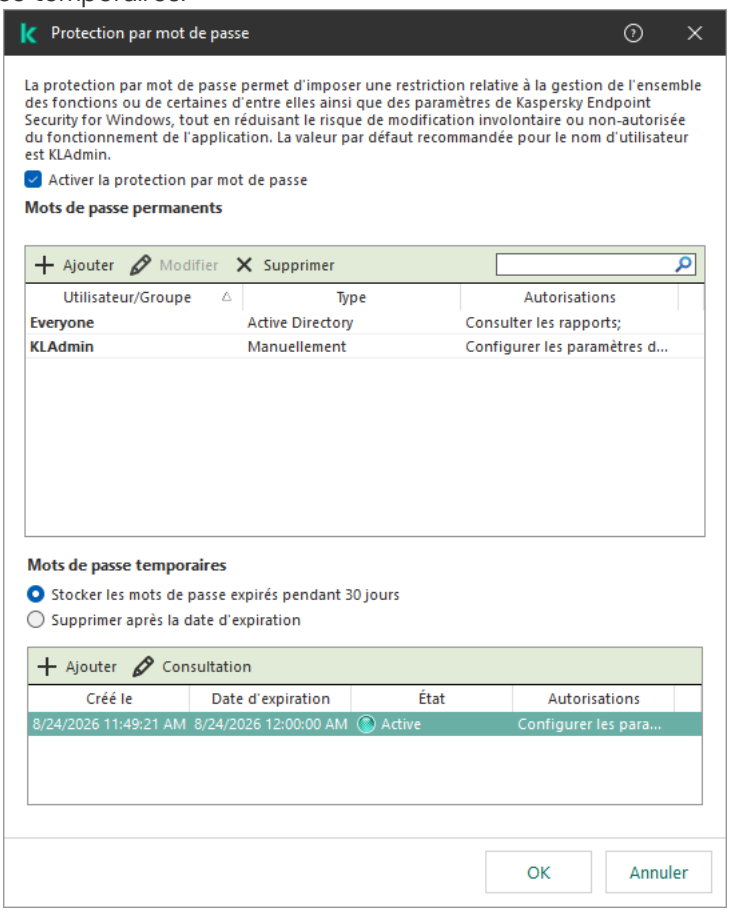
Mot de passe temporaire

Révocation du mot de passe temporaire

À partir de la version 12.9, Kaspersky Endpoint Security for Windows inclut la fonctionnalité *Gestion des mots de passe temporaires*. La gestion des mots de passe temporaires permet de réaliser les actions suivantes :

- Enregistrer l'historique des mots de passe (jusqu'à 30 jours).
- Surveiller l'état du mot de passe temporaire : *Active*, *Expirée* et *Révoquée*.

- Révoquer les mots de passe temporaires.



Gestion des mots de passe temporaires

La gestion des mots de passe temporaires met à jour l'état du mot de passe et ne révoque le mot de passe qu'après la synchronisation de l'ordinateur avec Kaspersky Security Center.

Comment révoquer un mot de passe temporaire 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 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 (14.2)**, puis ouvrez les propriétés de l'application d'un double-clic.
7. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.
8. Cliquez sur le bouton **Paramètres** dans le groupe **Protection par mot de passe**.
9. Cette action ouvre une fenêtre. Dans cette fenêtre, sous **Mot de passe temporaire**, configurez les paramètres de stockage pour les mots de passe expirés.

10. Cliquez sur **Liste des mots de passe temporaires**.

    La fenêtre Gestion des mots de passe temporaires s'ouvre. Gestion des mots de passe temporaires affiche la date d'expiration du mot de passe, l'état du mot de passe et la liste des autorisations.

11. Sélectionnez le mot de passe temporaire actif que vous souhaitez révoquer et double-cliquez sur le mot de passe pour ouvrir ses propriétés.

12. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Révoquer**.

13. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment révoquer un mot de passe temporaire à l'aide de Web Console et de Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez permettre à un utilisateur d'effectuer une action bloquée.

3. Sélectionnez l'onglet **Applications**.

4. Cliquez sur **Kaspersky Endpoint Security for Windows**.

   La fenêtre des paramètres locaux de l'application s'ouvre.

5. Sélectionnez l'onglet **Paramètres de l'application**.

6. Dans la fenêtre des paramètres de l'application, sélectionnez **Paramètres généraux** → **Interface**.

7. Sous **Mots de passe temporaires**, configurez le stockage des mots de passe expirés.

8. Cliquez sur le lien **Mot de passe temporaire**.

   La fenêtre Gestion des mots de passe temporaires s'ouvre. Gestion des mots de passe temporaires affiche la date d'expiration du mot de passe, l'état du mot de passe et la liste des autorisations.

9. Sélectionnez le mot de passe temporaire actif que vous souhaitez révoquer.

10. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Révoquer le mot de passe**.

11. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Par conséquent, la gestion des mots de passe temporaires définit l'état du mot de passe sur *Révocation (synchronisation avec un hôte)*. Après la synchronisation de l'ordinateur avec Kaspersky Security Center, l'application révoque le mot de passe temporaire et bloque immédiatement les autorisations accordées.

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.

Configurer les 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.

Désactiver les 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 désactiver des modules de la protection, ajoutez l'utilisateur ou le groupe avec l'autorisation **Désactiver les 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 **Configurer les 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 **Désactiver les modules de la protection** en plus de l'autorisation **Désactiver les modules de contrôle**.

Désactiver les 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 **Désactiver les 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 **Configurer les paramètres de l'application**.
- Pour désactiver les modules de contrôle via le menu contextuel (option **Suspendre la protection**), l'utilisateur doit avoir l'autorisation **Désactiver les modules de contrôle** en plus de l'autorisation **Désactiver les modules de la protection**.

Désactiver 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 **Désactiver la stratégie de Kaspersky Security Center** dans les paramètres de la Protection par mot de passe.

Supprimer la clé

Il n'y a aucune particularité ou restriction.

Supprimer / Modifier / Réparer 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.

Restaurer l'accès aux données sur un lecteur chiffré

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.

Restaurer depuis la Sauvegarde

Il n'y a aucune particularité ou restriction.

Exporter les paramètres

Par défaut, l'exportation des paramètres de l'application vers le groupe « Tous » est refusée. Vous pouvez exporter les paramètres de l'application à l'aide du compte utilisateur KLAdmin. L'exportation des paramètres de l'application inclut uniquement la création d'un fichier de configuration avec les paramètres de Kaspersky Endpoint Security dans l'interface de l'application. Cette autorisation ne limite pas l'exportation de listes d'exclusions d'analyses, d'adresses Internet de confiance, d'appareils de confiance ou d'autres listes gérées par des modules d'application.

Réinitialisation du mot de passe KLAdmin

Si vous avez oublié le mot de passe de votre compte KLAdmin, vous pouvez le réinitialiser dans les propriétés de la stratégie. Vous ne pouvez pas réinitialiser le mot de passe dans l'interface de l'application.

Vous pouvez effectuer des actions protégées par un mot de passe en utilisant un mot de passe temporaire. Dans ce cas, vous n'avez pas besoin de saisir les identifiants KLAdmin.

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.

Comment réinitialiser le mot de passe du compte KLAdmin à l'aide de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Interface**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection par mot de passe**.
5. Dans la fenêtre qui s'ouvre, décochez la case **Activer la protection par mot de passe**.
6. Enregistrez vos modifications.
7. Cochez de nouveau la case **Activer la protection par mot de passe**.
8. Cliquez sur le bouton **OK**.
   Cette action ouvre la fenêtre du mot de passe de l'administrateur.
9. Définissez le nouveau mot de passe pour le compte utilisateur KLAdmin et confirmez-le.
10. Enregistrez vos modifications.

Comment réinitialiser le mot de passe du compte KLAdmin dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
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. Sélectionnez l'onglet **Applications**.

4. Cliquez sur **Kaspersky Endpoint Security for Windows 14.2**.
   La fenêtre des paramètres locaux de l'application s'ouvre.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Passez à la section **Paramètres généraux** → **Autodéfense**.
7. Sous **Protection par mot de passe**, désactivez le commutateur **Protection par mot de passe**.
8. Enregistrez vos modifications.
9. Réactivez le commutateur **Protection par mot de passe**.
10. Définissez le nouveau mot de passe pour le compte utilisateur KLAdmin et confirmez-le.
11. Enregistrez vos modifications.

Par conséquent, le mot de passe de votre compte KLAdmin est mis à jour après l'application de la stratégie.

Protection de la connexion au Serveur d'administration

La connexion de l'ordinateur au Serveur d'administration est réalisée à l'aide du module *Agent d'administration* de Kaspersky Security Center. Si un intrus dispose de droits suffisants pour modifier les paramètres de connexion au serveur, il existe un risque de connexion de l'ordinateur à un serveur non fiable. Dans ce cas, l'intrus pourrait appliquer ses propres stratégies de groupe et, par exemple, désactiver l'autodéfense de l'application. Kaspersky Endpoint Security peut empêcher la reconnexion non autorisée d'un ordinateur à un autre serveur. Pour protéger la connexion au serveur, l'application propose de définir un mot de passe et d'utiliser la fonction dérivée Password-Based key Derivation Function (PBKDF2). Par conséquent, l'accès à l'application sans mot de passe est impossible.

Pour garantir une protection complète de Kaspersky Endpoint Security et de l'Agent d'administration contre les accès non autorisés, nous vous recommandons d'activer une protection supplémentaire. Pour Kaspersky Endpoint Security, nous recommandons d'activer la protection par mot de passe. Pour protéger l'Agent d'administration, nous vous recommandons de définir un mot de passe de désinstallation. Pour en savoir plus sur la protection de l'Agent d'administration contre la suppression, consultez l'aide de Kaspersky Security Center.

La gestion de la connexion de l'ordinateur au Serveur d'administration est réussie à l'aide de la tâche *Protection de la connexion au Serveur d'administration*. La tâche permet d'effectuer les opérations suivantes :

- Définir un mot de passe pour protéger la connexion au serveur.
- Modifier le mot de passe.
- Reconnecter l'ordinateur à un autre serveur.
- Désactiver la protection de la connexion au serveur.

Authentification de l'ordinateur lors de la connexion au Serveur d'administration

Après avoir défini un mot de passe, l'application crée un tableau de données en utilisant la transformation PBKDF2 du mot de passe. L'application chiffre ensuite ce tableau de données à l'aide de la clé de l'Agent d'administration. L'application utilise le tableau de données chiffrées pour vérifier les droits et privilèges du Serveur d'administration pour les connexions ultérieures.

Par la suite, à chaque tentative de reconnexion de l'ordinateur au Serveur d'administration, l'application déchiffre le tableau de données au moyen de la clé de l'Agent d'administration et le compare avec la copie locale. Si les données ne correspondent pas, l'accès à l'application est restreint.

Protection de la connexion au Serveur d'administration

Comment définir un mot de passe pour la protection de la connexion au serveur dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Protection de la connexion au Serveur d'administration**.

Étape 2. Protection de la connexion au Serveur d'administration

Définissez un mot de passe pour protéger la connexion au Serveur d'administration :

1. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger avec un mot de passe**.

2. Dans la liste déroulante **Serveur d'administration**, choisissez **Nouveau serveur**.

3. Dans le champ **Mot de passe de connexion au Serveur d'administration**, définissez un mot de passe pour la connexion au Serveur d'administration et confirmez-le.

   Si vous oubliez le mot de passe, vous pouvez le modifier à l'aide d'une tâche.

4. Si la version 12.7 ou une version antérieure de l'application Kaspersky Endpoint Security est déployée, cochez la case **Activer la compatibilité du chiffrement des mots de passe pour les versions antérieures de l'application (12.7 et antérieures)**.

   À partir de Kaspersky Endpoint Security 12.8 for Windows, l'application utilise un chiffrement renforcé du mot de passe. Si la version 12.8 ou une version ultérieure de Kaspersky Endpoint Security est déployée, nous vous recommandons de décocher cette case et d'utiliser le chiffrement renforcé du mot de passe. Les versions antérieures de l'application ne prennent pas en charge le chiffrement renforcé du mot de passe. Pour exécuter la tâche, vous devez cocher la case.

Étape 3. Sélection du compte utilisateur pour lancer la tâche

Choisissez le **Compte par défaut**. Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

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

Sous **Lancement planifié**, sélectionnez **Manuel**.

Étape 5. Définition du nom de la tâche

Saisissez un nom de tâche, par exemple, *Mot de passe de connexion au serveur principal*.

Étape 6. Fin de la création de la tâche

Quittez l'Assistant. Cochez la case **&Lancer la tâche à la fin de l'Assistant** ou exécutez la tâche manuellement. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment définir un mot de passe pour la protection de la connexion au serveur dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Protection de la connexion au Serveur d'administration**.

c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Mot de passe de connexion au serveur principal*.

d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte utilisateur par défaut. Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la tâche **Protection de la connexion au Serveur d'administration** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger avec un mot de passe**.

10. Dans la liste déroulante **Connexion au Serveur d'administration**, choisissez **Nouveau mot de passe**.

11. Dans le champ **Mot de passe de connexion au Serveur d'administration**, définissez un mot de passe pour la connexion au Serveur d'administration et confirmez-le.

    Si vous oubliez le mot de passe, vous pouvez le modifier à l'aide d'une tâche.

12. Si la version 12.7 ou une version antérieure de l'application Kaspersky Endpoint Security est déployée, cochez la case **Activer la compatibilité avec le chiffrement des mots de passe pour les versions antérieures de l'application (12.7 et versions antérieures)**.

    À partir de Kaspersky Endpoint Security 12.8 for Windows, l'application utilise un chiffrement renforcé du mot de passe. Si la version 12.8 ou une version ultérieure de Kaspersky Endpoint Security est déployée, nous vous recommandons de décocher cette case et d'utiliser le chiffrement renforcé du mot de passe. Les versions antérieures de l'application ne prennent pas en charge le chiffrement renforcé du mot de passe. Pour exécuter la tâche, vous devez cocher la case.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

Reconnexion de l'ordinateur à un autre Serveur d'administration

La reconnexion de l'ordinateur à un autre Serveur d'administration implique les étapes suivantes :

1. Dans la console du serveur `[KSC1]` actuel, exécutez la tâche *Modification du Serveur d'administration* pour l'Agent d'administration.

Après l'exécution de la tâche, l'ordinateur est reconnecté au nouveau serveur `[KSC2]`.

L'ordinateur s'affichera dans la console de serveur `[KSC1]` avec l'état *Critique*. Il est impossible de configurer l'application à l'aide de stratégies ou d'exécuter des tâches à distance sur l'ordinateur.

2. Dans la console du nouveau serveur `[KSC2]`, créez une tâche *Protection de la connexion au Serveur d'administration* pour Kaspersky Endpoint Security. Dans les propriétés de la tâche, saisissez le mot de passe du serveur précédent et définissez un mot de passe pour le nouveau serveur.

   Comment définir un nouveau mot de passe pour se reconnecter à un nouveau serveur dans la Console d'administration (MMC)

   1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

      La liste des tâches s'ouvre.

   2. Cliquez sur **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 (14.2)** → **Protection de la connexion au Serveur d'administration**.

Étape 2. Protection de la connexion au Serveur d'administration

Définissez un mot de passe pour protéger la connexion au nouveau Serveur d'administration :

1. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger avec un mot de passe**.

2. Dans la liste déroulante **Serveur d'administration**, choisissez **Se reconnecter à partir d'un autre serveur**.

3. Dans le champ **Mot de passe actuel**, saisissez le mot de passe défini pour la connexion au serveur de confiance précédemment utilisé.

4. Dans le champ **Nouveau mot de passe**, définissez un mot de passe pour la connexion au nouveau Serveur d'administration et confirmez-le.

   Si vous oubliez le mot de passe, vous pouvez le modifier à l'aide d'une tâche.

5. Si la version 12.7 ou une version antérieure de l'application Kaspersky Endpoint Security est déployée, cochez la case **Activer la compatibilité du chiffrement des mots de passe pour les versions antérieures de l'application (12.7 et antérieures)**.

   À partir de Kaspersky Endpoint Security 12.8 for Windows, l'application utilise un chiffrement renforcé du mot de passe. Si la version 12.8 ou une version ultérieure de Kaspersky Endpoint Security est déployée, nous vous recommandons de décocher cette case et d'utiliser le chiffrement renforcé du mot de passe. Les versions antérieures de l'application ne prennent pas en charge le chiffrement renforcé du mot de passe. Pour exécuter la tâche, vous devez cocher la case.

Étape 3. Sélection du compte utilisateur pour lancer la tâche

Choisissez le **Compte par défaut**. Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

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

Sous **Lancement planifié**, sélectionnez **Manuel**.

Étape 5. Définition du nom de la tâche

Saisissez un nom de tâche, par exemple, *Mot de passe de connexion au serveur principal*.

Étape 6. Fin de la création de la tâche

Quittez l'Assistant. Cochez la case **&Lancer la tâche à la fin de l'Assistant** ou exécutez la tâche manuellement. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment définir un nouveau mot de passe pour se reconnecter à un nouveau serveur dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Protection de la connexion au Serveur d'administration**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Mot de passe de connexion au serveur principal*.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Sélectionnez un compte utilisateur par défaut. Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la tâche **Protection de la connexion au Serveur d'administration** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger avec un mot de passe**.

10. Dans la liste déroulante **Connexion au Serveur d'administration**, choisissez **Se reconnecter à partir d'un autre serveur**.

11. Dans le champ **Mot de passe actuel**, saisissez le mot de passe défini pour la connexion au serveur de confiance précédemment utilisé.

12. Dans le champ **Nouveau mot de passe**, définissez un mot de passe pour la connexion au nouveau Serveur d'administration et confirmez-le.

    Si vous oubliez le mot de passe, vous pouvez le modifier à l'aide d'une tâche.

13. Si la version 12.7 ou une version antérieure de l'application Kaspersky Endpoint Security est déployée, cochez la case **Activer la compatibilité avec le chiffrement des mots de passe pour les versions antérieures de l'application (12.7 et versions antérieures)**.

    À partir de Kaspersky Endpoint Security 12.8 for Windows, l'application utilise un chiffrement renforcé du mot de passe. Si la version 12.8 ou une version ultérieure de Kaspersky Endpoint Security est déployée, nous vous recommandons de décocher cette case et d'utiliser le chiffrement renforcé du mot de passe. Les versions antérieures de l'application ne prennent pas en charge le chiffrement renforcé du mot de passe. Pour exécuter la tâche, vous devez cocher la case.

14. Enregistrez vos modifications.

15. Cochez la case en regard de la tâche.

16. Cliquez sur **Démarrer**.

    Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

Une fois que la tâche a été accomplie, assurez-vous que l'ordinateur présente l'état *OK* dans la console du nouveau serveur `[KSC2]`. Vérifiez si vous pouvez exécuter des tâches à distance et configurer l'application à l'aide de stratégies.

Réinitialisation du mot de passe de connexion au Serveur d'administration

Si vous avez oublié votre mot de passe de connexion au Serveur d'administration ou si le mot de passe est compromis, vous pouvez réinitialiser le mot de passe dans les propriétés de la tâche. Vous pouvez également réinitialiser le mot de passe et en définir un nouveau pour un groupe d'ordinateurs présentant des états de protection de la connexion au Serveur d'administration différents. Autrement dit, si la protection est activée sur certains ordinateurs et désactivée sur d'autres, la tâche définit un mot de passe pour tous les ordinateurs.

Vous pouvez réinitialiser le mot de passe de connexion au Serveur d'administration uniquement dans la console du serveur de confiance auquel l'ordinateur est connecté.

Comment réinitialiser le mot de passe de connexion au Serveur d'administration à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.
3. Sélectionnez la tâche **Protection de la connexion au Serveur d'administration** et ouvrez les propriétés de la tâche d'un double-clic.
4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.
5. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger et modifier le mot de passe**.
6. Dans le champ **Mot de passe de connexion au Serveur d'administration**, définissez un nouveau mot de passe pour la connexion au serveur de confiance actuel et confirmez-le.
7. Enregistrez vos modifications.
8. Exécutez la tâche.

Comment réinitialiser le mot de passe de connexion au Serveur d'administration dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur la tâche **Protection de la connexion au Serveur d'administration** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Protéger et modifier le mot de passe**.
5. Dans le champ **Mot de passe de connexion au Serveur d'administration**, définissez un nouveau mot de passe pour la connexion au serveur de confiance actuel et confirmez-le.
6. Enregistrez vos modifications.
7. Cochez la case en regard de la tâche.
8. Cliquez sur **Démarrer**.

Une fois que la tâche est terminée, le mot de passe de connexion au Serveur d'administration est réinitialisé.

Désactivation de la protection de la connexion au Serveur d'administration

Vous pouvez désactiver à distance la protection de la connexion au Serveur d'administration uniquement dans la console du serveur de confiance auquel l'ordinateur est connecté. Vous pouvez également désactiver la protection localement à l'aide de la ligne de commande.

Comment désactiver la protection de la connexion au serveur dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.
3. Sélectionnez la tâche **Protection de la connexion au Serveur d'administration** et ouvrez les propriétés de la tâche d'un double-clic.
4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.
5. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Ne pas protéger**.
6. Enregistrez vos modifications.
7. Exécutez la tâche.

   Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

Comment désactiver la protection de la connexion au serveur dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur la tâche **Protection de la connexion au Serveur d'administration** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sous **Protection de la connexion au Serveur d'administration**, sélectionnez **Ne pas protéger avec un mot de passe**.
5. Enregistrez vos modifications.
6. Cochez la case en regard de la tâche.
7. Cliquez sur **Démarrer**.

   Vous pouvez suivre l'état de la tâche, la quantité d'appareils sur lesquels l'exécution de la tâche a réussi ou échoué.

Comment désactiver la protection de la connexion au serveur à l'aide 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 fichier exécutable de Kaspersky Endpoint Security.

3. Exécutez la commande:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   où `<password>` est le mot de passe du compte utilisateur KL Admin ou le mot de passe de la tâche *Protection de la connexion au Serveur d'administration*. Si le paramètre n'est pas indiqué, Kaspersky Endpoint Security vous invite à saisir un mot de passe à la ligne suivante.

   > L'exécution de la commande requiert l'activation de la Protection par mot de passe.

Exemple

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

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 Advanced Encryption Standard (AES).

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.

Si Kaspersky Endpoint Security est installé sur un ordinateur doté d'un processeur ARM, seul le chiffrement de disque BitLocker est disponible. L'application ne prend pas en charge les autres modules de chiffrement des données.

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 (TPM), 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 *Administrer 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 Single Sign-On (SSO) 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 Endpoint 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 **Chiffrer uniquement l'espace occupé** activée, 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 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.

- Si Kaspersky Endpoint Security est installé sur un ordinateur basé sur l'architecture ARM, seul le chiffrement complet du disque utilisant la technologie BitLocker Drive Encryption est disponible, les autres modules de chiffrement ne sont pas pris en charge.

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, IEEE1934, 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 ExpressCache.
- 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 ThinkCentre 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 10O
- 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 fichier 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

Kaspersky Disk Encryption n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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 chiffrements 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 QWERTY) ;
- 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

Lancement de 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.

Avant de commencer le chiffrement du disque, vous devez vérifier les paramètres des comptes 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. 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 (voir les instructions ci-dessous). Vous pouvez également utiliser la technologie d'authentification unique (SSO).

Kaspersky Endpoint Security vous permet de créer automatiquement un Agent d'authentification pour les groupes d'utilisateurs suivants :

- **Tous les comptes de l'ordinateur**. Tous les comptes de l'ordinateur qui ont été actifs à un moment donné.
- **Tous les comptes de domaine de l'ordinateur**. Tous les comptes de l'ordinateur qui appartiennent à un domaine et qui ont été actifs à un moment donné.
- **Tous les comptes locaux de l'ordinateur**. Tous les comptes locaux de l'ordinateur qui ont été actifs à un moment donné.
- **Compte de service avec un mot de passe à usage unique**. Le compte de service est nécessaire pour accéder à l'ordinateur, par exemple lorsque l'utilisateur a oublié son mot de passe. Vous pouvez également utiliser le compte de service comme un compte de réserve. Vous devez saisir le nom du compte (par défaut, `ServiceAccount`). Kaspersky Endpoint Security crée automatiquement un mot de passe. Vous pouvez trouver le mot de passe dans Kaspersky Security Center Console.
- **Administrateur local**. Kaspersky Endpoint Security crée un compte utilisateur de l'Agent d'authentification pour l'administrateur local de l'ordinateur.
- **Gestionnaire de l'ordinateur**. Kaspersky Endpoint Security crée un compte utilisateur de l'Agent d'authentification pour le compte du gestionnaire de l'ordinateur. Vous pouvez déterminer quel compte présente le rôle de gestionnaire de l'ordinateur dans les propriétés de l'ordinateur dans Active Directory. Par défaut, le rôle de gestionnaire de l'ordinateur n'est pas défini, c'est-à-dire qu'il ne correspond à aucun compte.
- **Compte actif**. Kaspersky Endpoint Security crée automatiquement un compte d'Agent d'authentification pour le compte qui est actif au moment du chiffrement du disque.

Pour configurer les paramètres d'authentification des utilisateurs, utilisez la tâche *Administrer les comptes de l'Agent d'authentification*. Vous pouvez utiliser cette tâche pour ajouter de nouveaux comptes, modifier les paramètres des comptes actuels ou supprimer des comptes si nécessaire. 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.

Comment lancer Kaspersky Disk Encryption via la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
4. Dans la liste déroulante **Technologie de chiffrement**, choisissez **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.

5. Dans la liste déroulante **Mode de chiffrement**, choisissez **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.

6. Configurez les paramètres complémentaires de Kaspersky Disk Encryption (cf. tableau ci-dessous).
7. Enregistrez vos modifications.

Comment lancer Kaspersky Disk Encryption via Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données** → **Chiffrement du disque**.
5. Sélectionnez la technologie **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.

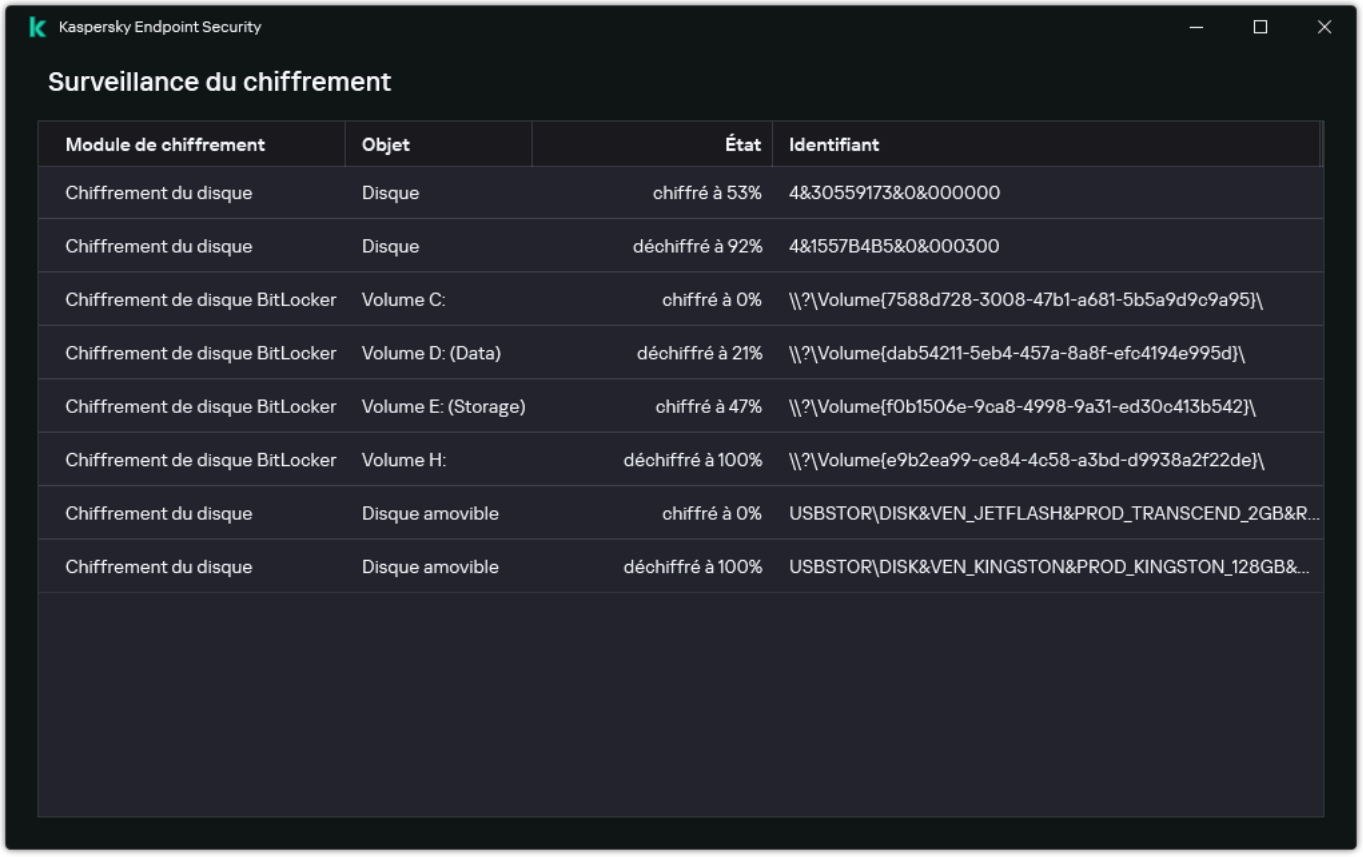
6. Dans le groupe **Action sur les appareils**, sélectionnez l'option **Chiffrer tous les disques durs**.

   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.

   Si certains disques durs doivent être exclus du chiffrement, consignez-les dans une liste.

7. Configurez les paramètres complémentaires de Kaspersky Disk Encryption (cf. tableau ci-dessous).
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.



Surveillance du chiffrement

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.

Paramètres du module Kaspersky Disk Encryption

Paramètre	Description
Créez automatiquement des comptes de l'Agent d'authentification pour utilisateurs lors du chiffrement	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 *Administrer les comptes de l'Agent d'authentification* pour les ordinateurs avec des disques déjà chiffrés.
Enregistrer le nom d'utilisateur saisi dans l'Agent d'authentification	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.

Paramètre	Description
Chiffrer uniquement l'espace occupé (réduit la durée du chiffrement)	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. 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. Par défaut, la case est décochée.
Utiliser le Legacy USB Support (déconseillé)	La case active ou désactive la fonctionnalité 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'incidence 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.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
4. Dans la liste déroulante **Technologie de chiffrement**, choisissez **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.

5. 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 **Ajouter**.

   b. Dans la fenêtre qui s'ouvre, indiquez les valeurs pour **Nom**, **Ordinateur**, **Type de disque**, **Kaspersky Disk Encryption**.

   c. Cliquez sur **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 **OK**.

   Les disques durs sélectionnés sont repris dans le tableau **Ne pas chiffrer les disques durs suivants**.

6. 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)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.

4. Dans la liste déroulante **Technologie de chiffrement**, choisissez **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.

5. 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. Appuyez 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. Enregistrez le fichier.

Kaspersky Endpoint Security exporte la liste complète des exclusions dans un fichier XML.

6. Pour importer la liste des règles, procédez comme suit :

a. Appuyez 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. Ouvrez le fichier.

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.

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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Chiffrement des données** → **Chiffrement du disque**.

Sélectionnez la technologie **Kaspersky Disk Encryption**.

5. 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. Appuyez sur le bouton → **Exporter**.

Kaspersky Endpoint Security exporte la liste des exclusions dans un fichier JSON dans le dossier des téléchargements par défaut.

7. Pour importer la liste des exclusions, procédez comme suit :

a. Appuyez sur le bouton → **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer la liste des exclusions.

b. Ouvrez le fichier.

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 JSON.

8. Enregistrez vos modifications.

Activation de l'utilisation de la technologie d'authentification unique (SSO)

La technologie Single Sign-On (SSO) vous permet de vous connecter automatiquement au système d'exploitation à l'aide des informations d'identification de l'Agent d'authentification. Cela signifie qu'un utilisateur doit saisir un mot de passe une seule fois lorsqu'il se connecte à Windows (mot de passe du compte de l'Agent d'authentification). La technologie d'authentification unique vous permet également de mettre automatiquement à jour le mot de passe du compte de l'Agent d'authentification lorsque le mot de passe du compte Windows est modifié.

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.

Activation de l'utilisation de la technologie d'authentification unique

Procédure d'activation de l'utilisation de la technologie d'authentification unique dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres des mots de passe**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Agent d'authentification**, cochez la case **Utiliser la technologie d'authentification unique (SSO)**.
6. Si vous utilisez un fournisseur d'informations d'identification tiers, cochez la case **Emballer les fournisseurs de certification tiers**.
7. 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 **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données** → **Chiffrement du disque**.

5. Sélectionnez la technologie **Kaspersky Disk Encryption**.

6. Dans le groupe **Paramètres de mot de passe**, cochez la case **Utiliser la technologie d'authentification unique (SSO)**.

7. Si vous utilisez un fournisseur d'informations d'identification tiers, cochez la case **Emballer les fournisseurs de certification tiers**.

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.

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. Ces actions ne doivent être effectuées qu'une seule fois pour synchroniser les mots de passe. Ensuite, Kaspersky Endpoint Security remplace le mot de passe du compte de l'Agent d'authentification par le mot de passe du compte Windows. Lorsque le mot de passe du compte Windows est modifié, l'application met automatiquement à jour le mot de passe du compte de l'Agent d'authentification.

Fournisseurs d'informations d'identification tiers

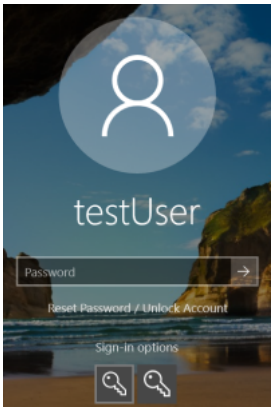
Kaspersky Endpoint Security prend en charge le fournisseur d'informations d'identification tiers ADSelfService Plus.

Dans le cadre du recours à des fournisseurs d'informations d'identification tiers, l'Agent d'authentification intercepte le mot de passe avant le chargement du système d'exploitation. Cela signifie qu'un utilisateur doit saisir un mot de passe une seule fois lorsqu'il se connecte à Windows. Après s'être connecté à Windows, l'utilisateur peut utiliser les fonctionnalités offertes par un fournisseur d'informations d'identification tiers pour s'authentifier auprès de services d'entreprise, par exemple. Les fournisseurs d'informations d'identification tiers permettent également aux utilisateurs de réinitialiser leur propre mot de passe de façon indépendante. Dans ce cas, Kaspersky Endpoint Security mettra automatiquement à jour le mot de passe de l'Agent d'authentification.

Si vous utilisez un fournisseur d'informations d'identification tiers qui n'est pas pris en charge par l'application, il se peut que vous rencontriez certaines limitations dans le fonctionnement de la technologie d'authentification unique. Lors de la connexion à Windows, deux profils seront disponibles pour l'utilisateur : fournisseur d'informations d'identification système et fournisseur d'informations d'identification tiers. Les icônes de ces profils seront identiques (cf. ill. ci-après). L'utilisateur aura le choix entre les options suivantes pour continuer :

- Si l'utilisateur sélectionne le *fournisseur d'informations d'identification tiers*, l'Agent d'authentification ne sera pas en mesure de synchroniser le mot de passe avec le compte Windows. Par conséquent, si l'utilisateur a modifié le mot de passe du compte Windows, Kaspersky Endpoint Security ne peut pas mettre à jour le mot de passe du compte de l'Agent d'authentification. Par conséquent, 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. Dans ce cas, l'utilisateur peut utiliser les fonctionnalités offertes par un fournisseur d'informations d'identification tiers pour s'authentifier auprès de services d'entreprise, par exemple.

- Si l'utilisateur sélectionne le *fournisseur d'informations d'identification système*, l'Agent d'authentification synchronisera les mots de passe avec le compte Windows. Dans ce cas, l'utilisateur ne peut pas utiliser les fonctionnalités offertes par un fournisseur tiers pour s'authentifier auprès de services d'entreprise, par exemple.



Profil d'authentification du système et profil d'authentification d'un tiers pour l'ouverture de session Windows

Administration des comptes 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 la 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 de l'Agent d'authentification via la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Administrer les comptes de l'Agent d'authentification**.

Étape 2. Sélection de la commande d'administration des comptes de l'Agent d'authentification

Composez la liste des commandes d'administration des comptes 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. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. 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.

Procédure de création de la tâche Administration des comptes de l'Agent d'authentification dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Kaspersky Endpoint Security for Windows 14.2**.

2. Dans la liste déroulante **Type de tâche**, choisissez **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 **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

Étape 2. Administration des comptes de l'Agent d'authentification

Composez la liste des commandes d'administration des comptes 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. 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).

Procédure d'ajout d'un compte utilisateur d'Agent d'authentification via la Console d'administration (MMC)

1. Ouvrez la tâche de groupe *Administrer les comptes 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 *Administrer les comptes 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 de l'Agent d'authentification. Cette étape n'est pas accessible si vous ajoutez une commande de création d'un compte utilisateur de l'Agent d'authentification dans les propriétés de la tâche locale *Administrer les comptes de l'Agent d'authentification*.

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. Dans le groupe **Accès à l'authentification dans l'Agent d'authentification**, configurez l'accès à l'authentification dans l'Agent d'authentification pour l'utilisateur qui utilise le compte indiqué 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter** et sélectionnez le type de commande **Ajouter un compte**.

5. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement. Passez à l'étape suivante.

   Kaspersky Endpoint Security détermine l'identificateur de sécurité du compte (Security Identifier, 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.

6. Configurez les paramètres du compte utilisateur de l'Agent d'authentification :

   - **Créer un compte d'Agent d'authentification pour remplacer le 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'authentification 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'authentification 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 au compte pour les 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.

7. Enregistrez vos modifications.

8. 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 *Gérer les comptes 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 *Administrer les comptes 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 *Administrer les comptes 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 de 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter** et sélectionnez le type de commande **Modifier le compte**.

5. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement. Passez à l'étape suivante.

   Kaspersky Endpoint Security détermine l'identificateur de sécurité du compte (Security Identifier, 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.

6. Cochez les cases en regard des paramètres que vous souhaitez modifier.

7. Configurez les paramètres du compte utilisateur de l'Agent d'authentification :

   - **Créer un compte d'Agent d'authentification pour remplacer le 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'authentification 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'authentification 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 au compte pour les 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**.

Pour supprimer un compte utilisateur d'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 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 *Administrer les comptes 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 *Administrer les comptes 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, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Gérer les comptes de l'Agent d'authentification** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la liste des comptes utilisateur de l'Agent d'authentification, cliquez sur le bouton **Ajouter** et sélectionnez le type de commande **Supprimer le compte**.

5. Sélectionnez un compte utilisateur. Vous pouvez sélectionner un compte utilisateur dans la liste des comptes de domaine ou saisir le nom du compte manuellement.

6. Enregistrez vos modifications.

7. 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 l'arborescence de la console, sélectionnez **Appareils**.

3. Ouvrez les propriétés de l'ordinateur d'un double clic.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Tâches**.

5. Dans la liste des tâches, sélectionnez **Administrer les comptes de l'Agent d'authentification** et ouvrez les propriétés de la tâche en double-cliquant.

6. 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.

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez afficher la liste des comptes utilisateur d'Agent d'authentification.

3. Dans les propriétés de l'ordinateur, sélectionnez l'onglet **Tâches**.

4. Dans la liste des tâches, sélectionnez **Gérer les comptes de l'Agent d'authentification**.

5. Dans les propriétés des tâches, 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 À 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 *Administrer 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 ;
- 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

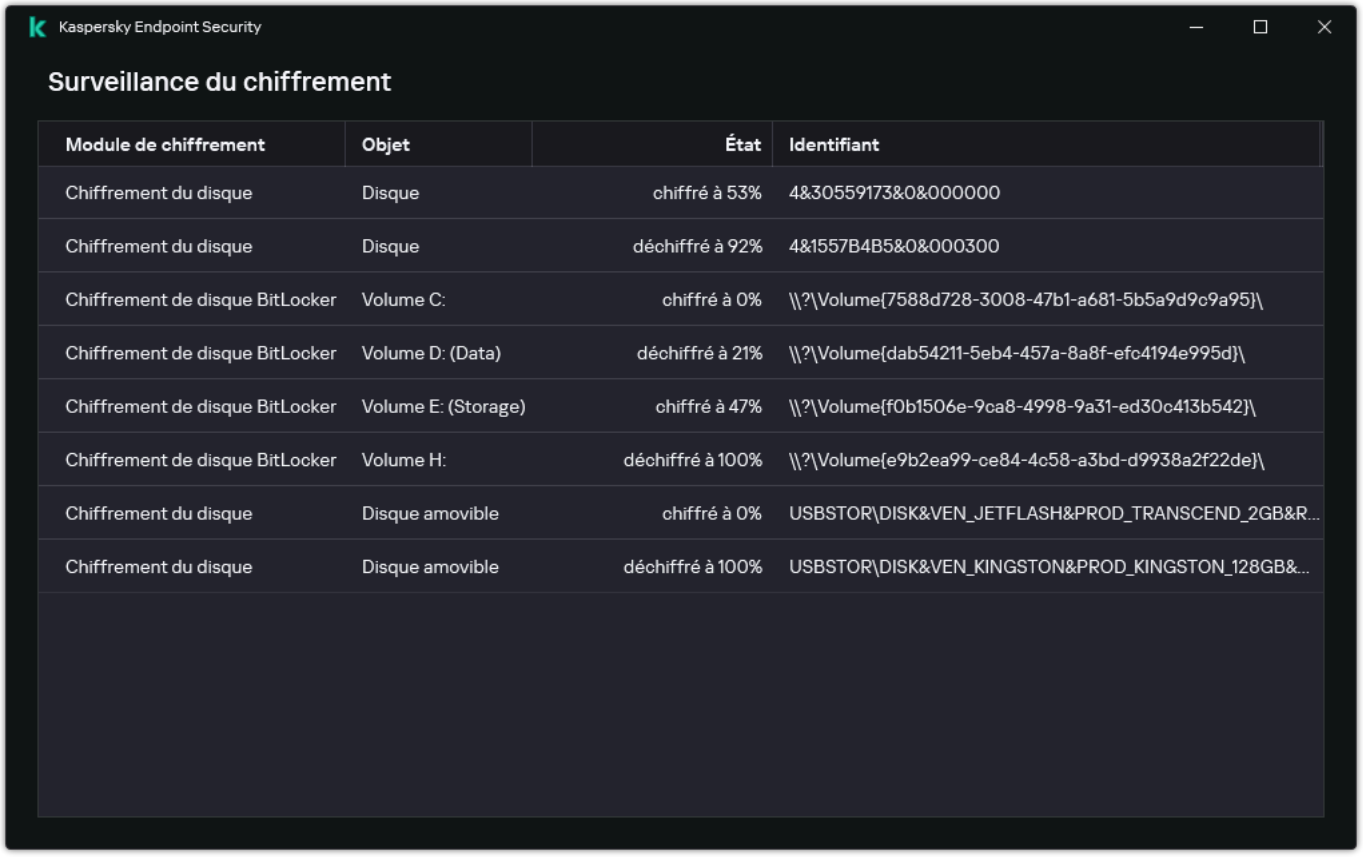
Vous pouvez déchiffrer les disques durs même en l'absence d'une licence valide qui autorise le chiffrement des données.

Pour déchiffrer des disques durs, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
4. Dans la liste déroulante **Technologie de chiffrement** choisissez la technologie à l'aide de laquelle les disques durs ont été chiffrés.
5. 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.
6. 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.



Module de chiffrement	Objet	État	Identifiant
Chiffrement du disque	Disque	chiffré à 53%	4&30559173&0&000000
Chiffrement du disque	Disque	déchiffré à 92%	4&1557B4B5&0&000300
Chiffrement de disque BitLocker	Volume C:	chiffré à 0%	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Chiffrement de disque BitLocker	Volume D: (Data)	déchiffré à 21%	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Chiffrement de disque BitLocker	Volume E: (Storage)	chiffré à 47%	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Chiffrement de disque BitLocker	Volume H:	déchiffré à 100%	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Chiffrement du disque	Disque amovible	chiffré à 0%	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Chiffrement du disque	Disque amovible	déchiffré à 100%	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Surveillance du chiffrement

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). Vous pouvez également utiliser le compte de service pour accéder au disque dur si cette fonction est activée dans les paramètres de chiffrement du disque.

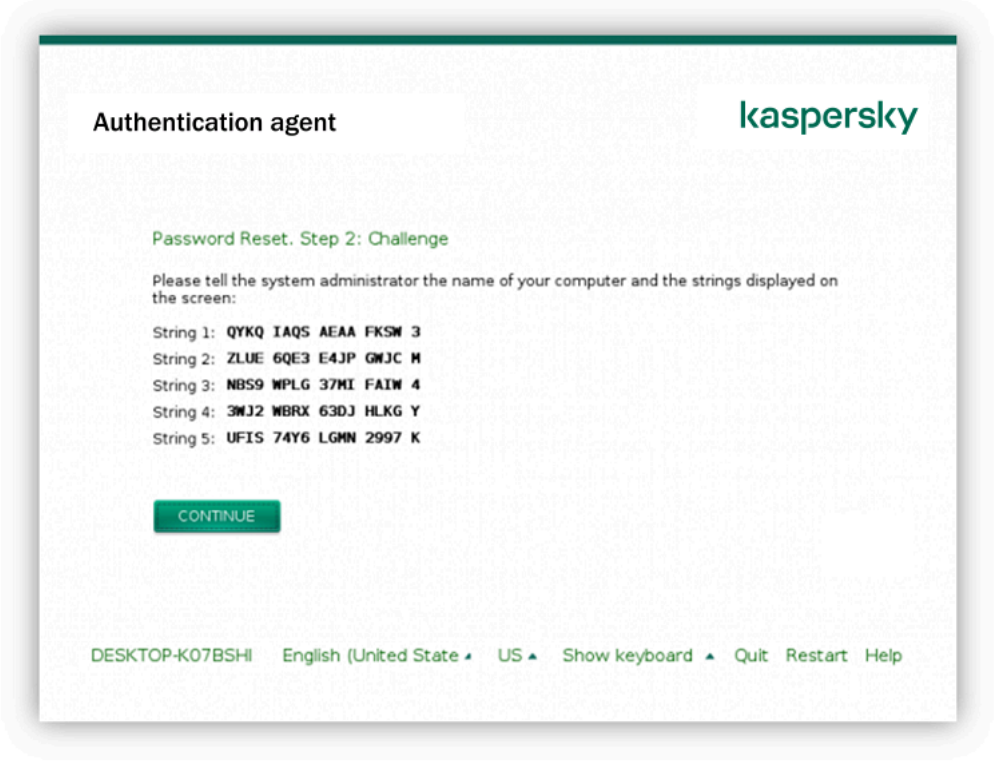
Restauration de l'accès au disque dur système

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 l'arborescence de la console, sélectionnez **Appareils**.

3. 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.

4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.

5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Agent d'authentification**.

6. Dans le groupe **Algorithme de chiffrement utilisé**, sélectionnez l'algorithme de chiffrement : **AES56** ou **AES256**.

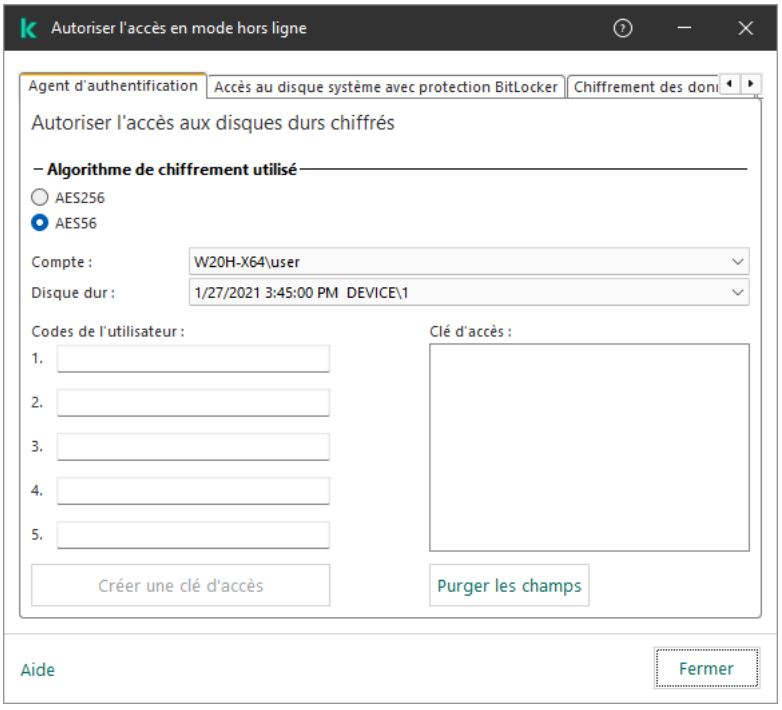
   L'algorithme de chiffrement des données dépend de la bibliothèque de chiffrement AES incluse dans la distribution : *Strong encryption (AES256)* ou *Lite encryption (AES56)*. La bibliothèque de chiffrement AES est installée en même temps que l'application.

7. Dans la liste déroulante **Compte**, sélectionnez le nom du compte d'Agent d'authentification de l'utilisateur qui a demandé la restauration de l'accès au disque.

8. Dans la liste déroulante **Disque dur**, choisissez le disque dur chiffré auquel il faut rétablir l'accès.

9. 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.



Accorder l'accès en mode hors ligne

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, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.

3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.

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 :

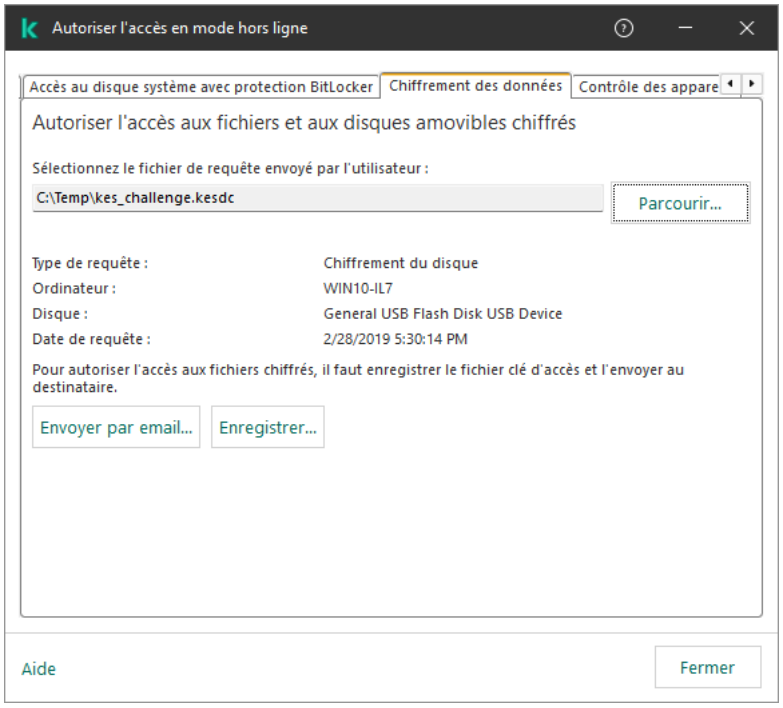
1. L'utilisateur envoie une requête d'accès au fichier à l'administrateur.
2. L'administrateur ajoute la requête d'accès au fichier à Kaspersky Security Center, crée le fichier de clé d'accès et l'envoie à l'utilisateur.
3. L'utilisateur ajoute le fichier de clé d'accès à Kaspersky Endpoint Security 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 l'arborescence de la console, sélectionnez **Appareils**.
3. 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.
4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Chiffrement des données**.
6. Sous l'onglet **Chiffrement des données**, cliquez sur le bouton **Parcourir**.
7. 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.



Accorder l'accès en mode hors ligne

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, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.
3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.
4. Choisissez le **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.

Connexion avec le compte de service de l'Agent d'authentification

Kaspersky Endpoint Security vous permet d'ajouter un compte de service d'Agent d'authentification lors du chiffrement d'un disque. Le compte de service est nécessaire pour accéder à l'ordinateur, par exemple lorsque l'utilisateur a oublié son mot de passe. Vous pouvez également utiliser le compte de service comme un compte de réserve. Pour ajouter un compte, sélectionnez un compte de service dans les paramètres de chiffrement du disque et saisissez le nom du compte utilisateur (par défaut, `ServiceAccount`). Pour vous authentifier à l'aide de l'agent, vous aurez besoin d'un mot de passe à usage unique.

Comment trouver le mot de passe à usage unique dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Tâches**.
5. Dans la liste des tâches, sélectionnez **Administrer les comptes de l'Agent d'authentification** et ouvrez les propriétés de la tâche en double-cliquant.
6. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Paramètres**.
7. Dans la liste des comptes, sélectionnez le compte de service de l'Agent d'authentification (par exemple, `WIN10-USER\ServiceAccount`).
8. Dans la liste déroulante **Action**, choisissez **Consulter le compte**.
9. Dans les propriétés du compte, cochez la case **Afficher le mot de passe d'origine**.
10. Copiez le mot de passe à usage unique pour vous connecter avec le compte de service.

Comment trouver le mot de passe à usage unique dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
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 les propriétés de l'ordinateur, sélectionnez l'onglet **Tâches**.
4. Dans la liste des tâches, sélectionnez **Gérer les comptes de l'Agent d'authentification**.
5. Dans les propriétés des tâches, sélectionnez l'onglet **Paramètres de l'application**.
6. Dans la liste des comptes, sélectionnez le compte de service de l'Agent d'authentification (par exemple, `WIN10-USER\ServiceAccount`).

7. Dans les propriétés du compte, cochez la case **Afficher le mot de passe**.

8. Copiez le mot de passe à usage unique pour vous connecter avec le compte de service.

Kaspersky Endpoint Security met automatiquement à jour le mot de passe chaque fois qu'un utilisateur s'authentifie avec le compte de service. Après vous être authentifié à l'aide de l'agent, vous devez saisir le mot de passe du compte Windows. Lorsque vous vous connectez avec le compte de service, vous ne pouvez pas utiliser la technologie d'authentification unique.

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.

Caractéristiques de la mise à jour du système d'exploitation :

- **Mise à jour du système d'exploitation via WSUS**. Vous pouvez mettre à jour le système d'exploitation normalement.

- **Mise à jour du système d'exploitation à partir d'une image ISO**. Pour mettre à jour le système d'exploitation, vous devez indiquer le dossier avec les pilotes de chiffrement de disque Kaspersky . L'application copie automatiquement les pilotes dans un dossier distinct. Procédez comme suit :

  1. Montez l'image ISO.

  2. Démarrez l'installation de la mise à jour du système à l'aide de la clé suivante :

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

> La mise à jour automatique du système d'exploitation est disponible uniquement si l'ordinateur exécute Windows 10 1607 (RS1) ou une version ultérieure. Pour mettre à jour des versions antérieures du système d'exploitation, il est recommandé de déchiffrer le disque, d'effectuer une mise à jour du système d'exploitation, puis de chiffrer le disque.

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 14.2, la fonctionnalité Chiffrement du disque est mise à jour.

Les erreurs suivantes peuvent surgir 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 sont 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.

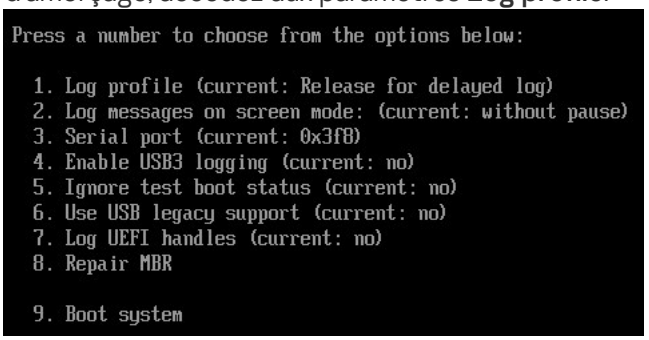
Traçage de l'Agent d'authentification

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 activer le traçage de l'Agent d'authentification, procédez comme suit :

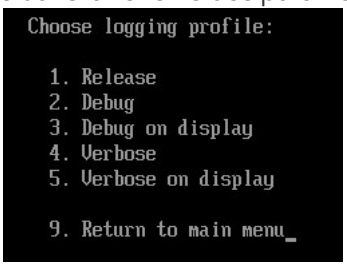
1. Activez le traçage de Kaspersky Endpoint Security.
2. Redémarrez l'ordinateur.
3. Directement après le démarrage de l'ordinateur doté de disques durs chiffrés, appuyez sur la touche **F3** afin d'ouvrir la fenêtre de configuration de l'Agent d'authentification.
4. Après le lancement du programme d'amorçage FDE, sélectionnez le gestionnaire d'amorçage **KES (FDE <version>)**.

5. Dans le menu du gestionnaire d'amorçage, accédez aux paramètres **Log profile**.



Menu du gestionnaire d'amorçage

6. Sélectionnez le niveau de traçage souhaité dans la fenêtre des paramètres du profil du journal :



Niveaux de traçage de l'Agent d'authentification

- **Release**. 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.

- **Debug**. 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.

- **Debug on display**. 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.

- **Verbose**. 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 détails des entrées dans ce cas est plus élevé qu'au niveau **Debug**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

- **Verbose on display**. 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 **Debug on display**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

Une fois que vous avez sélectionné un niveau de traçage, le gestionnaire de démarrage affiche à nouveau le menu.

7. Dans le menu du gestionnaire de démarrage, sélectionnez **Boot system**.

   Le programme d'amorçage FDE lance l'Agent d'authentification.

   Reproduisez le problème.

   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.

8. Pour arrêter le processus de traçage, retournez à la fenêtre Outils de support et désactivez le traçage.

En conséquence, les fichiers de traçage des opérations de l'Agent d'authentification KES.SRV sont créés dans le dossier `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.

4. Cliquez sur le bouton **Aide** dans le groupe **Modèles**.

5. Dans la fenêtre qui s'ouvre, 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 **Modification 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 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.

6. 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.

7. 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 objets et données restants au terme du fonctionnement test de l'Agent d'authentification 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, sélectionnez l'appareil requis.
3. Cliquez sur **Analyser**.
4. Si, après le diagnostic du disque dur système, vous recevez un message indiquant que des objets et des données subsistent après le fonctionnement en mode test de l'Agent d'authentification, cliquez sur **Supprimer les objets et les données AA**.

   Le bouton **Supprimer les objets et les données AA** est disponible uniquement si des objets et des données subsistant après le fonctionnement en mode test de l'Agent d'authentification sont détectés.

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 l'infrastructure Kaspersky Next. BitLocker chiffre le volume logique. BitLocker ne permet de pas de chiffrer les disques amovibles. Pour en savoir plus sur le fonctionnement de BitLocker, consultez la documentation de Microsoft.

Lors du chiffrement du disque, BitLocker place le programme de démarrage et les autres fichiers auxiliaires dans la system partition. Cette partition n'est pas chiffrée. Lors de l'installation de Windows, le système d'exploitation crée la partition système automatiquement. Si le disque est entièrement partitionné avant l'installation de Windows, le système d'exploitation ne peut pas créer de partition système. Dans ce cas, lorsque vous démarrez le chiffrement de disque BitLocker, le système d'exploitation vous invite à repartitionner le disque et à créer une partition système. Une fois que vous aurez créé une partition système, le système d'exploitation lancera le chiffrement BitLocker.

L'algorithme de chiffrement BitLocker ne dépend pas de la bibliothèque AES incluse dans le paquet de distribution (AES256 ou AES56). Le chiffrement utilise la bibliothèque de chiffrement intégrée au système d'exploitation.

Par défaut, l'application utilise l'algorithme de chiffrement BitLocker avec une longueur de clé effective de 256 bits pour chiffrer les appareils qui n'ont jamais été chiffrés. Pour un appareil qui était chiffré avant l'installation de l'application, l'algorithme de chiffrement peut être différent. Pour en savoir plus sur le choix de l'algorithme de chiffrement, consultez le site de l'assistance technique de Microsoft. À partir de la version 12.9, Kaspersky Endpoint Security envoie à Kaspersky Security Center la clé de récupération d'origine des appareils précédemment chiffrés par des applications tierces.

BitLocker fournit un stockage sécurisé des clés d'accès à l'aide d'un module de plateforme sécurisée. *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 dur du système, l'utilisateur doit passer par l'authentification BitLocker pour lancer le système d'exploitation. Après l'authentification, BitLocker autorise l'utilisateur à se connecter. BitLocker n'est pas compatible avec la technologie d'authentification unique (SSO).

Après avoir chiffré le disque, BitLocker crée une clé de récupération. Kaspersky Endpoint Security envoie la clé de réserve 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 la clé de récupération et les informations sur le chiffrement du disque à Kaspersky Security Center.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.
4. Dans la liste déroulante **Technologie de chiffrement**, choisissez **Chiffrement de disque BitLocker**.
5. Dans la liste déroulante **Mode de chiffrement**, choisissez **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.

6. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).
7. Enregistrez vos modifications.

Lancement du chiffrement de disque BitLocker via la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

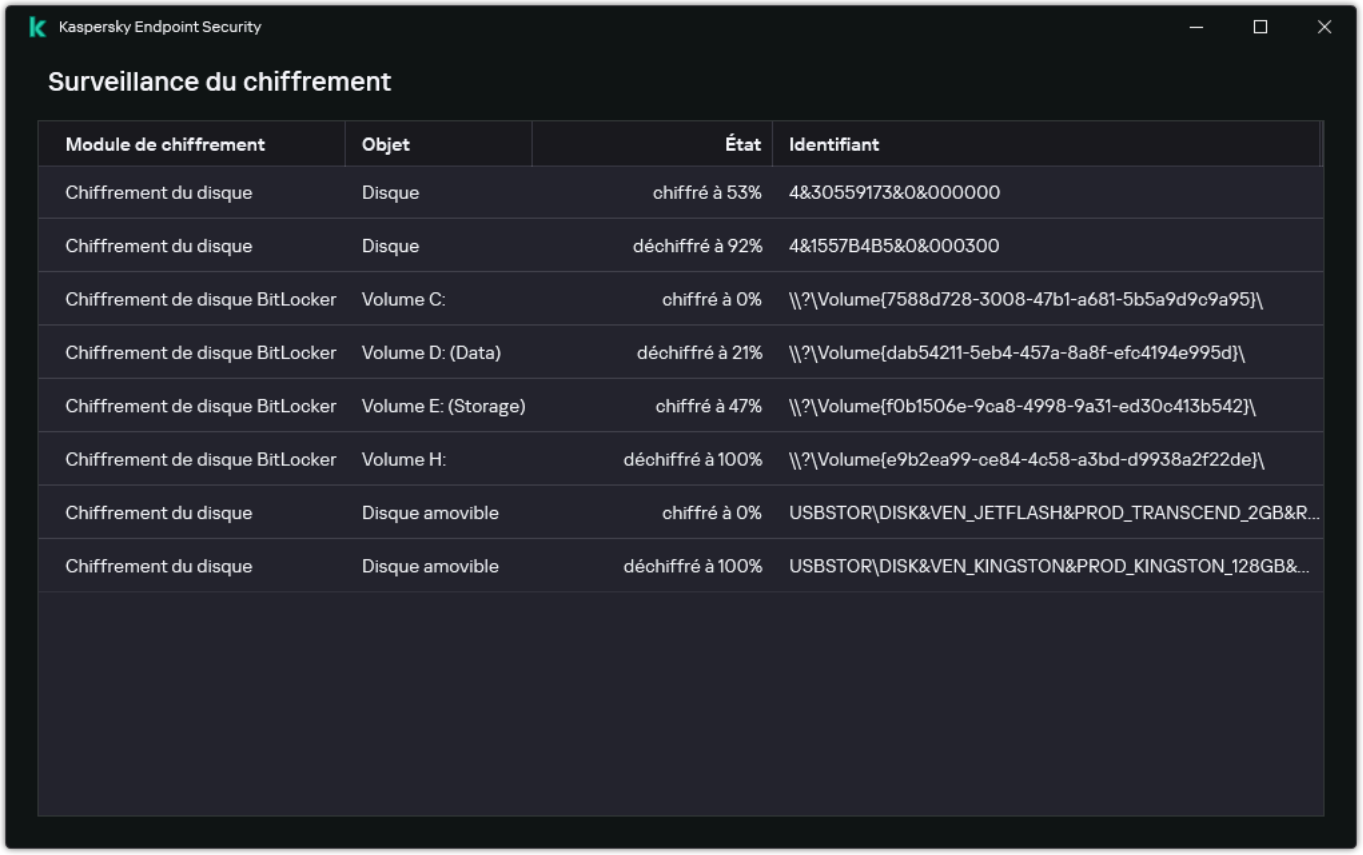
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données** → **Chiffrement du disque**.
5. Sélectionnez la technologie **Chiffrement de disque BitLocker**.
6. Dans le groupe **Action sur les appareils**, 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.

7. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).

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.



Surveillance du chiffrement

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
Autoriser l'utilisation de l'authentification BitLocker qui requiert une saisie au clavier avant le démarrage sur les tablettes	L'utilisation d'une 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). 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. 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. Si cette case est décochée, le chiffrement de disque BitLocker n'est pas possible sur les tablettes.
Utiliser le chiffrement au niveau matériel (Windows 8 et versions ultérieures)	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.
Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures)	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. 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. Par défaut, la case est décochée.

Paramètre	Description
Méthode d'authentification	**Mot de passe uniquement (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. **Trusted Platform Module (TPM)** Si vous avez choisi cette option, BitLocker utilise le Trusted Platform Module (TPM). *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 un 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. • **Trusted Platform Module (TPM) ou mot de passe si le TPM n'est pas disponible**. Si cette option est sélectionnée, 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. La méthode d'authentification sélectionnée doit être configurée en précisant les exigences en matière de mot de passe ou de code PIN : • **Longueur minimale du code PIN (caractères)** (la valeur par défaut est 6). • **Longueur minimale du mot de passe (caractères)** (la valeur par défaut est 8). • **Nombre maximal de mots de passe/codes PIN enregistrés** (la valeur par défaut est 5). • **Limiter la durée de validité du mot de passe/code PIN pour le TPM (jours)** (désactivé par défaut). • **Utiliser un code PIN amélioré (lettres et chiffres)**. Le *code PIN renforcé* permet l'utilisation d'autres caractères en plus des caractères numériques : lettres latines majuscules et minuscules, caractères spéciaux et espaces. Désactivé par défaut.
Recréer automatiquement la clé de récupération (jours)	Mettez automatiquement à jour le mot de passe pour restaurer l'accès à un disque protégé par BitLocker. Si la case est cochée, précisez la période de validité du mot de passe de la clé de récupération. Cette mesure permet d'éviter la réutilisation du mot de passe de la clé de récupération.

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement du disque**.

4. Dans la liste déroulante **Technologie de chiffrement**, choisissez **Chiffrement de disque BitLocker**.

5. Dans la liste déroulante **Mode de chiffrement**, choisissez **Déchiffrer tous les disques durs**.

6. 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, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

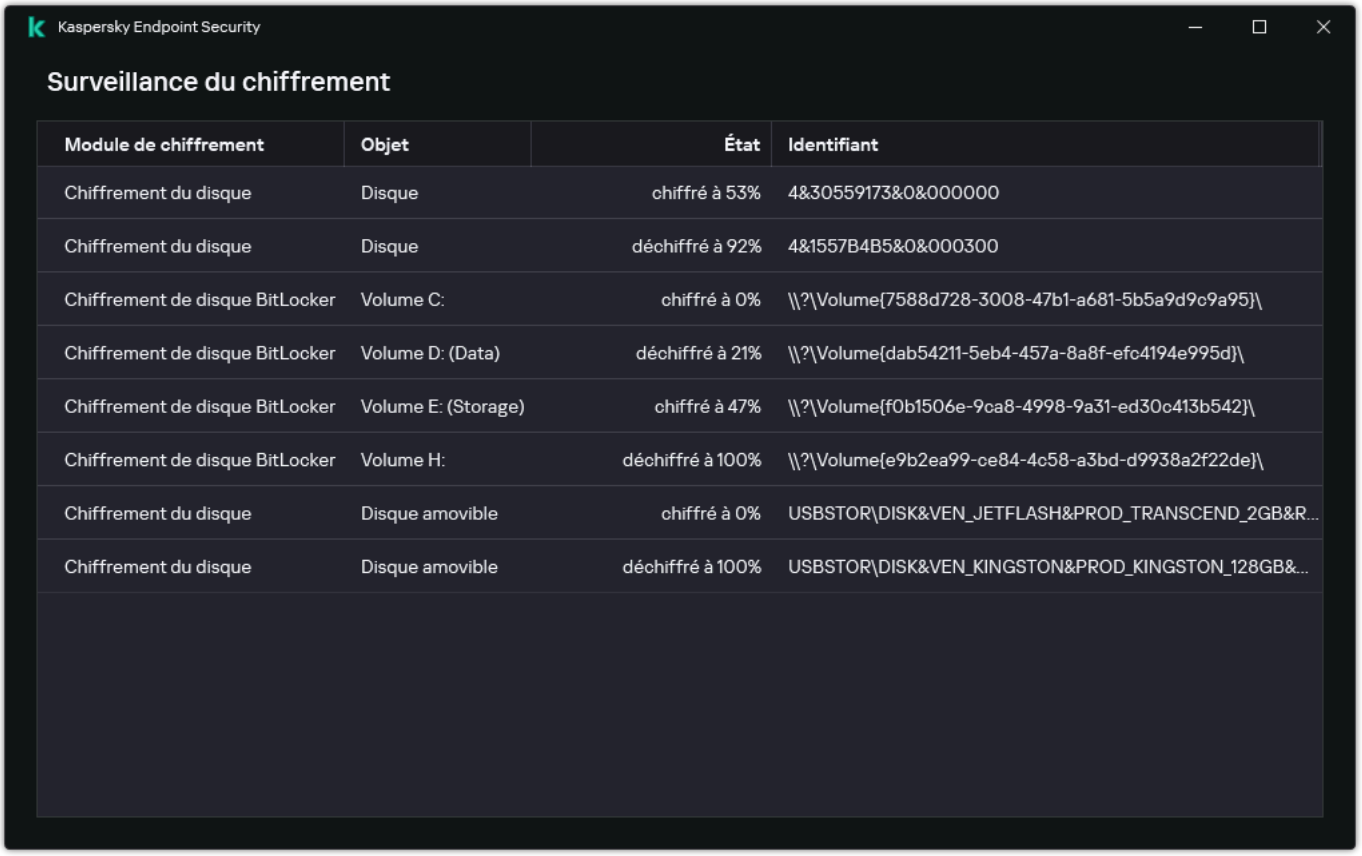
4. Passez à la section **Chiffrement des données** → **Chiffrement du disque**.

5. Sélectionnez la technologie **Chiffrement de disque BitLocker**.

6. Dans le groupe **Action sur les appareils**, sélectionnez l'option **Déchiffrer tous les disques durs**.

7. 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.



Module de chiffrement	Objet	État	Identifiant
Chiffrement du disque	Disque	chiffré à 53%	4&30559173&0&000000
Chiffrement du disque	Disque	déchiffré à 92%	4&1557B4B5&0&000300
Chiffrement de disque BitLocker	Volume C:	chiffré à 0%	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Chiffrement de disque BitLocker	Volume D: (Data)	déchiffré à 21%	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Chiffrement de disque BitLocker	Volume E: (Storage)	chiffré à 47%	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Chiffrement de disque BitLocker	Volume H:	déchiffré à 100%	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Chiffrement du disque	Disque amovible	chiffré à 0%	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Chiffrement du disque	Disque amovible	déchiffré à 100%	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Surveillance du chiffrement

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.

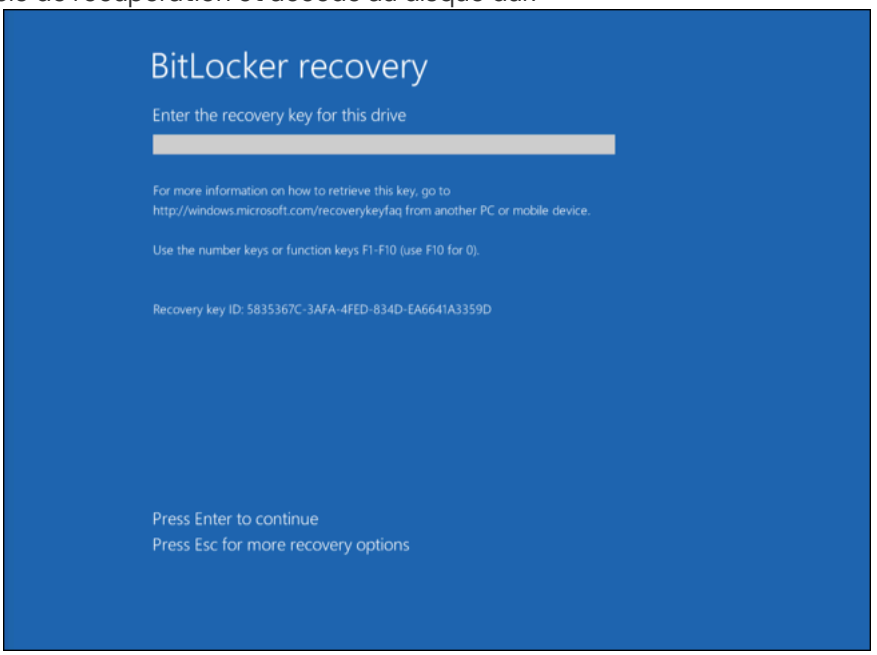
   Le fichier de clé de récupération est utilisé pour les ordinateurs qui tournent sous les systèmes d'exploitation suivants :

   - 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.

   Pour éviter la réutilisation du mot passe de la clé de récupération, vous pouvez configurer la mise à jour automatique du mot de passe dans les paramètres de la stratégie.

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

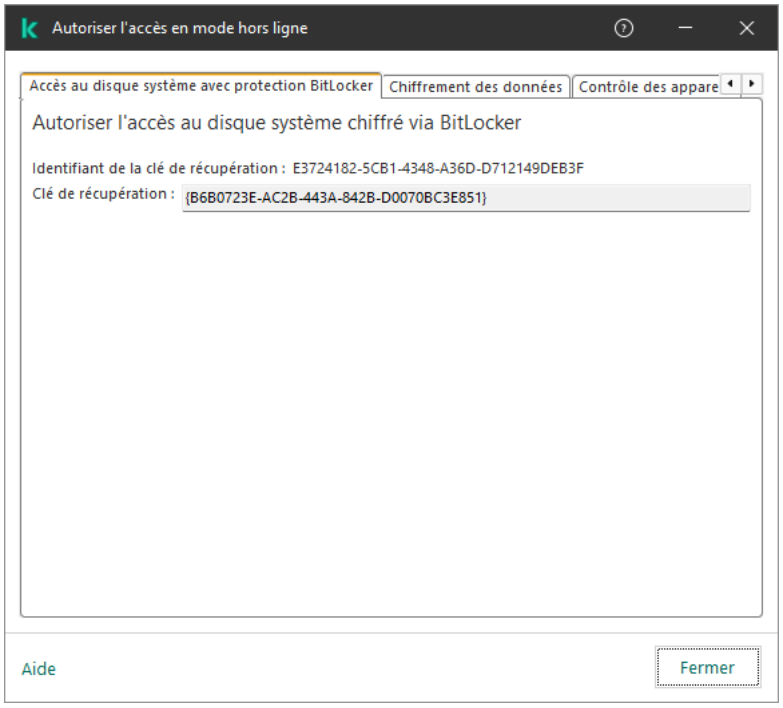
Pour lancer la procédure de récupération, l'utilisateur doit appuyer sur la touche **Échap** lors de l'identification avant le chargement.

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 l'arborescence de la console, sélectionnez **Appareils administrés**.
3. 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.
4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Accès au disque système avec protection BitLocker**.
6. 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.



Restauration de l'accès au disque chiffré à l'aide de BitLocker

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, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.
3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.
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. Cliquez sur **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 de réserve 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

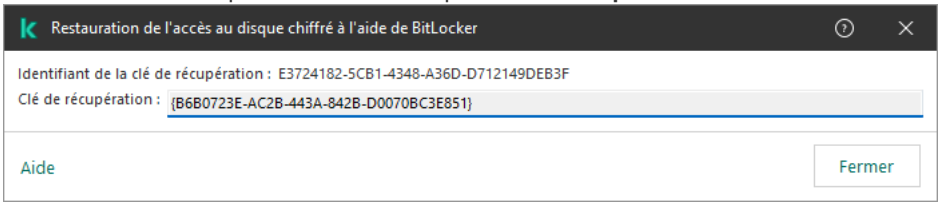
Pour lancer la procédure de récupération, l'utilisateur doit cliquer sur le lien **Forgot your password** dans la fenêtre d'accès au disque. Une fois que l'utilisateur a obtenu l'accès au lecteur chiffré, il peut activer le déverrouillage automatique du disque lors de l'authentification Windows dans 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 d'administration, sélectionnez le dossier **Avancé** → **Chiffrement et protection des données** → **Disques chiffrés**.
3. Dans l'espace de travail, sélectionnez l'appareil chiffré pour lequel vous souhaitez créer un fichier de clé d'accès, puis dans le menu contextuel de l'appareil, cliquez sur **Obtenir l'accès à l'appareil dans Kaspersky Endpoint Security**.
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**.



Restauration de l'accès au disque chiffré à l'aide de BitLocker

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** → **Disques chiffrés**.

2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.

3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.

   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. Cliquez sur **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.

Interruption de la protection BitLocker pour mettre à jour un logiciel

Il existe un certain nombre de considérations particulières concernant la mise à jour du système d'exploitation, l'installation de paquets de mise à jour pour le système d'exploitation ou la mise à jour d'autres logiciels lorsque la protection BitLocker est activée. L'installation des mises à jour peut exiger le redémarrage de l'ordinateur à plusieurs reprises. Après chaque redémarrage, l'utilisateur doit procéder à l'authentification BitLocker. Pour vous assurer que les mises à jour s'installent correctement, vous pouvez désactiver temporairement l'authentification BitLocker. Dans ce cas, le disque reste chiffré et l'utilisateur a accès aux données après s'être connecté au système. Pour gérer l'authentification BitLocker, vous pouvez utiliser la tâche *Gestion de la protection BitLocker*. Vous pouvez utiliser cette tâche pour préciser le nombre de redémarrages de l'ordinateur qui ne nécessitent pas d'authentification BitLocker. De cette façon, une fois que les mises à jour sont installées et que la tâche *Gestion de la protection BitLocker* est terminée, l'authentification BitLocker est automatiquement activée. Vous pouvez activer l'authentification BitLocker à tout moment.

Interruption de la protection BitLocker à l'aide de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 (14.2)** → **Gestion de la protection BitLocker**.

Étape 2. Gestion de la protection BitLocker

Configurez l'authentification BitLocker. Pour interrompre la protection BitLocker, sélectionnez **Autoriser temporairement le contournement de l'authentification BitLocker** et saisissez le nombre de redémarrages sans authentification BitLocker (1 à 15 fois). Si nécessaire, saisissez une date et une heure d'expiration pour la tâche. À l'heure indiquée, la tâche est automatiquement désactivée, et l'utilisateur doit terminer l'authentification BitLocker lorsque l'ordinateur est redémarré.

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 le nom de la tâche, par exemple *Mise à jour vers Windows 10*.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Interruption de la protection BitLocker à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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**.
2. Dans la liste déroulante **Type de tâche**, choisissez **Gestion de la protection BitLocker**.
3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Mise à jour vers Windows 10*.
4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

Étape 2. Gestion de la protection BitLocker

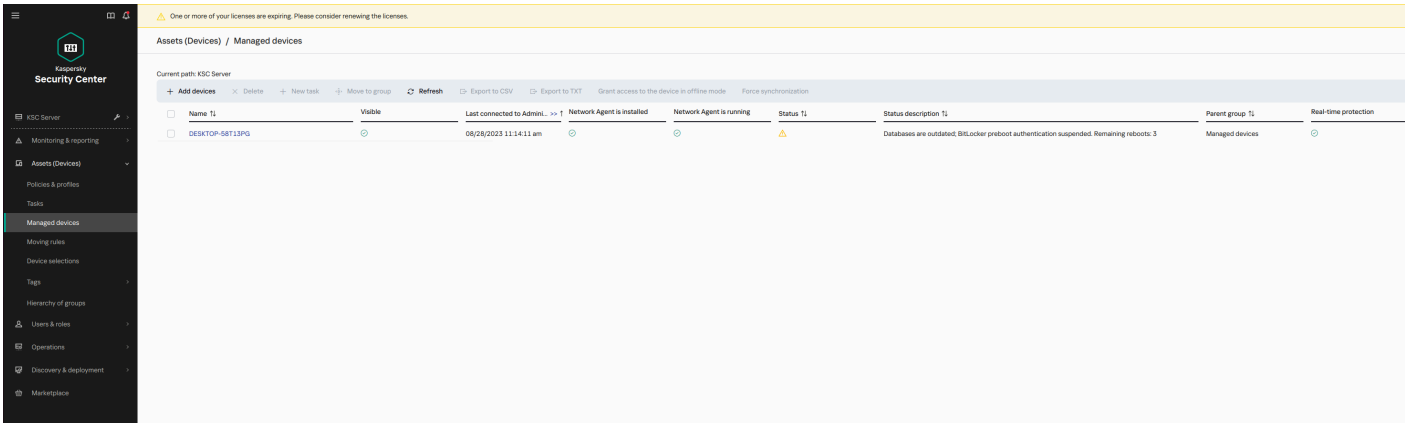
Configurez l'authentification BitLocker. Pour interrompre la protection BitLocker, sélectionnez **Autoriser temporairement le contournement de l'authentification BitLocker** et saisissez le nombre de redémarrages sans authentification BitLocker (1 à 15 fois). Si nécessaire, saisissez une date et une heure d'expiration pour la tâche. À l'heure indiquée, la tâche est automatiquement désactivée, et l'utilisateur doit terminer l'authentification BitLocker lorsque l'ordinateur est redémarré.

Étape 3. Fin de la création de la tâche

Quittez l'Assistant. 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**.

Ainsi, lorsque la tâche est en cours d'exécution, après le prochain redémarrage de l'ordinateur, BitLocker ne demande pas à l'utilisateur de s'authentifier. Après chaque redémarrage de l'ordinateur sans authentification BitLocker, Kaspersky Endpoint Security génère un événement correspondant et enregistre le nombre de redémarrages restants. Kaspersky Endpoint Security envoie ensuite l'événement à Kaspersky Security Center pour être surveillé par l'administrateur. Vous pouvez également afficher le nombre de redémarrages restants dans le dossier **Appareils administrés** de la console Kaspersky Security Center dans la description de l'état de l'appareil.



La liste des appareils administrés

Lorsque le nombre de redémarrages indiqué ou le délai d'expiration de la tâche est atteint, l'authentification BitLocker est automatiquement activée. Pour accéder aux données, l'utilisateur doit procéder à une authentification BitLocker.

Sur les ordinateurs fonctionnant sous Windows 7, BitLocker ne peut pas compter les redémarrages de l'ordinateur. Le comptage des redémarrages sur les ordinateurs Windows 7 est géré par Kaspersky Endpoint Security. Ainsi, pour activer automatiquement l'authentification BitLocker après chaque redémarrage, Kaspersky Endpoint Security doit être démarré.

Pour activer l'authentification BitLocker à l'avance, ouvrez les propriétés de la tâche *Gestion de la protection BitLocker* et sélectionnez **Demander une authentification à chaque fois en pré-lancement**.

Chiffrement des fichiers sur les disques locaux de l'ordinateur

Le chiffrement des fichiers n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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 qui se trouvent dans le stockage cloud OneDrive ou dans d'autres dossiers dont le nom est OneDrive. Kaspersky Endpoint Security bloque également la copie des fichiers chiffrés vers les dossiers OneDrive si ces fichiers ne sont pas ajoutés à la règle de déchiffrement.

Pour chiffrer des fichiers sur les disques locaux de l'ordinateur, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
4. Dans la liste déroulante **Mode de chiffrement**, choisissez **Selon les règles**.
5. 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.

     Il n'est pas recommandé de chiffrer les fichiers temporaires, car cela peut entraîner une perte de données. Par exemple, Microsoft Word crée des fichiers temporaires lors du traitement d'un document. Si les fichiers temporaires sont chiffrés, mais que le fichier d'origine ne l'est pas, l'utilisateur peut recevoir une erreur *Accès refusé* lors de la tentative d'enregistrement du document. De plus, Microsoft Word peut enregistrer le fichier, mais il ne sera pas possible d'ouvrir le document la prochaine fois, c'est-à-dire que les données seront perdues.

   - **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 personnalisé** 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.
- 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.

6. 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

Par défaut, toutes les applications fonctionnent avec des fichiers chiffrés à l'état déchiffré. Si vous utilisez souvent certaines applications (les navigateurs ou les éditeurs de texte par exemple), vous pouvez créer des règles d'accès aux fichiers chiffrés pour protéger les informations.

Nous vous recommandons de créer une règle d'accès aux fichiers chiffrés pour les navigateurs Microsoft Internet Explorer et Microsoft Edge. En raison du fonctionnement de ces navigateurs, si vous chargez un fichier chiffré sur un site Internet (sur un stockage dans le cloud, par exemple), le fichier est déchiffré automatiquement. Cette situation peut entraîner une fuite de données. Il n'est pas possible de charger un fichier chiffré en utilisant ces navigateurs. Nous vous recommandons de configurer la règle **Autoriser l'accès aux fichiers chiffrés uniquement sous la forme de texte chiffré**. Il n'est pas nécessaire de créer une règle pour les autres navigateurs (comme Google Chrome).

Pour composer des règles d'accès des applications aux fichiers chiffrés, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
4. Dans la liste déroulante **Mode de chiffrement**, choisissez **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.

5. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.
6. 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 **Actualiser**.

   c. Le tableau reprend les applications qui répondent aux filtres définis.

   d. Dans la colonne **Application**, 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.

Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

7. 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.

   Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

8. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.

4. Dans la liste déroulante **Mode de chiffrement**, choisissez **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.

5. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.

6. 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 **Actualiser**.

      Le tableau reprend les applications qui répondent aux filtres définis.

   c. Dans la colonne **Application**, 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 **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.

   Les informations sur la règle de chiffrement des fichiers créés ou modifiés par les applications choisies s'affichent dans le tableau de l'onglet **Règles pour les applications**.

7. 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 **Chiffrer tous les fichiers créés**.

   Les informations sur la règle de chiffrement des fichiers créés ou modifiés par les applications choisies s'affichent dans le tableau de l'onglet **Règles pour les applications**.

8. Enregistrez vos modifications.

Composition de la règle de déchiffrement

Pour composer la règle de déchiffrement, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
4. Dans la liste déroulante **Mode de chiffrement**, choisissez **Selon les règles**.
5. 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 personnalisé** 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.
6. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des fichiers**.
4. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Chiffrement**.

5. 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**.

   Les fichiers et dossiers supprimés de la liste de chiffrement sont ajoutés automatiquement à la liste de déchiffrement.

6. Composez la liste des fichiers à déchiffrer.

7. 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres des mots de passe**.

5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Archives chiffrées**.

6. 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 **Gestion des ressources** → **Stratégies**.

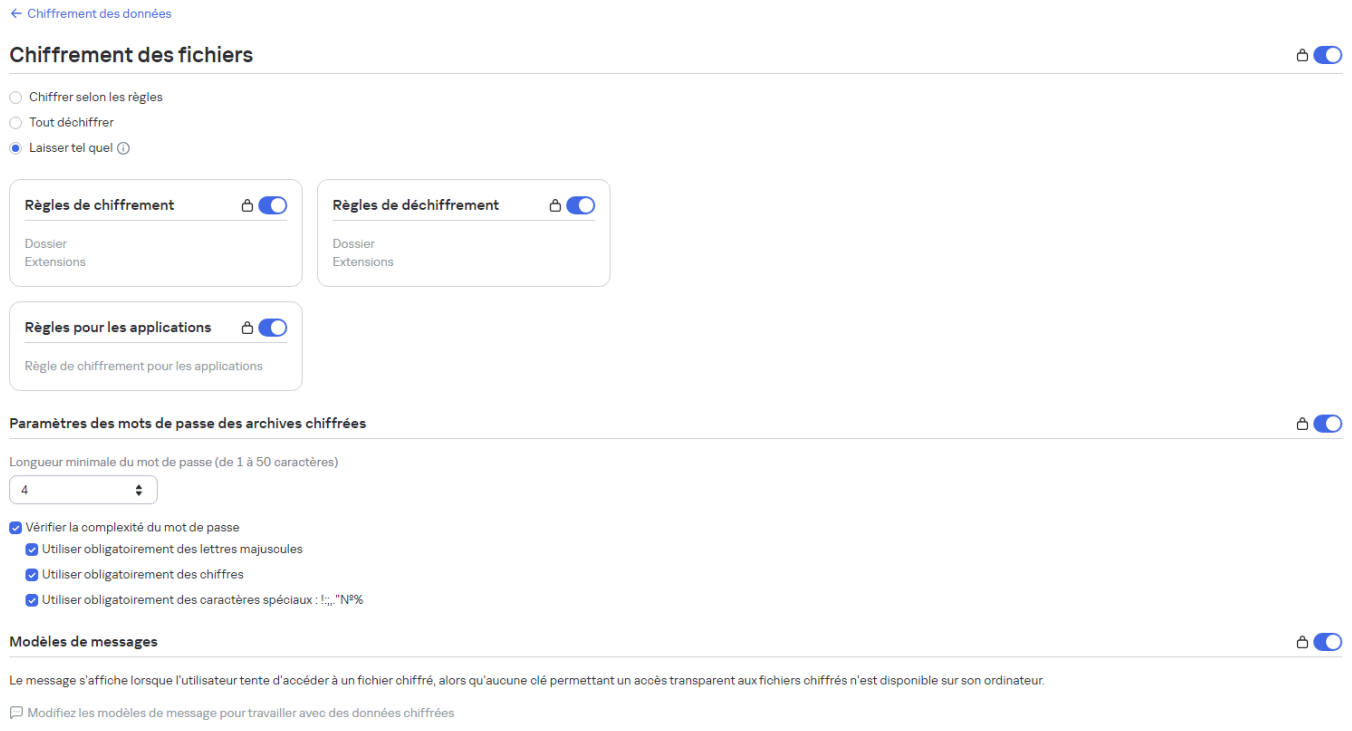
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Chiffrement des données** → **Chiffrement des fichiers**.

5. Dans le groupe **Paramètres des mots de passe des archives chiffrées**, configurez les critères du niveau de sécurité du mot de passe exigés lors de la création de paquets chiffrés.



Paramètres de chiffrement des fichiers

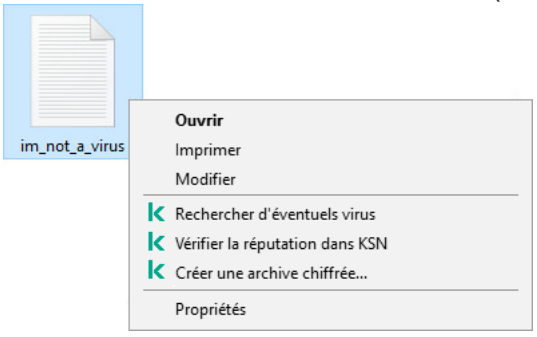
Vous pouvez créer des archives chiffrées sur des ordinateurs dotés de Kaspersky Endpoint Security avec la fonction de chiffrement de fichiers.

> 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 chiffrées. Cliquez-droit pour ouvrir leur menu contextuel.

2. Sélectionnez l'option **Créer une archive chiffrée** dans le menu contextuel (cf. ill. ci-dessous).



Création d'une archive chiffrée

3. 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.

4. Cliquez sur **Créer**.

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) - .

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 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 :

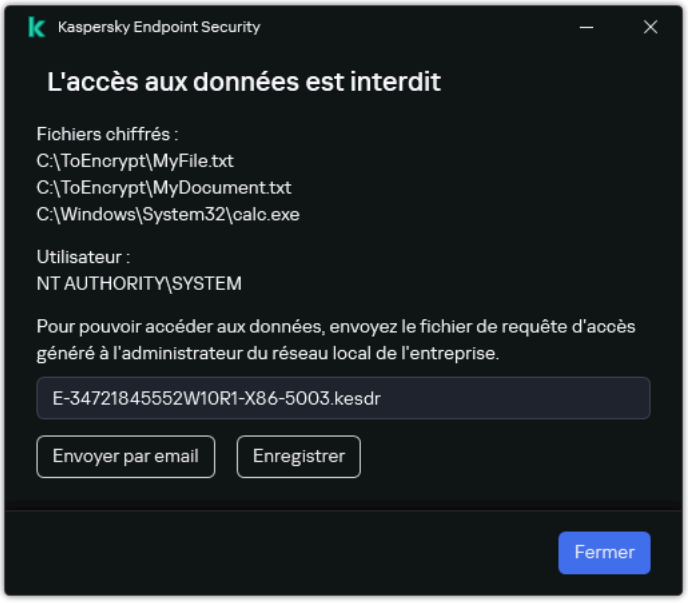
  - Les fichiers se trouvent dans des archives chiffrées créées sur l'ordinateur à l'aide de l'application Kaspersky Endpoint Security installée.
  - Les fichiers se trouvent sur des disques amovibles pour lesquels le fonctionnement en mode portable est autorisé.

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

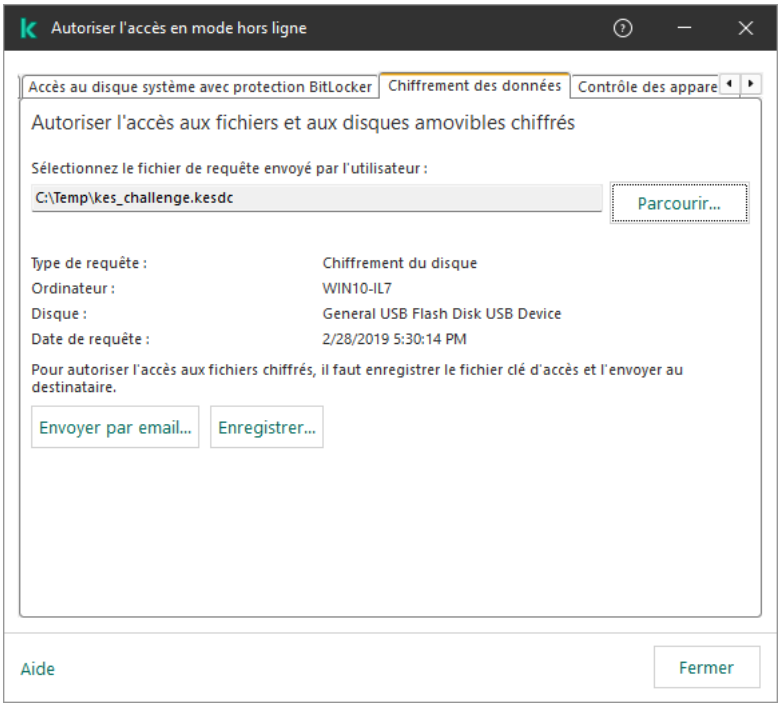
Pour lancer la procédure de restauration, l'utilisateur doit accéder au fichier. Kaspersky Endpoint Security crée alors une requête d'accès au fichier (fichier avec l'extension kesdc), que l'utilisateur doit transmettre à l'administrateur, par exemple par email.

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 l'arborescence de la console, sélectionnez **Appareils**.
3. 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.
4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Chiffrement des données**.
6. Sous l'onglet **Chiffrement des données**, cliquez sur le bouton **Parcourir**.
7. 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.



Accorder l'accès en mode hors ligne

Procédure d'obtention du fichier de clé d'accès aux données chiffrées dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.
3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.
4. Choisissez le **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

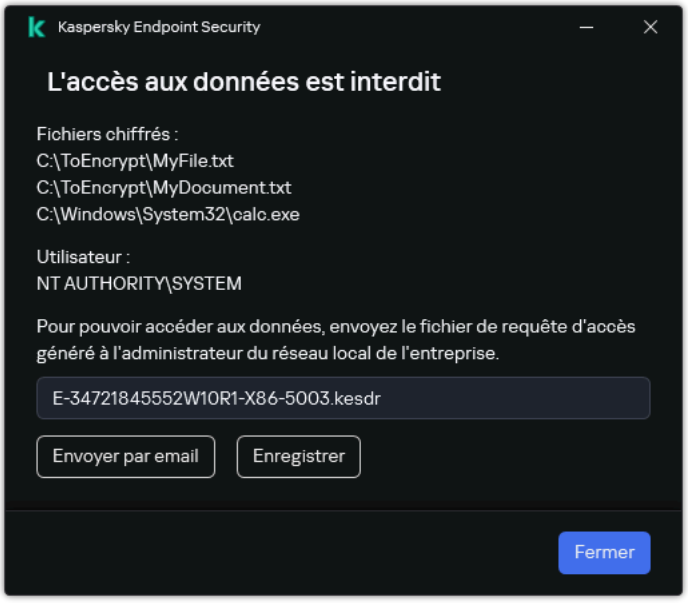
Pour modifier les modèles de messages pour l'octroi de l'accès aux fichiers chiffrés, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Paramètres généraux de chiffrement**.
4. Cliquez sur le bouton **Modèles** dans le groupe **Modèles**.
5. Dans la fenêtre qui s'ouvre, 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 suivante s'ouvre (cf. ill. ci-dessous). Le bouton **Envoyer par email** permet de créer automatiquement un message d'utilisateur. 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**. L'utilisateur reçoit ce message une fois que l'accès aux fichiers chiffrés a été accordé.
6. Modifiez le modèle de message.

   Pour ajouter une variable au texte du modèle, positionnez le curseur à l'endroit souhaité, cliquez sur **Variable** et sélectionnez la variable requise dans la liste des options disponibles.

Vous pouvez également restaurer le texte du modèle par défaut à l'aide du bouton **Par défaut**.

7. Enregistrez vos modifications.



Restauration de l'accès aux fichiers chiffrés

Chiffrement des disques amovibles

Le chiffrement des disques amovibles n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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 :

- Full Disk Encryption (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).

- File Level Encryption (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 déchiffre 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 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".

Avant de chiffrer des fichiers sur un disque amovible, assurez-vous que celui-ci est formaté et qu'il n'y a pas de partitions cachées (comme une partition système EFI). Si le disque contient des partitions non formatées ou masquées, le chiffrement des fichiers peut se solder par une erreur.

Pour chiffrer des disques amovibles, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
4. 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.

5. 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.

6. 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.

7. Si vous souhaitez configurer le chiffrement pour des disques amovibles individuels, définissez les règles de chiffrement.

8. 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 disque amovible n'est pas possible.

9. Enregistrez vos modifications.

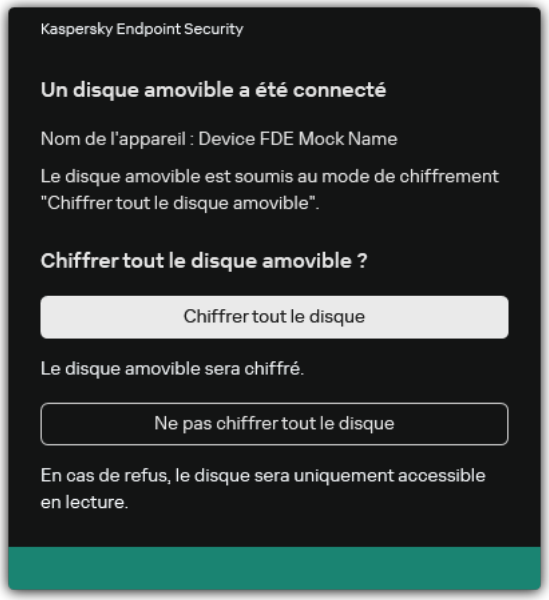
Suite à l'application de la stratégie, si un utilisateur connecte un disque amovible ou si un disque amovible est déjà connecté, Kaspersky Endpoint Security demande une confirmation avant d'exécuter le chiffrement (cf. fig. ci-dessous).

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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
4. 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**.
5. 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.

6. 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.

7. 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.

8. 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 **Actualiser**.

9. 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. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données** → **Chiffrement des disques amovibles**.

5. Dans le groupe **Règles de chiffrement des appareils sélectionnés**, cliquez sur le lien **<N> règles**.

   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 **Exporter**.

   c. Confirmez que vous souhaitez exporter uniquement les règles sélectionnées ou exporter la liste complète.

   d. Enregistrez le fichier.

      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. Ouvrez le fichier.

      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.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.

4. 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. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte la liste des règles dans un fichier XML.

5. 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. Ouvrez le fichier.

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.

6. 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 :

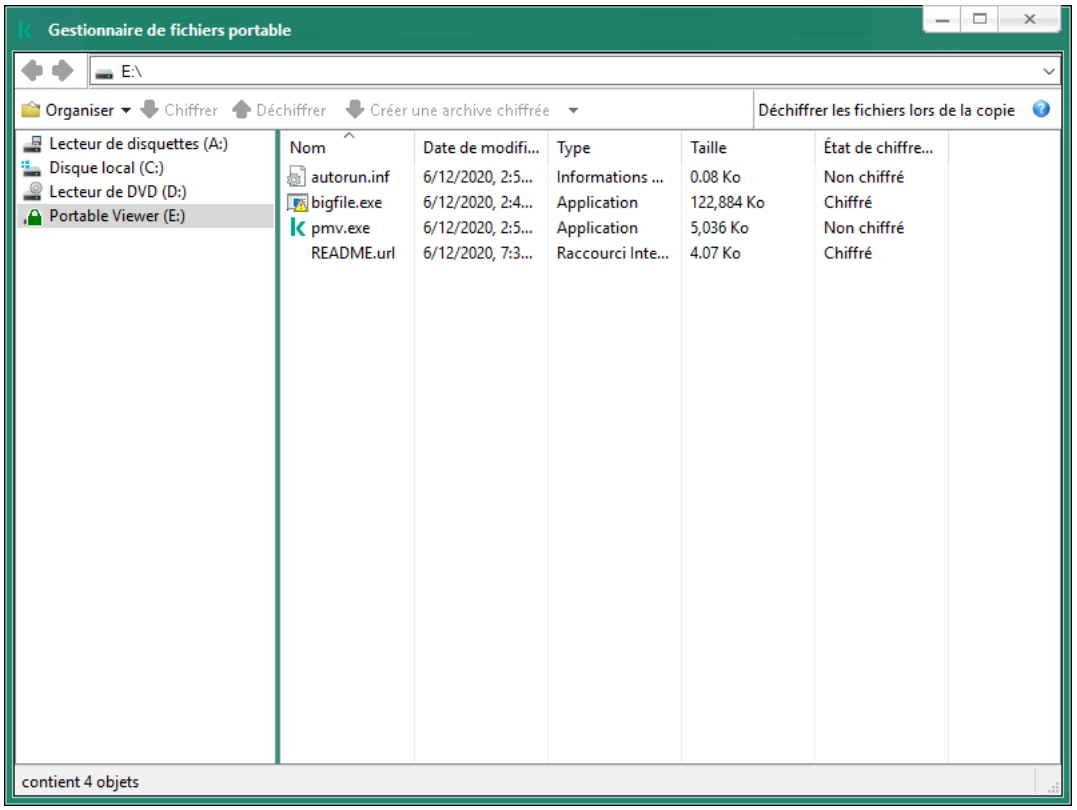
- Il n'y a pas de connexion entre l'ordinateur et le Serveur d'administration de Kaspersky Security Center.
- L'infrastructure a changé avec la modification du Serveur d'administration de Kaspersky Security Center.
- Kaspersky Endpoint Security n'est pas installé sur l'ordinateur.

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

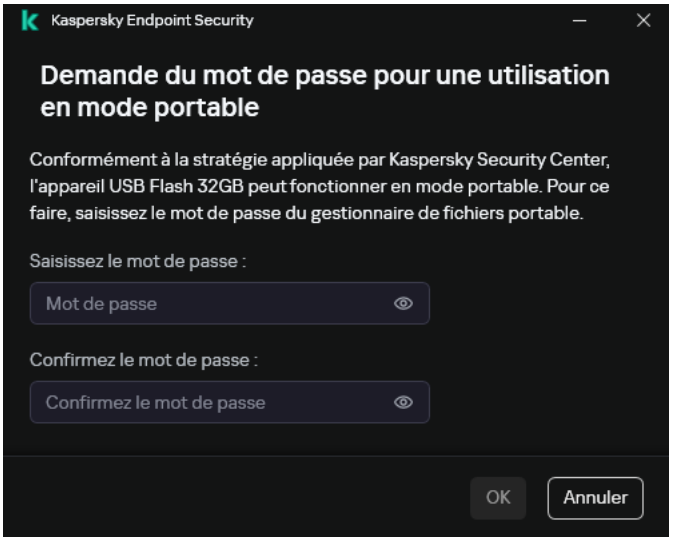
Comment activer la prise en charge du mode portable pour travailler avec des fichiers chiffrés sur des lecteurs amovibles dans la console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.
4. Sélectionnez '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).

5. Cochez la case **Mode portable**.
6. Si nécessaire, ajoutez des règles de chiffrement pour chaque disque amovible.
7. Enregistrez vos modifications.
8. Après avoir appliqué la stratégie, connectez le disque amovible à l'ordinateur.
9. Confirmez l'opération de chiffrement du disque amovible.

La fenêtre de création du mot de passe pour le gestionnaire de fichiers portable s'ouvre.



Demande du mot de passe pour une utilisation en mode portable

10. Définissez un mot de passe qui respecte les exigences en matière de complexité et confirmez-le.

11. Enregistrez vos modifications.

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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Chiffrement des données** → **Chiffrement des disques amovibles**.

5. Dans le groupe **Action par défaut**, 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**.

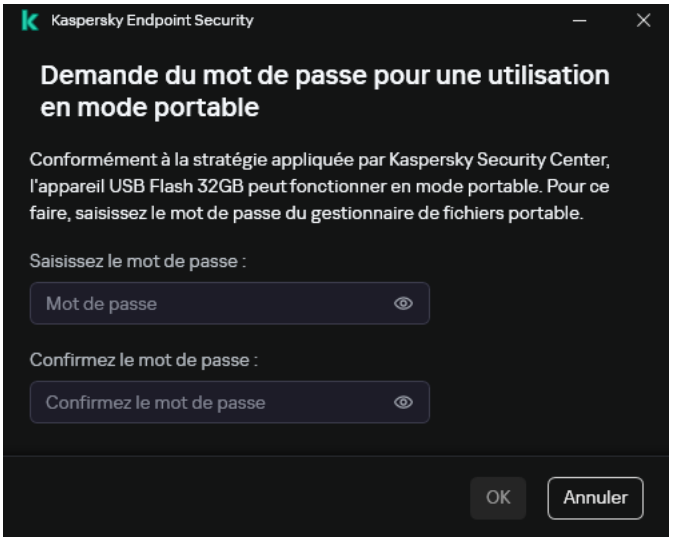
7. Si nécessaire, ajoutez des règles de chiffrement pour chaque disque amovible.

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.



Demande du mot de passe pour une utilisation en mode portable

11. Définissez un mot de passe qui respecte les exigences en matière de complexité et confirmez-le.

12. Enregistrez vos modifications.

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.

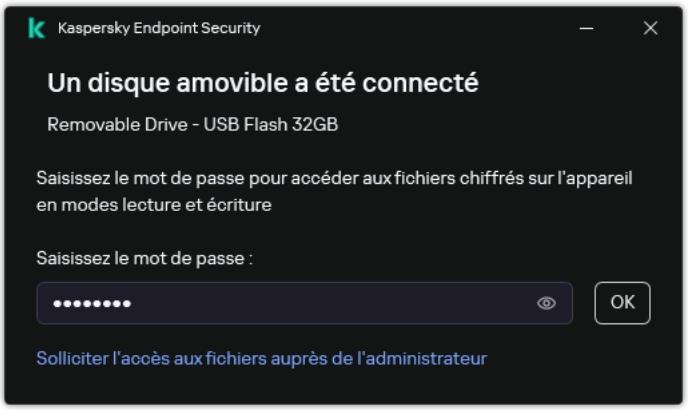
Obtention de l'accès aux fichiers chiffrés sur le disque amovible

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 (voir schéma ci-dessous).

- 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 une clé privée depuis le Serveur d'administration de Kaspersky Security Center auquel l'ordinateur est connecté.



Obtention de l'accès aux fichiers chiffrés sur le disque amovible

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 email par exemple. L'administrateur envoie le fichier d'accès aux données chiffrées (fichier portant l'extension kesdr).

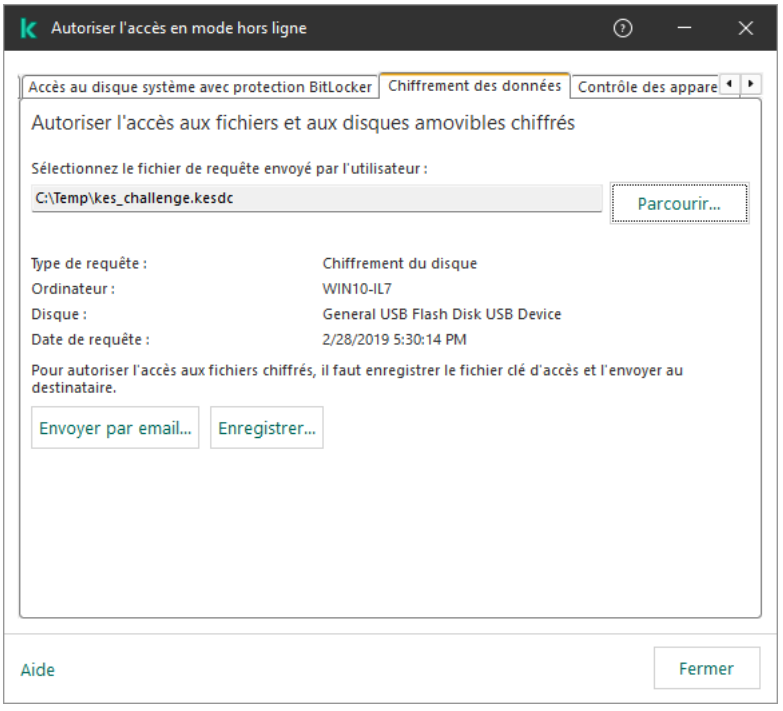
Après avoir suivi la procédure de récupération de mot de passe (Requête- Réponse), vous obtiendrez un accès transparent aux fichiers sur le disque amovible et un accès complet au disque amovible (accès écriture et lecture).

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 l'arborescence de la console, sélectionnez **Appareils**.
3. 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.
4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Chiffrement des données**.
6. Sous l'onglet **Chiffrement des données**, cliquez sur le bouton **Parcourir**.
7. 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.



Accorder l'accès en mode hors ligne

Comment obtenir le fichier d'accès aux données chiffrées dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès aux données.

3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.

4. Choisissez le **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 déchiffre 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. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Chiffrement des données** → **Chiffrement des disques amovibles**.

4. 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**.

5. 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.

   c. Dans le menu contextuel du bouton **Définir la règle**, sélectionnez l'option **Déchiffrer tout le disque amovible**.

6. 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.

Consultation des états du chiffrement

Vous pouvez consulter l'état pour surveiller le chiffrement des données. Kaspersky Endpoint Security attribue les états de chiffrement suivants :

- **Ne correspond pas à la stratégie à cause du refus de l'utilisateur**. L'utilisateur a annulé le chiffrement des données.
- **Ne correspond pas à la stratégie à cause de l'erreur**. Erreur de chiffrement des données, par exemple, une licence est manquante.
- **Stratégie en cours d'application ; le redémarrage est requis**. Le chiffrement des données est en cours sur l'ordinateur. Redémarrez l'ordinateur pour terminer le chiffrement des données.
- **La stratégie de chiffrement n'est pas définie**. Le chiffrement des données est désactivé dans les paramètres de la stratégie.

- **Non pris en charge**. Les modules de chiffrement des données ne sont pas installés sur l'ordinateur.
- **Stratégie en cours d'application**. Le chiffrement et/ou le déchiffrement des données est en cours sur l'ordinateur.

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 l'arborescence de la console, sélectionnez **Appareils administrés**.
3. Sous l'onglet **Appareils** de l'espace de travail, déplacez le curseur au maximum à droite. Si la colonne **État de chiffrement** n'est pas affichée, ajoutez cette colonne dans les paramètres de la console de Kaspersky Security Center.

   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.
4. Si l'état du chiffrement des données pour l'ordinateur est **Stratégie en cours d'application**, vous pouvez surveiller le volet de progression du chiffrement :
   a. Ouvrez les propriétés de l'ordinateur avec l'état **Stratégie en cours d'application** en double-cliquant dessus.
   b. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.
   c. Dans la liste des applications Kaspersky installées sur l'ordinateur, sélectionnez **Kaspersky Endpoint Security for Windows**.
   d. Cliquez sur **Statistiques**.
   e. Sous **Chiffrement des appareils**, vous pouvez voir la progression actuelle du chiffrement des données sous forme de pourcentage.

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, sélectionnez le nœud **Serveur d'administration**.
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**.
   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

c. Une fenêtre s'ouvre alors. Dans cette fenêtre, dans la section **Général**, saisissez le nom de la page.

d. Dans la section **Panneaux d'informations**, cliquez sur **Ajouter**.

e. Dans la fenêtre qui s'ouvre, dans le groupe **État de la protection**, choisissez l'option **Chiffrement des appareils**.

f. Cliquez sur le bouton **OK**.

g. Le cas échéant, les paramètres du panneau de détails doivent être modifiés. Pour ce faire, utilisez les sections **Consulter** et **Appareils**.

h. Cliquez sur le bouton **OK**.

i. Répétez les étapes d à h des instructions et dans la section **État de la protection**, sélectionnez l'option **Chiffrement des disques amovibles**.

   Les panneaux de détails ajoutés s'affichent dans la liste **Panneaux d'informations**.

j. Cliquez sur le bouton **OK**.

   Le nom des pages contenant les barres d'informations créées aux étapes antérieures apparaît dans la liste **Pages**.

k. Cliquez sur le bouton **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 l'arborescence de la console, sélectionnez **Appareils administrés**.

3. Sous l'onglet **Appareils**, sélectionnez l'ordinateur dans la liste et ouvrez le menu contextuel d'un clic droit.

4. Dans le menu contextuel de l'ordinateur, sélectionnez l'option **Propriétés**. Dans la fenêtre qui s'ouvre, sélectionnez la section **Protection**.

5. À l'aide du lien **Consulter les erreurs de chiffrement des données**, accédez à 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

Kaspersky Security Center vous permet de créer des rapports de chiffrement des données :

- **Rapport de l'état de chiffrement des appareils administrés**. Le rapport inclut des informations indiquant si l'état de chiffrement de l'ordinateur est conforme à la stratégie de chiffrement.
- **Rapport de l'état de chiffrement des appareils de stockage de masse**. Le rapport inclut des informations sur l'état de chiffrement des appareils externes et des appareils de stockage.
- **Rapport sur les privilèges d'accès aux disques chiffrés**. Le rapport inclut des informations sur l'état des comptes qui ont accès aux disques chiffrés.
- **Rapport sur les erreurs de chiffrement des fichiers**. Le rapport inclut des informations sur les erreurs qui se sont produites lors de l'exécution des tâches de chiffrement ou de déchiffrement des données sur les ordinateurs.
- **Rapport sur le blocage de l'accès aux fichiers chiffrés**. Le rapport inclut des informations sur les applications dont l'accès aux fichiers chiffrés est bloqué.

Pour consulter le rapport sur le chiffrement des données, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le nœud **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 fenêtre **Sélection du type de modèle de rapport**, dans la section **Autres**, sélectionnez l'un des rapports sur le chiffrement des données.

   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 un 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 d'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.

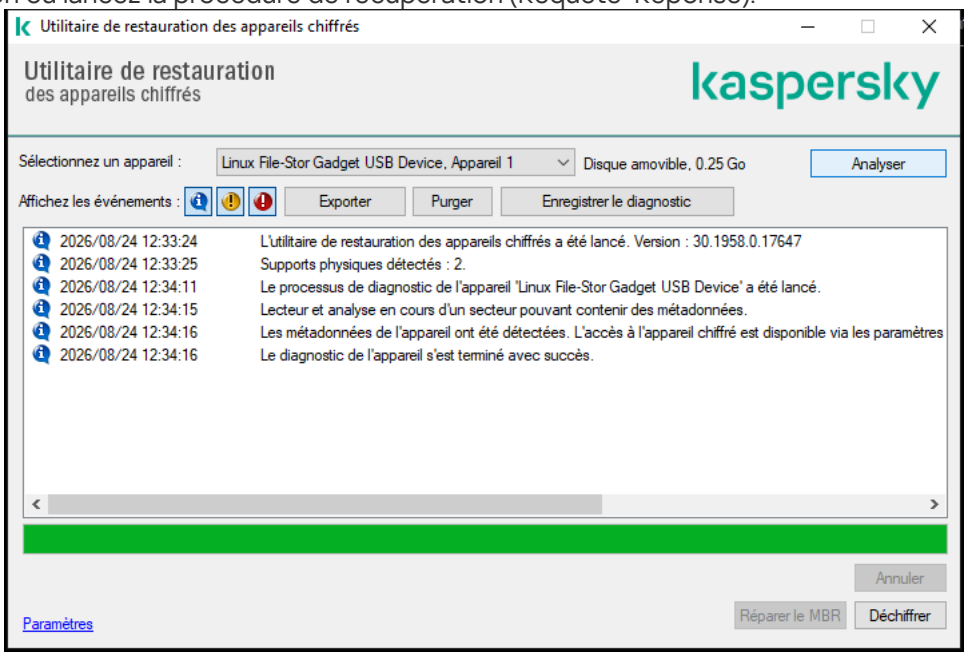
La récupération de données sur un disque protégé par la technologie Kaspersky Disk Encryption comprend les étapes suivantes :

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 .
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 Utilitaire de restauration, 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 **Enregistrer 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 **Ouvrir** 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 **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 d'administration, sélectionnez le dossier **Avancé** → **Chiffrement et protection des données** → **Disques chiffrés**.

3. Dans l'espace de travail, sélectionnez l'appareil chiffré pour lequel vous souhaitez créer un fichier de clé d'accès, puis dans le menu contextuel de l'appareil, cliquez sur **Obtenir l'accès à l'appareil dans Kaspersky Endpoint Security**.

   Si vous n'êtes pas certain de connaître l'ordinateur pour lequel le fichier de demande d'accès a été créé, dans l'arborescence de la Console d'administration, sélectionnez le dossier **Avancé** → **Chiffrement et protection des données**, puis, dans l'espace de travail, cliquez sur **Obtenir la clé de chiffrement de l'appareil dans Kaspersky Endpoint Security**.

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 **Parcourir** pour ouvrir une fenêtre. Dans cette fenêtre, indiquez le chemin d'accès au fichier de demande avec l'extension fdertc que l'utilisateur a reçu.

6. Cliquez sur **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** → **Disques chiffrés**.

2. Cochez la case en regard du nom de l'ordinateur sur lequel vous souhaitez récupérer les données.

3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.

   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. Sélectionnez la requête d'accès au fichier reçue de l'utilisateur (fichier portant l'extension FDERTC).

   d. Sélectionnez un dossier pour enregistrer le fichier clé d'accès aux données chiffrées (fichier portant 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).

Solutions Detection and Response

Les solutions Kaspersky Detection and Response sont des systèmes de sécurité permettant de détecter les menaces avancées et les indicateurs d'attaque à différents niveaux de l'infrastructure d'une organisation. Les solutions Detection and Response fournissent des informations sur la menace détectée et permettent de gérer les actions de réponse aux menaces.

Ainsi, la solution Detection and Response effectue les opérations suivantes :

- Réception des informations sur le fonctionnement d'un ordinateur, d'un serveur ou d'autres appareils (télémétrie).
- Analyse automatique des informations dans le but de détecter les menaces.
- Génération des détails de l'alerte sous forme de colonnes de la chaîne de développement des menaces à des fins d'analyse et pour choisir les actions de réponse aux menaces.
- Exécution des actions de réponse aux menaces (par exemple, isolation réseau de l'ordinateur).

Kaspersky Endpoint Security prend en charge les solutions Detection and Response grâce à un agent intégré. L'agent intégré envoie les données télémétriques aux serveurs de solutions et exécute des actions de réponse aux menaces. L'agent intégré prend en charge ce qui suit :

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform :
  - Endpoint Detection and Response (EDR) version 7.1 ou version antérieure
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Vous pouvez utiliser la solution Kaspersky Endpoint Security with Detection and Response dans différentes configurations, par exemple, [EDR Optimum+MDR].

Licences MDR et EDR Optimum

Kaspersky Endpoint Security prend en charge les fonctionnalités des solutions Kaspersky Managed Detection and Response (MDR) et Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Vous pouvez utiliser Kaspersky Endpoint Security avec ces solutions dans différentes configurations et créer un système de protection personnalisé répondant à vos besoins. Pour cela, il convient d'acheter une licence pour chacune des solutions. La licence peut couvrir le droit d'utiliser une seule solution (par exemple, le module complémentaire MDR seulement) ou plusieurs solutions, par exemple le module complémentaire [EDR Optimum+MDR].

MDR et EDR Optimum prennent en charge les modes de licence suivants :

- La fonctionnalité MDR ou EDR Optimum est couverte par la licence de Kaspersky Endpoint Security for Windows.

  La fonction est disponible immédiatement après l'activation de Kaspersky Endpoint Security for Windows. Il vous suffit d'ajouter une clé.

- Licences distinctes pour MDR ou EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  La fonctionnalité est disponible après l'ajout d'une clé distincte pour le module complémentaire MDR, le module complémentaire EDR Optimum ou le module complémentaire [EDR Optimum+MDR]. Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour MDR ou EDR Optimum. La clé Kaspersky Endpoint Security doit être ajoutée en premier.

Kaspersky Endpoint Security permet d'ajouter une seule *clé active* pour les licences MDR et EDR Optimum. Par conséquent, s'il faut activer ces deux solutions, il faut ajouter une clé de [EDR Optimum+MDR] Add-on au lieu d'une clé distincte pour chaque solution. Vous pouvez également ajouter une *clé de réserve*.

> Si vous avez utilisé un fichier BLOB lors du déploiement de MDR, vous n'avez pas besoin d'une clé distincte pour activer MDR. Le fichier BLOB contient déjà des informations sur la licence.

Licence initiale des solutions

Lors du premier déploiement de MDR et d'EDR Optimum, les solutions sont activées au même titre que l'application Kaspersky Endpoint Security. Vous pouvez ajouter une clé à l'aide de la tâche *Ajout d'une clé* ou utiliser la fonctionnalité de distribution automatique des clés. La clé de licence est ajoutée à l'application en tant que deuxième clé active ou en tant que clé de réserve si vous cochez la case correspondante.

Passage d'une licence à une autre

Si votre organisation a déjà déployé l'une de ces solutions et que la clé correspondante a été ajoutée dans l'application, l'octroi de licences pour la nouvelle configuration implique certaines considérations particulières. Lors du passage à une autre licence, l'application n'ajoute pas la nouvelle clé à l'application, mais remplace la clé actuelle par la nouvelle. La raison en est la restriction qui permet à l'application d'ajouter une seule clé pour activer MDR et EDR Optimum.

Par exemple, supposons que votre organisation ait déployé la solution [EDR Optimum+MDR] et que vous ayez décidé de passer à la configuration du module complémentaire MDR. Pour passer à la nouvelle configuration, il convient de remplacer la clé du [EDR Optimum+MDR] Add-on par la clé du module complémentaire MDR.

Les licences distinctes pour EDR Optimum et MDR (module complémentaire [EDR Optimum+MDR]) ne sont plus disponibles. Pour pouvoir utiliser ces deux solutions, il faut activer MDR à l'aide d'un fichier BLOB et EDR Optimum contenant une clé de licence.

Avec la fonction de distribution automatique des clés, l'application n'accepte pas les clés de licence qui couvrent le même nombre de solutions. Autrement dit, si vous avez ajouté une clé de module complémentaire EDR Optimum, vous ne pouvez pas remplacer cette clé par une clé de module complémentaire MDR. Cependant, vous pouvez remplacer la clé de module complémentaire EDR Optimum par une clé de module complémentaire [EDR Optimum+MDR]. L'application refusera également les clés si vous essayez de remplacer une clé de module complémentaire MDR par une clé de module complémentaire EDR. Pour remplacer une clé, vous pouvez exécuter la tâche *Ajout d'une clé*. La tâche *Ajout d'une clé* permet de remplacer les clés de licence par n'importe quel nombre de solutions.

Si vous avez ajouté une clé de réserve de [EDR Optimum+MDR] Add-on, pour ajouter correctement une clé active pour le module complémentaire EDR Optimum ou MDR, il faut d'abord remplacer la clé de réserve par une clé de module complémentaire EDR Optimum ou MDR ou, à défaut, supprimer la clé de réserve, puis remplacer la clé active.

Compatibilité avec des solutions EDR tierces

Vous pouvez utiliser Kaspersky Endpoint Security pour protéger les postes de travail et les serveurs avec des solutions EDR tierces. Pour éliminer les faux positifs, nous recommandons d'ajouter les fichiers exécutables de Kaspersky Endpoint Security et Network Agent à la zone de confiance de votre solution EDR tierce.

	Kaspersky Endpoint Security for Windows	Agent d'administration de Kaspersky Security Center
Dossier de travail	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Fichiers exécutables	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

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 utiliser Kaspersky Endpoint Agent dans le cadre des solutions Kaspersky, vous devez activer ces solutions avec une clé de licence correspondante.

Pour en savoir plus à propos de Kaspersky Endpoint Agent 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 :

- Aide de Kaspersky Anti Targeted Attack Platform
- Aide de Kaspersky Sandbox
- Aide de Kaspersky Endpoint Detection and Response Optimum
- Aide de Kaspersky Managed Detection and Response

Le kit de distribution pour les versions 11.2.0 à 11.8.0 de Kaspersky Endpoint Security inclut Kaspersky Endpoint Agent. Vous pouvez sélectionner Kaspersky Endpoint Agent lorsque vous installez Kaspersky Endpoint Security for Windows. Deux applications seront alors installées sur votre ordinateur : KEA et KES. Dans Kaspersky Endpoint Security 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution de Kaspersky Endpoint Security.

Correspondance des versions KEA (dans le cadre de KES) aux versions KES

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky modifie le processus pour que toutes les solutions Detection and Response fonctionnent avec l'agent intégré de Kaspersky Endpoint Security à la place de Kaspersky Endpoint Agent. Kaspersky ajoute progressivement la prise en charge de ces solutions et abandonne progressivement Kaspersky Endpoint Agent (voir tableau ci-dessous). À partir de la version 12.1, l'application prend en charge toutes les solutions Detection and Response. De plus, à partir de la version 12.1, l'application n'est plus compatible avec Kaspersky Endpoint Agent, et il n'est plus possible d'installer les deux applications côte à côte sur le même ordinateur.

Déploiement de l'agent intégré pour gérer les solutions Detection and Response

Version de Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (module Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (module Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	Kaspersky Endpoint Agent
12.6	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**	**Agent intégré**

Migration de la configuration [KES+KEA] vers la configuration [KES+agent intégré]

Kaspersky Endpoint Security inclut des agents intégrés pour travailler avec les solutions Detection and Response. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser ces solutions. Lorsque vous déployez Kaspersky Endpoint Security sur des ordinateurs sur lesquels Kaspersky Endpoint Agent est installé, les solutions Detection and Response continueront à fonctionner avec Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur.

Le kit de distribution pour les versions 11.2.0 à 11.8.0 de Kaspersky Endpoint Security inclut Kaspersky Endpoint Agent. Vous pouvez sélectionner Kaspersky Endpoint Agent lorsque vous installez Kaspersky Endpoint Security for Windows. Deux applications seront alors installées sur votre ordinateur : KEA et KES. Dans Kaspersky Endpoint Security 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution de Kaspersky Endpoint Security.

La migration de la configuration de [KES+KEA] vers [KES+agent intégré] comprend les étapes suivantes :

1. **Mise à jour de Kaspersky Security Center**

   Mettez à jour tous les modules de Kaspersky Security Center vers la version 13.2 ou une version ultérieure, y compris l'Agent d'administration, sur les ordinateurs des utilisateurs et Web Console.

2. **Mise à jour du plug-in Internet de Kaspersky Endpoint Security**

   Dans Kaspersky Security Center Web Console, mettez à jour le plug-in Internet de Kaspersky Endpoint Security vers la version 11.7.0 ou une version ultérieure. Pour administrer les modules EDR Optimum et Kaspersky Sandbox, vous devez utiliser Web Console.

   Pour utiliser Kaspersky Anti Targeted Attack Platform (EDR), vous avez besoin d'un plug-in Internet pour Kaspersky Endpoint Security version 12.1 ou toute version ultérieure.

   Pour utiliser Kaspersky Anti Targeted Attack Platform (NDR), vous avez besoin d'un plug-in Internet pour Kaspersky Endpoint Security version 12.7 ou toute version ultérieure.

3. **Migration de la stratégie et des tâches**

   Utilisez l'Assistant de migration des stratégies et des tâches de Kaspersky Endpoint Agent pour procéder à la migration des paramètres de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows.

   Vous pouvez créer une stratégie Kaspersky Endpoint Security. La nouvelle stratégie porte l'état *Inactive*. Pour appliquer la stratégie, ouvrez-en les propriétés, acceptez la Déclaration de Kaspersky Security Network et définissez l'état sur *Actif*.

4. **Fonctionnalités des licences**

   Si vous utilisez une licence commune Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Security for Windows et Kaspersky Endpoint Agent, la fonctionnalité EDR Optimum sera activée automatiquement après la mise à jour de l'application vers la version 11.7.0. Aucune autre action n'est nécessaire.

   Si vous utilisez une licence autonome de l'extension Kaspersky Endpoint Detection and Response Optimum pour activer la fonctionnalité EDR Optimum, vous devez vous assurer que la clé de module complémentaire EDR Optimum est ajoutée au stockage de Kaspersky Security Center et que la fonctionnalité de distribution automatique des clés de licence est activée. Une fois que la mise à jour de l'application vers la version 11.7.0 est effectuée, la fonctionnalité EDR Optimum est activée automatiquement.

Si vous utilisez une licence Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Agent et une autre licence pour activer Kaspersky Endpoint Security for Windows, vous devez remplacer la clé de Kaspersky Endpoint Security for Windows par la clé commune de Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security. Vous pouvez remplacer la clé à l'aide de la tâche *Ajout d'une clé*.

Vous n'avez pas besoin d'activer la fonctionnalité de Kaspersky Sandbox. La fonctionnalité de Kaspersky Sandbox sera disponible immédiatement après la mise à jour et l'activation de Kaspersky Endpoint Security for Windows.

Seule la licence Kaspersky Anti Targeted Attack Platform peut être utilisée pour activer Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Anti Targeted Attack Platform. Une fois que la mise à jour de l'application vers la version 12.1 est effectuée, la fonctionnalité EDR (KATA) est activée automatiquement. Aucune autre action n'est nécessaire.

5 **Mise à jour de l'application Kaspersky Endpoint Security**

Pour mettre à jour l'application et procéder à la migration des fonctionnalités d'EDR Optimum et de Kaspersky Sandbox, il est recommandé d'utiliser une tâche d'installation à distance.

Pour mettre à jour l'application à l'aide d'une tâche d'installation à distance, vous devez modifier les paramètres suivants :

- Sélectionnez les modules des solutions Detection and Response dans les paramètres du paquet d'installation.
- Excluez le module Kaspersky Endpoint Agent dans les paramètres du paquet d'installation (pour les versions 11.2.0 à 11.8.0 de Kaspersky Endpoint Security for Windows).
- Si la Protection par mot de passe est activée pour restreindre l'accès à Kaspersky Endpoint Agent, saisissez le mot de passe de désinstallation de l'application dans les paramètres de la tâche *Installation à distance d'une application*. Vous pouvez saisir le mot de passe de désinstallation à partir de Kaspersky Security Center Linux 15.1.

Vous pouvez également mettre à jour l'application en utilisant les méthodes suivantes :

- En utilisant le service de mise à jour de Kaspersky (Mises à jour transparentes - SMU).
- Localement à l'aide de l'Assistant d'installation de l'application.

Kaspersky Endpoint Security prend en charge la sélection automatique des modules lors de la mise à jour de l'application sur un ordinateur sur lequel est installée l'application Kaspersky Endpoint Agent. La sélection automatique des modules dépend des autorisations du compte utilisateur qui met à jour l'application.

Si vous mettez à jour Kaspersky Endpoint Security en utilisant le fichier EXE ou MSI sous le compte système (SYSTEM), Kaspersky Endpoint Security obtient l'accès aux licences valides des solutions Kaspersky. Par conséquent, si, par exemple, Kaspersky Endpoint Agent est installé et la solution EDR Optimum est activée sur l'ordinateur, le programme d'installation de Kaspersky Endpoint Security configure automatiquement l'ensemble des modules et sélectionne le module EDR Optimum. Cette opération fait passer Kaspersky Endpoint Security à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. L'exécution du programme d'installation MSI sous le compte système (SYSTEM) est généralement effectuée lors de la mise à jour via le service de mise à jour Kaspersky (SMU) ou lors du déploiement d'un paquet d'installation via Kaspersky Security Center.

Si vous mettez à jour Kaspersky Endpoint Security à l'aide d'un fichier MSI sous un compte utilisateur non privilégié, Kaspersky Endpoint Security n'a pas accès aux licences valides des solutions Kaspersky. Dans ce cas, Kaspersky Endpoint Security sélectionne automatiquement les modules en fonction de la configuration de Kaspersky Endpoint Agent. Après cela, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

6. **Redémarrage de l'ordinateur**

   Redémarrez votre ordinateur pour terminer la mise à jour de l'application avec l'agent intégré. Lors de la mise à jour de l'application, le programme d'installation supprime Kaspersky Endpoint Agent avant le redémarrage de l'ordinateur. Une fois que l'ordinateur a redémarré, le programme d'installation ajoute l'agent intégré. Cela signifie que Kaspersky Endpoint Security n'exécute pas les fonctions d'EDR et de Kaspersky Sandbox tant que l'ordinateur n'a pas redémarré.

7. **Vérification de l'état de santé de Kaspersky Endpoint Detection and Response Optimum et de Kaspersky Sandbox**

   Si après la mise à jour, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

   - Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
   - Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*.
   - Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.
   - Assurez-vous que la fonctionnalité EDR Optimum est activée à l'aide de l'icône *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous que la fonctionnalité de distribution automatique des clés de licence de EDR Optimum est activée.

Migration des stratégies et des tâches pour Kaspersky Endpoint Agent

Kaspersky Endpoint Security for Windows inclut un Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security. Vous pouvez réaliser la migration des paramètres de stratégie et de tâches pour les solutions suivantes :

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

L'Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security fonctionne uniquement dans Web Console et Cloud Console. Dans la Console d'administration (MMC), vous ne pouvez migrer les paramètres de la solution Kaspersky Anti Targeted Attack Platform (EDR) qu'à l'aide de l'Assistant de migration standard des tâches et des stratégies de Kaspersky Security Center.

> Il est conseillé de débuter par la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security sur un seul ordinateur, puis sur un groupe d'ordinateurs et pour conclure, de réaliser la migration sur l'ensemble des ordinateurs de l'organisation.

Pour migrer les paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security,

dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Migration depuis Kaspersky Endpoint Agent**.

Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

Étape 1. Migration de stratégie

L'Assistant de migration crée une stratégie que fusionne les paramètres des stratégies de Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez fusionner les paramètres avec ceux de la stratégie de Kaspersky Endpoint Security. Cliquez sur une stratégie de Kaspersky Endpoint Agent pour sélectionner la stratégie Kaspersky Endpoint Security avec laquelle vous souhaitez fusionner les paramètres. Confirmez que vous avez sélectionné les bonnes stratégies, puis passez à l'étape suivante.

Étape 2. Migration d'une tâche

L'Assistant de migration crée de nouvelles tâches pour Kaspersky Endpoint Security. Dans la liste de tâches, sélectionnez les tâches de Kaspersky Endpoint Agent que vous souhaitez créer pour une stratégie de Kaspersky Endpoint Security. L'Assistant prend en charge les tâches pour Kaspersky Endpoint Detection and Response et Kaspersky Sandbox. Passez à l'étape suivante.

Étape 3. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- Crée une stratégie Kaspersky Endpoint Security.

  La stratégie fusionne les paramètres de Kaspersky Endpoint Security et Kaspersky Endpoint Agent La stratégie porte le nom *<Nom de stratégie de Kaspersky Endpoint Security> et <Nom de stratégie de Kaspersky Endpoint Agent>*. La nouvelle stratégie porte l'état *Inactive*. Pour continuer, changez l'état des stratégies de Kaspersky Endpoint Agent et Kaspersky Endpoint Security sur *Inactive* et activez la nouvelle stratégie fusionnée.

  Après avoir procédé à la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows, veuillez vous assurer que la fonctionnalité de transfert de données vers le Serveur d'administration (données du fichier de quarantaine et données de la chaîne de développement des menaces) est configurée dans la nouvelle stratégie. Les valeurs des paramètres de transfert de données ne sont pas migrées à partir d'une stratégie de Kaspersky Endpoint Agent.

Lors de la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security pour la solution Kaspersky Anti Targeted Attack Platform (EDR), vous pouvez rencontrer des erreurs lors de la connexion de l'ordinateur aux serveurs de Central Node. La raison en est que l'Assistant de migration de Web Console ignore les paramètres de stratégie suivants et ne les migre pas :

- Interdiction de modification des paramètres **Connexion aux serveurs KATA** (« cadenas »).

  Par défaut, les paramètres peuvent être modifiés (le « cadenas » est ouvert). Par conséquent, les paramètres ne sont pas appliqués sur l'ordinateur. Vous devez interdire la modification des paramètres et fermer le « cadenas ».

- Conteneur crypto.

  Si vous utilisez l'authentification bidirectionnelle pour vous connecter aux serveurs de Central Node, vous devez rajouter le conteneur crypto. L'Assistant de migration migre correctement le certificat TLS du serveur.

L'Assistant de migration des stratégies et des tâches de la Console d'administration (MMC) migre tous les paramètres de la solution Kaspersky Anti Targeted Attack Platform (EDR).

- Crée de nouvelles tâches de Kaspersky Endpoint Security.

  Les nouvelles tâches sont des copies des tâches de Kaspersky Endpoint Agent pour Kaspersky Endpoint Detection and Response et Kaspersky Sandbox. En même temps, l'Assistant laisse les tâches de Kaspersky Endpoint Agent inchangées.

Comment migrer les paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security dans la Console d'administration (MMC) (uniquement pour KATA (EDR))

1. Dans la Console d'administration, sélectionnez le Serveur d'administration et faites un clic droit pour ouvrir le menu contextuel.

2. Choisissez **Toutes les tâches** → **Assistant de conversion de masse des stratégies et des tâches**.

Ensuite, l'Assistant de conversion de masse des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Étape 1. Sélectionnez l'application dont il faut convertir les stratégies et les tâches

À cette étape, vous devez sélectionner Kaspersky Endpoint Security for Windows. Passez à l'étape suivante.

Étape 2. Conversion des stratégies

L'Assistant de migration crée une stratégie de Kaspersky Endpoint Security dans laquelle les paramètres de la stratégie de Kaspersky Endpoint Agent seront migrés. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez transférer les paramètres vers la stratégie de Kaspersky Endpoint Security. Passez à l'étape suivante.

L'Assistant de migration commencera alors à convertir les stratégies. Lors de la conversion de la stratégie, l'Assistant de migration vous invite à accepter la déclaration de Kaspersky Security Network. Les nouvelles stratégies seront nommées *<nom de la stratégie> (convertie)*.

Étape 3. Conversion des tâches

Ignorez cette étape. L'Assistant prend en charge les tâches uniquement pour Kaspersky Endpoint Detection and Response Optimum et Kaspersky Sandbox. La gestion de ces modules n'est disponible que dans Web Console. Passez à l'étape suivante.

Étape 4. Fin de l'Assistant

Quittez l'Assistant. À la suite de l'Assistant, une nouvelle stratégie de Kaspersky Endpoint Security sera créée.

Endpoint Detection and Response Agent (EDR Agent)

À partir de Kaspersky Endpoint Security 12.3 for Windows, l'application inclut la configuration Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* est une application installée sur les postes de travail et les serveurs individuels de l'infrastructure informatique de l'organisation pour prendre en charge les solutions Detection and Response suivantes par Kaspersky :

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (à partir de la version 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (à partir de la version 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (à partir de la version 12.11)

EDR Agent ne prend pas en charge l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent surveille en permanence les processus en cours d'exécution sur ces ordinateurs, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les modules de protection et de contrôle de l'application ne sont pas disponibles pour EDR Agent.

EDR Agent est compatible avec les applications PPE tierces. Vous pouvez ainsi utiliser des outils de sécurité d'infrastructure tiers ainsi que la solution Detection and Response de Kaspersky.

Pour que vous puissiez déployer EDR Agent, l'Agent d'administration doit être installé sur l'ordinateur, et l'ordinateur doit être ajouté à la console Kaspersky Security Center. Pour activer l'interaction d'EDR Agent avec Kaspersky Security Center, vous devez installer le plug-in d'administration de Kaspersky Endpoint Security for Windows. Vous pouvez préciser les paramètres d'EDR Agent à l'aide d'une stratégie de groupe. Pour intégrer EDR Agent, vous devez configurer l'intégration dans les sections de stratégie appropriées.

Les applications Kaspersky suivantes doivent être installées sur l'infrastructure pour prendre en charge les solutions Kaspersky Detection and Response :

	• Agent d'administration • EDR Agent
Terminal	
	Plug-in d'administration de Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
Solutions Detection and Response : MDR, KATA (EDR), KATA (NDR), KUMA et EDR Expert (on-premises)	

Installation d'EDR Agent

Dans la configuration Endpoint Detection and Response Agent (EDR Agent) pour les solutions Kaspersky Detection and Response, Kaspersky Endpoint Security s'installe de la même manière.

EDR Agent peut être installé sur l'ordinateur de l'une des manières suivantes :

- À distance via Kaspersky Security Center.
- Localement à l'aide de l'Assistant d'installation de l'application.
- Localement à partir de la ligne de commande (uniquement pour KATA (EDR) et EDR Expert (on-premises)).

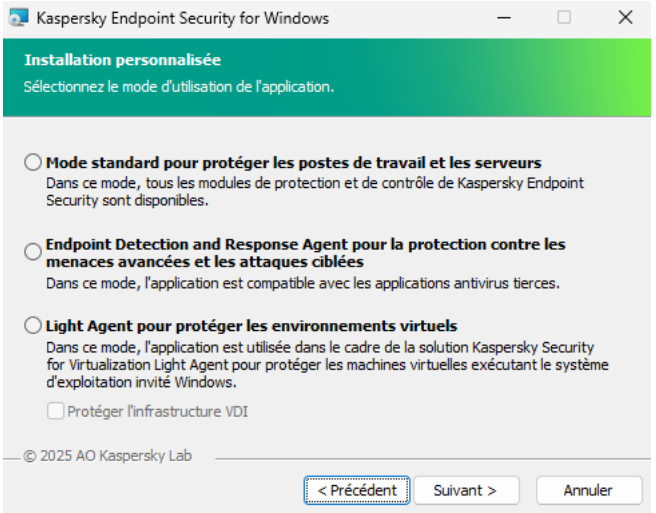
Pour installer EDR Agent, vous devez sélectionner la configuration appropriée dans les paramètres du paquet d'installation ou dans l'Assistant d'installation.

Comment installer EDR Agent à l'aide de l'Assistant d'installation

1. Copiez le dossier du kit de distribution sur l'ordinateur de l'utilisateur.
2. Exécutez le fichier setup_kes.exe.

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

Configuration de Kaspersky Endpoint Security



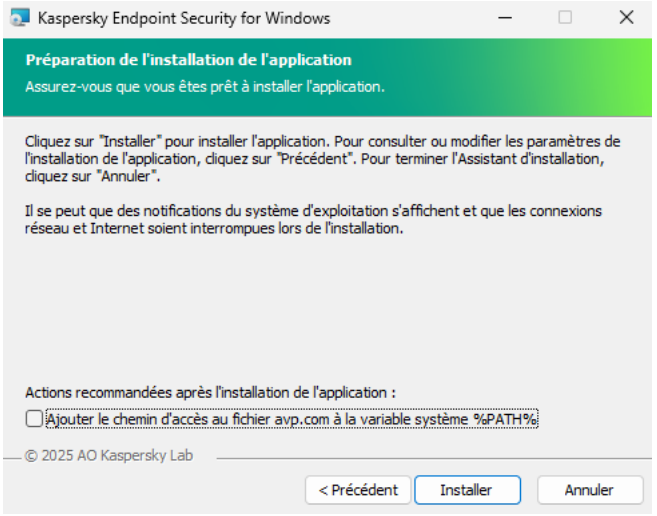
Choix de la configuration de l'application

Sélectionnez la configuration **Endpoint Detection and Response Agent**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

Modules de Kaspersky Endpoint Security

Sélectionnez les modules que vous souhaitez installer. 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



Paramètres d'installation avancés de l'application

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 d'accès au fichier avp.com à la variable système %PATH%. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% pour le confort de l'utilisation de l'interface de la ligne de commande.

Comment installer EDR Agent à partir de la ligne de commande (uniquement pour KATA (EDR) et EDR Expert (on-premises))

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 /pSTANDALONEMODE=1 [/s]
   ```

   ou

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   En conséquence, l'application EDR Agent destinée à être intégrée avec Kaspersky Anti Targeted Attack Platform (EDR) ou Kaspersky Endpoint Detection and Response Expert (on-premises) est installée sur l'ordinateur. Vous pouvez confirmer que l'application est installée et vérifier les paramètres de l'application en lançant la commande `status`.

Comment installer EDR Agent à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.

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

3. Ouvrez les propriétés du fichier d'installation.

   Si nécessaire, créez un autre paquet d'installation.

4. Passez à la section **Modules de protection**.

5. Sélectionnez la configuration **Endpoint Detection and Response Agent pour la protection contre les menaces avancées et les attaques ciblées**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

6. Sélectionnez les modules que vous souhaitez installer.

   Vous pouvez modifier la liste des modules après avoir installé l'application.

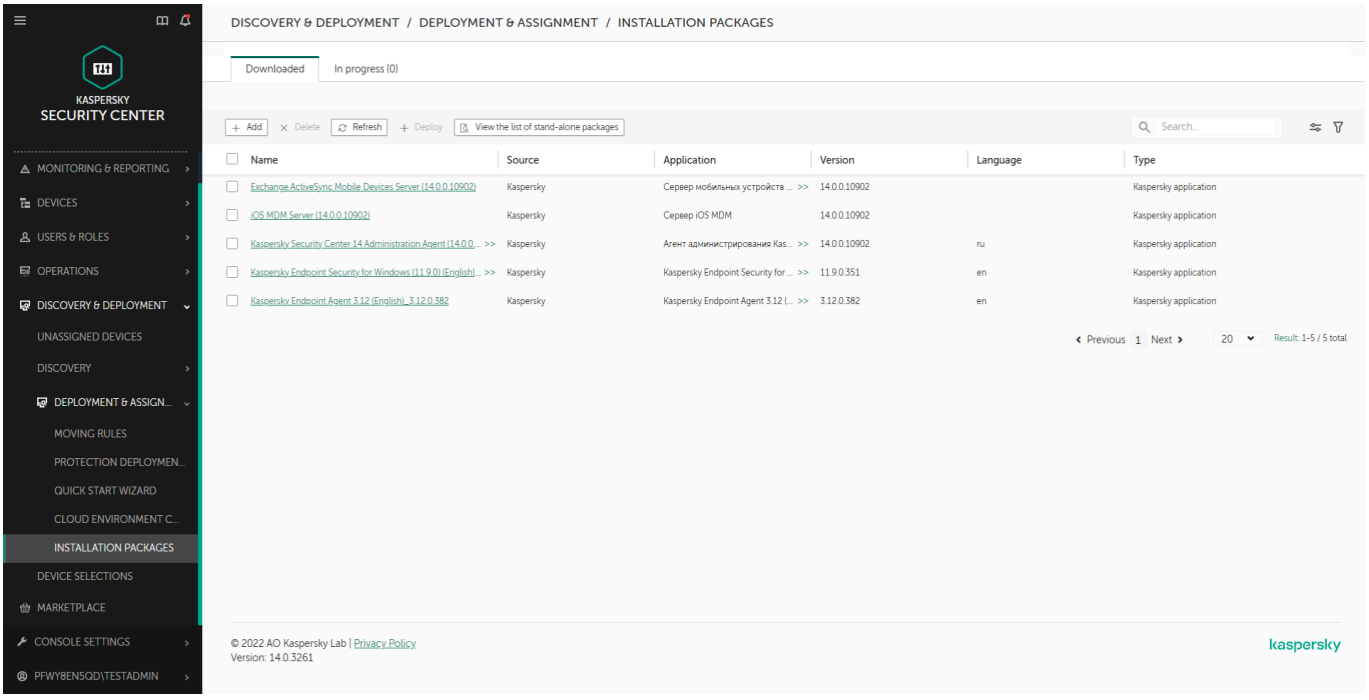
7. Enregistrez vos modifications.

8. Créez une tâche d'installation à distance. Dans les propriétés de la tâche, sélectionnez le paquet d'installation que vous avez créé.

Comment installer EDR Agent à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

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



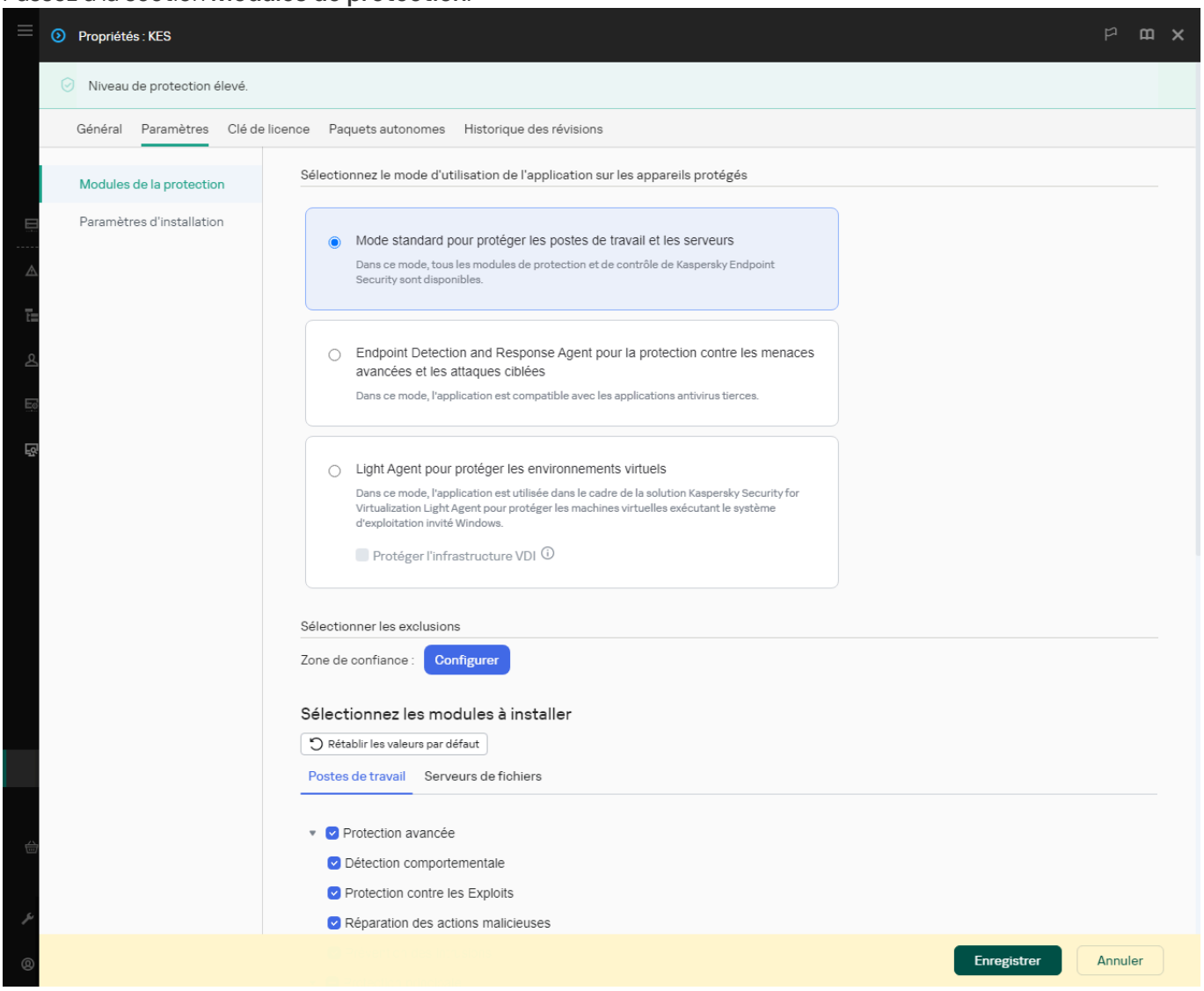
Liste des paquets d'installation

2. Ouvrez les propriétés du fichier d'installation.

   Si nécessaire, créez un autre paquet d'installation.

3. Sélectionnez l'onglet **Configuration**.

4. Passez à la section **Modules de protection**.



Modules inclus dans le paquet d'installation

5. Sélectionnez la configuration **Endpoint Detection and Response Agent**. Dans cette configuration, vous ne pouvez installer que les modules assurant la prise en charge des solutions Detection and Response : MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) ainsi que KUMA. Cette configuration est nécessaire si une plateforme Endpoint Protection Platform (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.

6. Sélectionnez les modules que vous souhaitez installer.

   Vous pouvez modifier la liste des modules après avoir installé l'application.

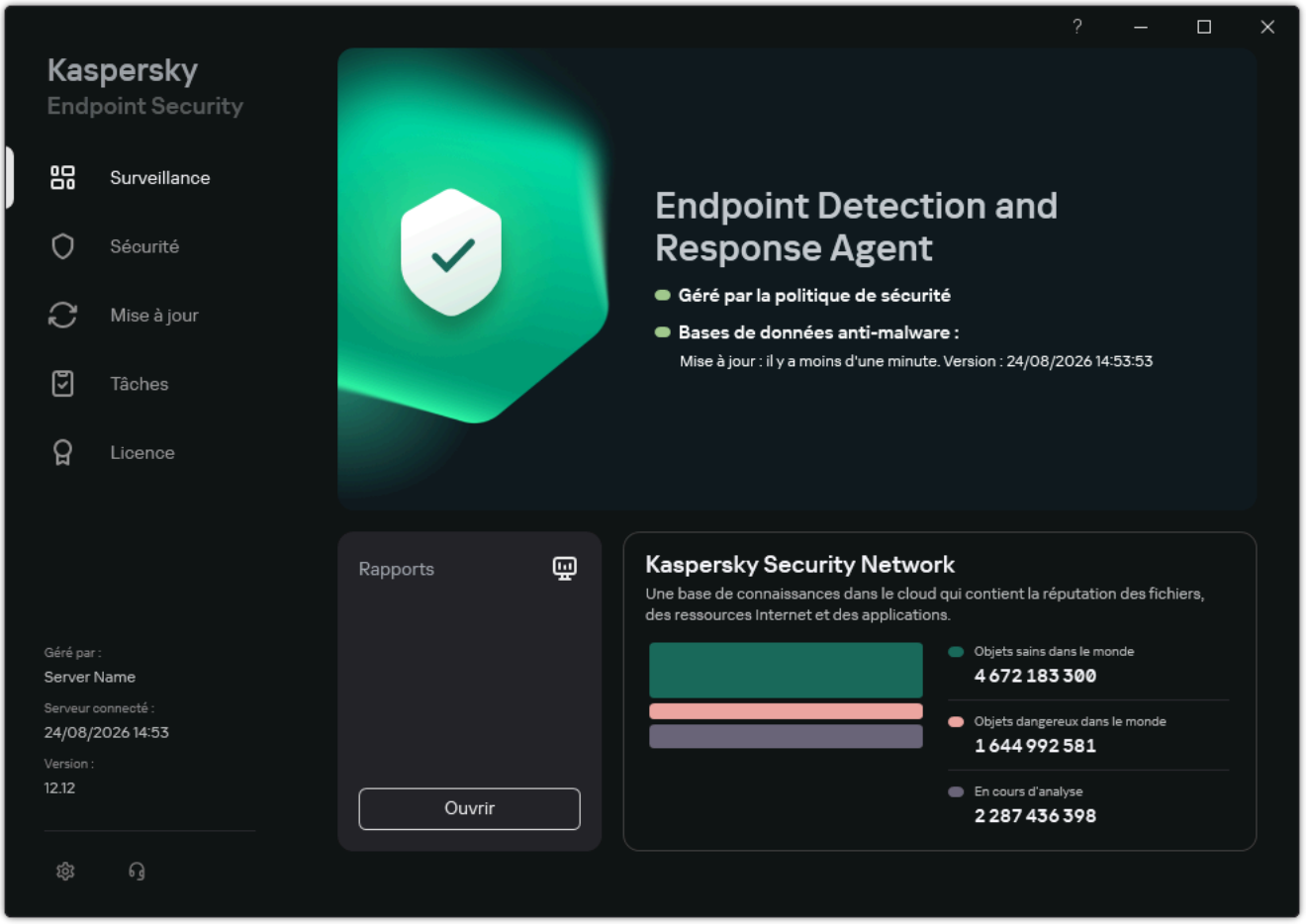
7. Enregistrez vos modifications.

8. Créez une tâche d'installation à distance. Dans les propriétés de la tâche, sélectionnez le paquet d'installation que vous avez créé.

EDR Agent est alors installé sur l'ordinateur de l'utilisateur. Vous pouvez utiliser l'interface de l'application, et une icône de l'application s'affiche dans la zone de notification .

Dans Kaspersky Security Center, l'ordinateur sur lequel l'application est installée dans la configuration d'EDR Agent présente l'état *Critique* – . L'ordinateur présente cet état parce que le module Protection contre les fichiers malicieux est manquant. Aucune action n'est requise de votre part.

Si vous ne parvenez pas à installer EDR Agent sur un ordinateur disposant d'une application PPE tierce parce que le programme d'installation a détecté un logiciel incompatible sur l'ordinateur, vous pouvez ignorer la vérification des logiciels incompatibles.



Fenêtre principale d'EDR Agent

Vous devez maintenant configurer l'intégration avec la solution Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) ou Kaspersky Anti Targeted Attack (NDR). Vous pouvez également définir les paramètres avancés de l'application et, par exemple, créer une zone de confiance ou masquer l'interface de l'application. Les paramètres des sections suivantes sont disponibles :

- Kaspersky Security Network
- Paramètres de l'application
- Paramètres du réseau
- Exclusions
- Rapports

- Interface
- Administration des paramètres

Intégration d'EDR Agent avec MDR

EDR Agent est installé sur les postes de travail et les serveurs de l'infrastructure informatique de l'organisation. EDR Agent traite les données et les envoie via les flux de Kaspersky Security Network à Kaspersky Managed Detection and Response.

Pour que Kaspersky Managed Detection and Response fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*. Kaspersky Managed Detection and Response vous invite à établir une connexion d'arrière-plan lorsque vous déployez la solution. Confirmez que la connexion d'arrière-plan existe.

Établissement d'une connexion en arrière-plan dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Intégration**.
2. Passez à la section **Intégration**.
3. Activez le commutateur **Connexion en arrière-plan pour l'intégration Activé**.
4. Enregistrez vos modifications.

L'intégration avec Kaspersky Managed Detection and Response comprend les étapes suivantes :

1. **Installation du module Managed Detection and Response**

   Vous pouvez sélectionner le module MDR lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   > Pour installer le module Managed Detection and Response sans redémarrer l'ordinateur à l'aide de la tâche *Modification de la sélection des modules de l'application*, vous devez désactiver l'option **Vérifier la présence d'applications incompatibles d'éditeurs tiers** dans les paramètres de la tâche.

2. **Configuration de Kaspersky Private Security Network**

   > Passez cette étape si vous utilisez Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configure automatiquement Kaspersky Private Security Network lors de l'installation du plug-in MDR.

   Kaspersky Private Security Network (KPSN) 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.

   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 à propos de la configuration de Kaspersky Private Security Network, veuillez consulter 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 Kaspersky Private Security Network 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 fichier exécutable de Kaspersky Endpoint Security.

3. Exécutez la commande:

```
avp.com KSN /private <file name>
```

où `<file name>` est le nom du fichier de configuration contenant les paramètres de Kaspersky Private Security Network (format de fichier PKCS7 ou PEM).

Exemple :
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

En conséquence, Kaspersky Endpoint Security utilisera Kaspersky Private Security Network pour déterminer la réputation des fichiers, des applications et des sites Internet. La section **Kaspersky Security Network** des paramètres de stratégie affichera l'état de fonctionnement suivant : *Infrastructure : Kaspersky Private Security Network*.

Vous devez activer le mode KSN étendu pour que Managed Detection and Response puisse fonctionner.

3 **Activation de Kaspersky Managed Detection and Response**

À compter de Kaspersky Endpoint Security for Windows 12.10, pour activer la fonctionnalité Managed Detection and Response, comme alternative à un code d'activation, vous pouvez également utiliser un fichier clé.

Vous devez acheter une licence distincte pour MDR (module complémentaire de Kaspersky Managed Detection and Response).

La fonctionnalité devient disponible après l'ajout d'une clé distincte pour le module complémentaire Kaspersky Managed Detection and Response. La licence pour la fonctionnalité autonome Managed Detection and Response est la même que celle de Kaspersky Endpoint Security.

Assurez-vous que la fonctionnalité MDR est incluse dans la licence et qu'elle fonctionne dans l'interface locale de l'application.

4 **Activation du 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'ID du client et des informations sur la licence de 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 l'aide de Kaspersky Managed Detection and Response.

À compter de Kaspersky Endpoint Security 12.6 for Windows, l'ajout d'un fichier BLOB est facultatif pour Kaspersky Managed Detection and Response sans abonnement si vous disposez d'une licence en cours.

Comment activer le module Managed Detection and Response dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.

4. Cochez la case **Managed Detection and Response (Industrial CyberSecurity)**.

5. Dans le groupe **Paramètres**, cliquez sur **Charger** et sélectionnez le fichier BLOB reçu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.

   Par défaut, l'utilisateur est autorisé à gérer les paramètres de l'application (« le cadenas » est ouvert). Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

6. Enregistrez vos modifications.

Comment activer le module Managed Detection and Response dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Managed Detection and Response**.

5. Activez le commutateur **Managed Detection and Response ACTIVÉ**.

6. Cliquez sur **Charger** et sélectionnez le fichier BLOB qui a été obtenu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.

   Par défaut, l'utilisateur est autorisé à gérer les paramètres de la stratégie (« le cadenas » est ouvert). Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

7. Enregistrez vos modifications.

Comment activer le 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 fichier exécutable de Kaspersky Endpoint Security.

3. Exécutez la commande:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Configurer les paramètres de l'application**.

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 téléchargera 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.

5. **Configuration de l'octroi de télémétries à d'autres modules de l'application**

   Vous devez activer les modules suivants pour que Managed Detection and Response puisse fonctionner :

   - Kaspersky Security Network (mode élargi).
   - Détection comportementale.
   - Protection contre les Exploits.
   - Protection contre les menaces Internet.
   - Protection contre les menaces par emails.
   - Protection contre les fichiers malicieux.
   - Protection contre les menaces réseau.
   - Pare-feu.
   - Protection AMSI.
   - Analyse en arrière-plan.

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.
   4. Passez à la section **Configuration des agents intégrés** → **Managed Detection and Response**.
   5. Activez le commutateur **Managed Detection and Response ACTIVÉ**.
   6. Enregistrez vos modifications.

   1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
   2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
   3. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
   4. Cochez la case **Managed Detection and Response (Industrial CyberSecurity)**.
   5. Enregistrez vos modifications.

Intégration d'EDR Agent avec EDR (KATA)

EDR Agent est installé sur les postes de travail et les serveurs de l'infrastructure informatique de l'organisation. Sur ces ordinateurs, EDR Agent surveille en permanence les processus, les connexions réseau ouvertes et les fichiers en cours de modification, et envoie les données de surveillance au serveur avec le module Central Node.

Pour intégrer EDR (KATA), vous devez activer le module Endpoint Detection and Response (KATA) et configurer EDR Agent.

Les conditions suivantes doivent être remplies pour que Endpoint Detection and Response (KATA) fonctionne :

- Kaspersky Anti Targeted Attack Platform 5.0–7.1.
- Kaspersky Security Center version 14.2 ou toute version ultérieure. Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonctionnalité Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

L'intégration avec Endpoint Detection and Response (KATA) comprend les étapes suivantes :

1. **Activation du module Endpoint Detection and Response (KATA)**

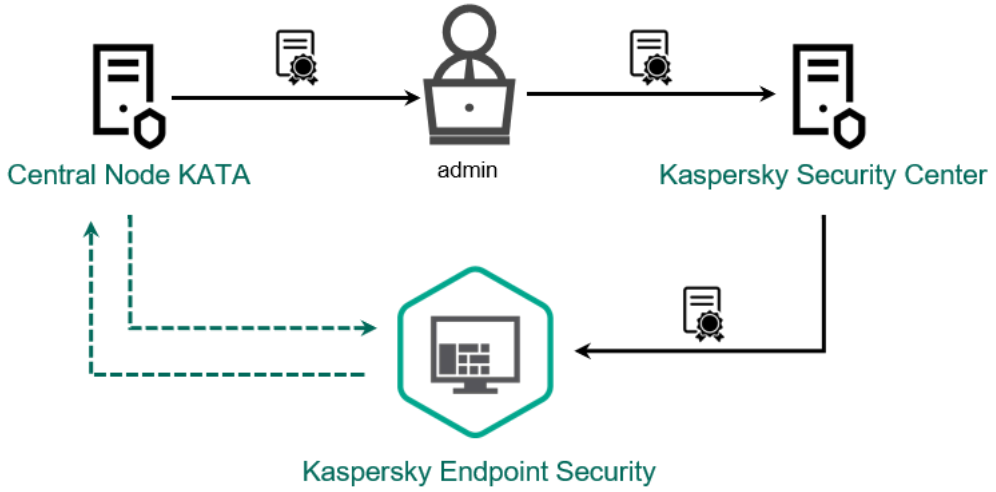
   Vous devez acheter une licence distincte pour EDR (KATA) (module complémentaire de Kaspersky Endpoint Detection and Response (KATA)).

   La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response (KATA). La licence de la fonctionnalité autonome Endpoint Detection and Response (KATA) est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité EDR (KATA) est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

2. **Connexion au module Central Node**

Kaspersky Anti Targeted Attack Platform requiert l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le module Central Node. Pour configurer une connexion sécurisée, vous devez utiliser un certificat TLS. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).



Ajouter un certificat TLS à Kaspersky Endpoint Security

Par défaut, Kaspersky Endpoint Security vérifie uniquement le certificat TLS du module Central Node. Pour rendre la connexion plus sécurisée, vous pouvez en outre activer la vérification de l'ordinateur sur le module Central Node (authentification bidirectionnelle). Pour activer cette vérification, vous devez activer l'authentification bidirectionnelle dans les paramètres du module Central Node et de Kaspersky Endpoint Security. Pour utiliser l'authentification bidirectionnelle, vous aurez également besoin d'un conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Endpoint Detection and Response Expert (on-premises)**.
5. Cochez la case **Endpoint Detection and Response Expert (on-premises)**.
6. Cliquez sur **Paramètres de connexion au serveur**.
7. Configurez la connexion au serveur :
   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.
   - **Certificat TLS du serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

- **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

  Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

8. Cliquez sur **OK**.

9. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

   Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

10. En cas de nécessité, configurez la télémétrie.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.

5. Activez le commutateur **Endpoint Detection and Response Expert (on-premises) ACTIVÉ**.

6. Pour configurer EDR (KATA), sélectionnez **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** dans la liste des solutions.

7. Cliquez sur **Paramètres de connexion**.

8. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.

   - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

- **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

  Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

9. Cliquez sur **OK**.

10. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

    Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

11. En cas de nécessité, configurez la télémétrie.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Par conséquent, l'ordinateur est ajouté à la console Kaspersky Anti Targeted Attack Platform. 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 **Endpoint Detection and Response Expert (on-premises)** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Intégration d'EDR Agent avec NDR (KATA)

EDR Agent est installé sur les postes de travail et les serveurs de l'infrastructure informatique de l'organisation. Sur ces ordinateurs, EDR Agent surveille en permanence les processus, les connexions réseau ouvertes et les fichiers en cours de modification, et envoie les données de surveillance au serveur avec le module Central Node.

Pour intégrer NDR (KATA), vous devez activer le module Network Detection and Response (KATA) et configurer EDR Agent.

Les conditions suivantes doivent être remplies pour que Network Detection and Response (KATA) fonctionne :

- Kaspersky Anti Targeted Attack Platform version 7.0 ou toute version ultérieure.
- Kaspersky Security Center version 14.2 ou toute version ultérieure. Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonctionnalité Network Detection and Response (KATA).

https://www.youtube.com/watch?v=gd-rySv0ThQ

L'intégration avec Network Detection and Response (KATA) comprend les étapes suivantes :

1. **Activation du module Network Detection and Response (KATA)**

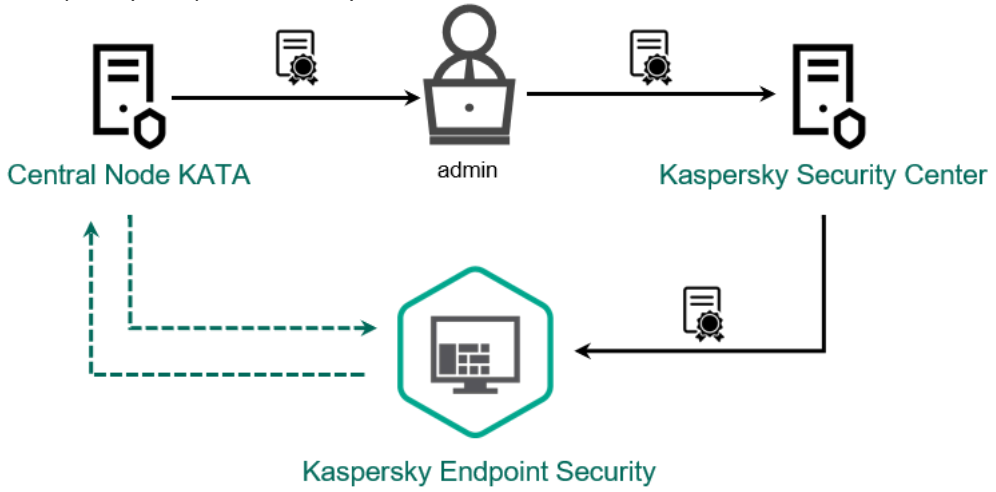
   Vous devez acheter une licence distincte pour NDR (KATA) (module complémentaire de Kaspersky Network Detection and Response (KATA)).

   La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Network Detection and Response (KATA). La licence de la fonctionnalité autonome Network Detection and Response (KATA) est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité NDR (KATA) est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

2. **Connexion au module Central Node**

   Kaspersky Anti Targeted Attack Platform requiert l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le module Central Node. Pour configurer une connexion sécurisée, vous devez utiliser un certificat TLS. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).



Ajouter un certificat TLS à Kaspersky Endpoint Security

Par défaut, Kaspersky Endpoint Security vérifie uniquement le certificat TLS du module Central Node. Pour rendre la connexion plus sécurisée, vous pouvez en outre activer la vérification de l'ordinateur sur le module Central Node (authentification bidirectionnelle). Pour activer cette vérification, vous devez activer l'authentification bidirectionnelle dans les paramètres du module Central Node et de Kaspersky Endpoint Security. Pour utiliser l'authentification bidirectionnelle, vous aurez également besoin d'un conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Network Detection and Response (KATA)**.

4. Cochez la case **Network Detection and Response (KATA)**.

5. Cliquez sur **Paramètres de connexion**.

6. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.

   - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

     Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

7. Cliquez sur **OK**.

8. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

9. Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

10. En cas de nécessité, configurez la télémétrie.

11. Enregistrez vos modifications.

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Network Detection and Response (KATA)**.

5. Activez le commutateur **Network Detection and Response (KATA) ACTIVÉ**.

6. Cliquez sur **Paramètres de connexion**.

7. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.

   - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

     Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

8. Cliquez sur **OK**.

9. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

10. Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

11. En cas de nécessité, configurez la télémétrie.

12. Enregistrez vos modifications.

Par conséquent, l'ordinateur est ajouté à la console Kaspersky Anti Targeted Attack Platform. 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 **Network Detection and Response (KATA)** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Intégration d'EDR Agent avec EDR Expert (on-premises)

EDR Agent est installé sur les postes de travail et les serveurs de l'infrastructure informatique de l'organisation. Sur ces ordinateurs, EDR Agent surveille en permanence les processus, les connexions réseau ouvertes et les fichiers en cours de modification, et envoie les données de surveillance au serveur EDR Expert (on-premises).

Pour intégrer EDR Expert (on-premises), vous devez activer le module Endpoint Detection and Response Expert (on-premises) et configurer EDR Agent.

L'intégration avec Endpoint Detection and Response Expert (on-premises) comprend les étapes suivantes :

1. **Activation de Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Vous devez acheter une licence distincte pour EDR Expert (on-premises) (module complémentaire de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response Expert (on-premises). La licence de la fonctionnalité autonome Endpoint Detection and Response Expert (on-premises) est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité EDR Expert (on-premises) est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

2. **Connexion au serveur de collecte de données télémétriques et au serveur de réponse**

   Kaspersky Endpoint Detection and Response Expert (on-premises) nécessite une connexion de confiance entre Kaspersky Endpoint Security et deux serveurs :

   - Un *serveur de collection de télémétrie* est un serveur qui fait partie d'une solution SIEM et qui collecte, normalise, corrèle, analyse et stocke les informations relatives aux événements qui se produisent sur l'ordinateur.

   - Un *serveur de réponse* est un serveur pour la réception et l'analyse des données, l'étude du comportement d'objets et la publication des résultats.

   Pour configurer une connexion sécurisée, vous devez utiliser un certificat TLS. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).

   Par défaut, Kaspersky Endpoint Security vérifie uniquement le certificat TLS des serveurs. Pour rendre la connexion plus sécurisée, vous pouvez en outre activer la vérification de l'ordinateur sur le serveur (authentification bidirectionnelle). Pour activer cette vérification, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur et de Kaspersky Endpoint Security. Pour utiliser l'authentification bidirectionnelle, vous aurez également besoin d'un conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

Comment connecter un ordinateur Kaspersky Endpoint Security au module EDR Expert (on-premises) à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.

5. Activez le commutateur **Endpoint Detection and Response Expert (on-premises) ACTIVÉ**.

6. Pour configurer EDR Expert (on-premises), sélectionnez **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)** dans la liste des solutions.

7. Configurez la connexion au *serveur de collecte de données télémétriques* :

   a. Dans le groupe **Connexion aux serveurs de collecte de données télémétriques**, cliquez sur le lien **Paramètres de connexion**.

   b. Configurez la connexion au serveur de collecte de données télémétriques :

      - **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.

      - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe.

        Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   c. Cliquez sur **OK**.

d. Ajoutez des serveurs de collecte de données télémétriques. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

   Vous pouvez ajouter plusieurs adresses de serveur de collecte de données télémétriques. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

e. En cas de nécessité, configurez la télémétrie.

8. Configurez la connexion des *serveurs de réponse* :

   a. Configurez le paramètre **Envoyer une demande de synchronisation au serveur toutes les (min.)** dans le groupe **Connexion aux serveurs de réponse**. Fréquence des requêtes de synchronisation envoyées au serveur. Pendant la synchronisation, Kaspersky Endpoint Security reçoit les tâches de réponse aux menaces et envoie les résultats des tâches.

   b. Cliquez sur le lien **Paramètres de connexion**.

   c. Configurez la connexion des serveurs de réponse :

      - **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.

      - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe.

        Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   d. Cliquez sur **OK**.

   e. Ajoutez des serveurs de réponse. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

      Vous pouvez ajouter plusieurs adresses de serveur de réponse. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Par conséquent, l'ordinateur est ajouté à la plateforme Open Single Management Platform (OSMP). 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 **Endpoint Detection and Response Expert (on-premises)** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Compatibilité avec les applications PPE tierces

EDR Agent prend en charge les fonctionnalités des solutions Kaspersky Detection and Response. Les modules de protection et de contrôle ne sont pas disponibles pour EDR Agent. Cette configuration permet d'installer des applications PPE tierces et de déployer les solutions Kaspersky Detection and Response dans l'infrastructure de l'organisation.

EDR Agent est compatible avec les applications PPE des fournisseurs suivants :

- **Dr.Web**

  EDR Agent est compatible avec Dr.Web Agent pour Windows version 13 et Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent est compatible avec la version 843.2 de Dallas Lock 8.0-C.

  Pour qu'EDR Agent s'exécute sur un ordinateur sur lequel le logiciel Dallas Lock est installé, vous devez autoriser la connexion aux services externes de Kaspersky dans les paramètres du module Pare-feu.

- **Secret Net Studio**

  EDR Agent est compatible avec la version 8.11 (20851) de Secret Net Studio.

  L'application ne peut pas être installée sur un ordinateur où Secret Net Studio est déployé avec le module Antivirus. Pour rendre l'interopérabilité possible, vous devez supprimer le module Antivirus de Secret Net Studio.

- **Trend Micro**

  EDR Agent est compatible avec Trend Micro Vision One (y compris Security Agent version 14.0.20731).

  EDR Agent est compatible avec Trend Micro Deep Security version 20.0.3-18160 (y compris Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent est compatible avec Sophos Intercept X version 2024.1.2 (y compris Endpoint Agent) et avec Sophos Core Agent version 2026.2.1.3.

- **Bitdefender**

  EDR Agent est compatible avec la version 8.26.7.647 de Bitdefender Endpoint Security Tools.

- **ESET**

  EDR Agent est compatible avec ESET Endpoint Security version 13.0.2044.0 et avec ESET Management Agent version 13.2.1189.0.

Sur les ordinateurs exécutant Windows 11 pour Arm64, EDR Agent n'est pas compatible avec Bitdefender Endpoint Security Tools.

Les applications doivent être installées dans l'ordre suivant : installez d'abord l'application PPE, puis l'Agent d'administration de Kaspersky Security Center et enfin EDR Agent. Cette procédure est nécessaire parce que le programme d'installation de l'application PPE pourrait détecter EDR Agent et l'Agent d'administration comme logiciels incompatibles et les supprimer. Le fonctionnement d'EDR Agent et de l'Agent d'administration doit également être vérifié après la mise à jour de l'application PPE tierce parce que son programme d'installation risque d'analyser de nouveau l'ordinateur à la recherche de logiciels incompatibles et supprimer les applications.

Si vous ne parvenez pas à installer EDR Agent sur un ordinateur disposant d'une application PPE tierce parce que le programme d'installation a détecté un logiciel incompatible sur l'ordinateur, vous pouvez ignorer la vérification des logiciels incompatibles.

Managed Detection and Response

Kaspersky Endpoint Security for Windows prend en charge l'intégration avec la solution Managed Detection and Response. La solution *Kaspersky Managed Detection and Response (MDR)* détecte et analyse automatiquement les incidents de sécurité dans votre infrastructure. Pour ce faire, MDR utilise les données de télémétrie reçues des terminaux et Machine learning. MDR envoie les données de l'incident aux experts de Kaspersky. Les experts peuvent alors traiter l'incident et, par exemple, ajouter une nouvelle entrée dans les bases antivirus. Les experts peuvent également émettre des recommandations sur le traitement de l'incident et, par exemple, suggérer d'isoler l'ordinateur du réseau. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Managed Detection and Response.

Configurations de Kaspersky Endpoint Security pour l'intégration avec MDR

Les configurations suivantes peuvent être appliquées pour utiliser MDR :

- **[KES+agent intégré]**. Dans cette configuration, Kaspersky Endpoint Security agit à la fois comme une application assurant la sécurité de l'ordinateur et comme une application permettant d'utiliser MDR.

- **[PPE tierce+EDR Agent]**. Dans cette configuration, la sécurité de l'infrastructure informatique est assurée par la plateforme de protection des terminaux (PPE) tierce. L'interaction avec MDR est assurée par Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent (EDR Agent). Dans cette configuration, EDR Agent est compatible avec les applications PPE tierces.

Intégration de l'agent intégré avec MDR

Pour configurer l'intégration avec Kaspersky Managed Detection and Response, vous devez activer le module Managed Detection and Response et configurer Kaspersky Endpoint Security.

Pour que Kaspersky Managed Detection and Response fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*. Kaspersky Managed Detection and Response vous invite à établir une connexion d'arrière-plan lorsque vous déployez la solution. Confirmez que la connexion d'arrière-plan existe.

Établissement d'une connexion en arrière-plan dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Intégration**.
2. Passez à la section **Intégration**.
3. Activez le commutateur **Connexion en arrière-plan pour l'intégration Activé**.
4. Enregistrez vos modifications.

L'intégration avec Kaspersky Managed Detection and Response comprend les étapes suivantes :

1. **Installation du module Managed Detection and Response**

   Vous pouvez sélectionner le module MDR lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   > Pour installer le module Managed Detection and Response sans redémarrer l'ordinateur à l'aide de la tâche *Modification de la sélection des modules de l'application*, vous devez désactiver l'option **Vérifier la présence d'applications incompatibles d'éditeurs tiers** dans les paramètres de la tâche.

2. **Configuration de Kaspersky Private Security Network**

   > Passez cette étape si vous utilisez Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configure automatiquement Kaspersky Private Security Network lors de l'installation du plug-in MDR.

   Kaspersky Private Security Network (KPSN) 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.

   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 à propos de la configuration de Kaspersky Private Security Network, veuillez consulter 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 Kaspersky Private Security Network 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 fichier exécutable de Kaspersky Endpoint Security.
   3. Exécutez la commande:

      ```
      avp.com KSN /private <file name>
      ```

où `<file name>` est le nom du fichier de configuration contenant les paramètres de Kaspersky Private Security Network (format de fichier PKCS7 ou PEM).

Exemple :
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

En conséquence, Kaspersky Endpoint Security utilisera Kaspersky Private Security Network pour déterminer la réputation des fichiers, des applications et des sites Internet. La section **Kaspersky Security Network** des paramètres de stratégie affichera l'état de fonctionnement suivant : *Infrastructure : Kaspersky Private Security Network*.

Vous devez activer le mode KSN étendu pour que Managed Detection and Response puisse fonctionner.

3 Activation de Kaspersky Managed Detection and Response

À compter de Kaspersky Endpoint Security for Windows 12.10, pour activer la fonctionnalité Managed Detection and Response, comme alternative à un code d'activation, vous pouvez également utiliser un fichier clé.

Kaspersky Managed Detection and Response prend en charge les méthodes de licence suivantes :

- La fonctionnalité Managed Detection and Response est couverte par la licence de Kaspersky Endpoint Security for Windows.

  La fonction est disponible immédiatement après l'activation de Kaspersky Endpoint Security for Windows.

- Une licence distincte pour MDR (module complémentaire de Kaspersky Managed Detection and Response) est utilisée.

  La fonctionnalité devient disponible après l'ajout d'une clé distincte pour le module complémentaire Kaspersky Managed Detection and Response. Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour Kaspersky Managed Detection and Response.

  La licence pour la fonctionnalité autonome Managed Detection and Response est la même que celle de Kaspersky Endpoint Security.

Assurez-vous que la fonctionnalité MDR est incluse dans la licence et qu'elle fonctionne dans l'interface locale de l'application.

4 Activation du 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'ID du client et des informations sur la licence de 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 l'aide de Kaspersky Managed Detection and Response.

À compter de Kaspersky Endpoint Security 12.6 for Windows, l'ajout d'un fichier BLOB est facultatif pour Kaspersky Managed Detection and Response sans abonnement si vous disposez d'une licence en cours.

Comment activer le module Managed Detection and Response dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.

4. Cochez la case **Managed Detection and Response (Industrial CyberSecurity)**.

5. Dans le groupe **Paramètres**, cliquez sur **Charger** et sélectionnez le fichier BLOB reçu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.

   Par défaut, l'utilisateur est autorisé à gérer les paramètres de l'application (« le cadenas » est ouvert 🔓). Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas 🔒.

6. Enregistrez vos modifications.

Comment activer le module Managed Detection and Response dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Managed Detection and Response**.

5. Activez le commutateur **Managed Detection and Response ACTIVÉ**.

6. Cliquez sur **Charger** et sélectionnez le fichier BLOB qui a été obtenu dans Kaspersky Managed Detection and Response Console. Le fichier présente l'extension P7.

   Par défaut, l'utilisateur est autorisé à gérer les paramètres de la stratégie (« le cadenas » est ouvert 🔓). Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas 🔒.

7. Enregistrez vos modifications.

Comment activer le 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 fichier exécutable de Kaspersky Endpoint Security.

3. Exécutez la commande:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Configurer les paramètres de l'application**.

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 téléchargera 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.

5. **Configuration de l'octroi de télémétries à d'autres modules de l'application**

   Vous devez activer les modules suivants pour que Managed Detection and Response puisse fonctionner :

   - Kaspersky Security Network (mode élargi).
   - Détection comportementale.
   - Protection contre les Exploits.
   - Protection contre les menaces Internet.
   - Protection contre les menaces par emails.
   - Protection contre les fichiers malicieux.
   - Protection contre les menaces réseau.
   - Pare-feu.
   - Protection AMSI.
   - Analyse en arrière-plan.

     1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
     2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

        La fenêtre des propriétés de la stratégie s'ouvre.
     3. Sélectionnez l'onglet **Paramètres de l'application**.
     4. Passez à la section **Configuration des agents intégrés** → **Managed Detection and Response**.
     5. Activez le commutateur **Managed Detection and Response ACTIVÉ**.
     6. Enregistrez vos modifications.

     1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
     2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
     3. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
     4. Cochez la case **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Enregistrez vos modifications.

Guide de migration KEA vers KES pour MDR

Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Managed Detection and Response. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser MDR. Toutes les fonctions de Kaspersky Endpoint Agent seront exécutées par Kaspersky Endpoint Security.

Lorsque vous déployez Kaspersky Endpoint Security sur des ordinateurs sur lesquels Kaspersky Endpoint Agent est installé, la solution Kaspersky Managed Detection and Response continuera à fonctionner avec Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur. Le même comportement dans le système se produira lors de la mise à jour de Kaspersky Endpoint Security vers la version 11.6.0 ou toute version ultérieure.

Kaspersky Endpoint Security n'est pas compatible avec Kaspersky Endpoint Agent. Vous ne pouvez pas installer ces deux applications sur le même ordinateur.

Les conditions suivantes doivent être remplies pour que Kaspersky Endpoint Security fonctionne dans le cadre de Kaspersky Managed Detection and Response :

- Kaspersky Security Center version 13.2 ou version ultérieure (y compris l'Agent d'administration). Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonctionnalité Managed Detection and Response.
- Une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie. Pour que MDR fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*.

Étapes de migration de la configuration [KES+KEA] vers [KES+agent intégré] pour MDR

1. **Mise à jour du plug-in d'administration de Kaspersky Endpoint Security**

   Le module MDR peut être géré à l'aide du plug-in d'administration de Kaspersky Endpoint Security version 11.6 ou version ultérieure. Selon le type de console Kaspersky Security Center que vous utilisez, mettez à jour le plug-in d'administration dans la Console d'administration (MMC) ou le plug-in Internet dans Web Console.

2. **Migration des stratégies et des tâches**

   Transférez les paramètres de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows. Les options suivantes existent :

   - Un Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security. L'Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security fonctionne uniquement dans Web Console

     Migration des paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security dans Web Console

     Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Migration depuis Kaspersky Endpoint Agent**.

     Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

Étape 1. Migration de stratégie

L'Assistant de migration crée une stratégie que fusionne les paramètres des stratégies de Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez fusionner les paramètres avec ceux de la stratégie de Kaspersky Endpoint Security. Cliquez sur une stratégie de Kaspersky Endpoint Agent pour sélectionner la stratégie Kaspersky Endpoint Security avec laquelle vous souhaitez fusionner les paramètres. Confirmez que vous avez sélectionné les bonnes stratégies, puis passez à l'étape suivante.

Étape 2. Migration d'une tâche

L'Assistant de migration ne prend pas en charge les tâches MDR. Ignorez cette étape.

Étape 3. Fin de l'Assistant

Quittez l'Assistant. À la suite de l'Assistant, une nouvelle stratégie de Kaspersky Endpoint Security sera créée. La stratégie fusionne les paramètres de Kaspersky Endpoint Security et Kaspersky Endpoint Agent La stratégie porte le nom *<Nom de stratégie de Kaspersky Endpoint Security> et <Nom de stratégie de Kaspersky Endpoint Agent>*. La nouvelle stratégie porte l'état *Inactive*. Pour continuer, changez l'état des stratégies de Kaspersky Endpoint Agent et Kaspersky Endpoint Security sur *Inactive* et activez la nouvelle stratégie fusionnée.

- Un Assistant standard de conversion de masse des stratégies et des tâches L'Assistant de conversion de masse des stratégies et des tâches est uniquement disponible dans la Console d'administration (MMC). Pour en savoir plus sur l'Assistant de conversion de masse des stratégies et des tâches, consultez l'aide de Kaspersky Security Center.

3. **Licence pour la fonctionnalité MDR**

   Pour activer Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Managed Detection and Response, vous avez besoin d'une licence distincte pour le module complémentaire Kaspersky Managed Detection and Response. Vous pouvez ajouter la clé à l'aide de la tâche *Ajout d'une clé*. En conséquence, deux clés seront ajoutées à l'application : *Kaspersky Endpoint Security* et *Kaspersky Managed Detection and Response*.

4. **Installation/Mise à jour de l'application Kaspersky Endpoint Security**

   Pour migrer la fonctionnalité MDR lors de l'installation ou de la mise à jour d'une application, il est recommandé d'utiliser la tâche d'installation à distance. Lors de la création d'une tâche d'installation à distance, vous devez sélectionner le module MDR dans les paramètres du paquet d'installation.

   Vous pouvez également mettre à jour l'application en utilisant les méthodes suivantes :

   - À l'aide du service de mise à jour de Kaspersky.
   - Localement à l'aide de l'Assistant d'installation de l'application.

   Kaspersky Endpoint Security prend en charge la sélection automatique des modules lors de la mise à jour de l'application sur un ordinateur sur lequel est installée l'application Kaspersky Endpoint Agent. La sélection automatique des modules dépend des autorisations du compte utilisateur qui met à jour l'application.

Si vous mettez à jour Kaspersky Endpoint Security en utilisant le fichier EXE ou MSI sous le compte système (SYSTEM), Kaspersky Endpoint Security obtient l'accès aux licences valides des solutions Kaspersky. Par conséquent, si Kaspersky Endpoint Agent est installé et la solution MDR est activée sur l'ordinateur, le programme d'installation de Kaspersky Endpoint Security configure automatiquement l'ensemble des modules et sélectionne le module MDR. Cette opération fait passer Kaspersky Endpoint Security à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. L'exécution du programme d'installation MSI sous le compte système (SYSTEM) est généralement effectuée lors de la mise à jour via le service de mise à jour Kaspersky ou lors du déploiement d'un paquet d'installation via Kaspersky Security Center.

Si vous mettez à jour Kaspersky Endpoint Security à l'aide d'un fichier MSI sous un compte utilisateur non privilégié, Kaspersky Endpoint Security n'a pas accès aux licences valides des solutions Kaspersky. Dans ce cas, Kaspersky Endpoint Security sélectionne automatiquement les modules en fonction d'un ensemble de modules de Kaspersky Endpoint Agent. Après cela, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

Kaspersky Endpoint Security prend en charge la mise à jour sans redémarrage de l'ordinateur. Vous pouvez sélectionner le mode de mise à jour de l'application dans les propriétés de la stratégie.

5 **Vérification du fonctionnement de l'application**

Si après l'installation ou la mise à jour de l'application, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

- Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
- Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous d'avoir activé la fonctionnalité d'agent intégré.
- Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Optimum (ci-après également « EDR Optimum »). À partir de la version 11.8.0, Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Expert (ci-après également « EDR Expert »). *Kaspersky Endpoint Detection and Response* est une gamme de solutions destinées à protéger l'infrastructure informatique des entreprises contre les cybermenaces avancées. La fonctionnalité des solutions combine la détection automatique des menaces avec la capacité de réagir à ces menaces pour contrer les attaques avancées, notamment les nouveaux exploits, les ransomwares, les attaques sans fichier ainsi que les méthodes utilisant des outils système légitimes. EDR Expert offre davantage de fonctionnalités de surveillance et de réponse aux menaces que EDR Optimum. Pour en savoir plus à propos des solutions, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Outils de Threat Intelligence

Kaspersky Endpoint Detection and Response utilise les outils Threat Intelligence suivants :

- L'intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations concernant la réputation des fichiers et des adresses Internet.
- La base de données Kaspersky Threats.

- L'infrastructure du service Cloud Kaspersky Security Network (ci-après également appelé "KSN"), qui donne accès à des informations en temps réel sur la réputation des fichiers, des sites Internet et des logiciels à partir de la base de connaissances de Kaspersky. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de protection et réduit la possibilité de faux positifs.

- La technologie Cloud Sandbox qui vous permet d'exécuter des fichiers détectés dans un environnement isolé et de vérifier leur réputation.

Principe de fonctionnement de la solution

Kaspersky Endpoint Detection and Response passe en revue et analyse le développement des menaces et fournit au *personnel de sécurité* ou à l'*administrateur* les informations sur l'attaque potentielle qui sont nécessaires pour assurer une réponse rapide. Kaspersky Endpoint Detection and Response affiche les détails de l'alerte dans une nouvelle fenêtre. Une *alerte* est un événement dans l'infrastructure informatique de l'entreprise que l'application a identifié comme inhabituel ou suspect et qui peut présenter une menace de sécurité pour l'infrastructure informatique de l'entreprise. Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Prise en charge des versions précédentes de Kaspersky Endpoint Security

Si vous utilisez Kaspersky Endpoint Security 11.2.0-11.6.0 pour l'interopérabilité avec Kaspersky Endpoint Detection and Response Optimum, l'application comprend Kaspersky Endpoint Agent. Vous pouvez installer Kaspersky Endpoint Agent en même temps que Kaspersky Endpoint Security. Dans Kaspersky Endpoint Security 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution de Kaspersky Endpoint Security.

> La solution Kaspersky Endpoint Detection and Response Expert ne prend pas en charge l'interopérabilité avec Kaspersky Endpoint Agent. La solution Kaspersky Endpoint Detection and Response Expert utilise Kaspersky Endpoint Security avec agent intégré (version 11.8.0 et ultérieure).

Intégration de l'agent intégré avec EDR Optimum / EDR Expert

Pour configurer l'intégration avec Kaspersky Endpoint Detection and Response, vous devez activer le module Endpoint Detection and Response Optimum ou le module Endpoint Detection and Response Expert (cloud) et configurer Kaspersky Endpoint Security.

> Les modules Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises) ne sont pas compatibles entre eux.

Les conditions suivantes doivent être remplies pour que Endpoint Detection and Response fonctionne :

- Kaspersky Security Center version 13.2 ou toute version ultérieure. Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonctionnalité Endpoint Detection and Response.

- Plug-in de gestion Kaspersky Endpoint Detection and Response.

  À partir de la version 12.6 de Kaspersky Endpoint Security, l'affichage des détails de l'alerte a été déplacé du plug-in de gestion Kaspersky Endpoint Security vers le plug-in de gestion EDR. Le plug-in d'administration EDR est un plug-in unique conçu pour fonctionner avec des agents sous les systèmes d'exploitation Windows, Mac et Linux. Désormais, lorsque vous utiliserez EDR Optimum, vous aurez besoin du plug-in d'administration de Kaspersky Endpoint Security pour créer des tâches de réponse aux menaces et du plug-in d'administration EDR pour consulter les détails des alertes.

- Le module Endpoint Detection and Response Optimum faisant partie de Kaspersky Endpoint Security permet l'interaction avec la solution Kaspersky Endpoint Detection and Response Optimum 2.0. L'interaction avec la version 1.0 de Kaspersky Endpoint Detection and Response Optimum n'est pas prise en charge.

- EDR Optimum peut être géré dans Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console.

  EDR Expert peut être géré uniquement à l'aide de Kaspersky Security Center Cloud Console. Vous ne pouvez pas gérer cette fonctionnalité à l'aide de la Console d'administration (MMC).

- L'application est activée, et la fonctionnalité est couverte par la licence.

- Le module Endpoint Detection and Response est activé.

- Les modules de l'application dont dépend Endpoint Detection and Response sont activés et opérationnels. Endpoint Detection and Response dépend des modules suivants :

  - Protection contre les fichiers malicieux.
  - Protection contre les menaces Internet.
  - Protection contre les menaces par emails.
  - Protection contre les Exploits.
  - Détection comportementale.
  - Prévention des intrusions.
  - Réparation des actions malicieuses.
  - Contrôle évolutif des anomalies.

L'intégration avec Kaspersky Endpoint Detection and Response comprend les étapes suivantes :

1. **Installation des modules Endpoint Detection and Response**

   Vous pouvez sélectionner le module Endpoint Detection and Response Optimum ou Endpoint Detection and Response Expert (cloud) lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   Vous devez redémarrer votre ordinateur pour terminer la mise à jour de l'application avec les nouveaux modules.

2. **Activation de Kaspersky Endpoint Detection and Response**

   Vous pouvez acquérir une licence d'utilisation de Kaspersky Endpoint Detection and Response de l'une des manières suivantes :

   - La fonctionnalité Endpoint Detection and Response est incluse dans la licence de Kaspersky Endpoint Security for Windows.

     La fonction est disponible immédiatement après l'activation de Kaspersky Endpoint Security for Windows.

   - Achat d'une licence distincte pour EDR Optimum ou EDR Expert (module complémentaire de Kaspersky Endpoint Detection and Response).

     La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response. Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour Kaspersky Endpoint Detection and Response.

     La licence de la fonctionnalité autonome Endpoint Detection and Response est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité EDR Optimum ou EDR Expert est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

   Pour en savoir plus sur le Contrat de licence utilisateur final d'EDR Optimum, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

3. **Activation des modules Endpoint Detection and Response**

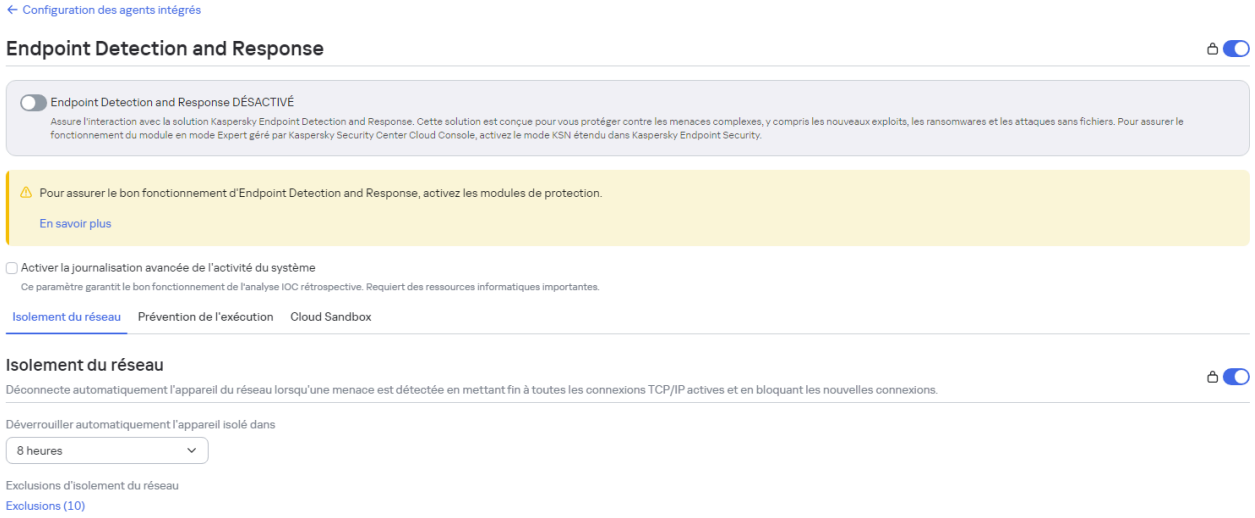
   Vous pouvez activer ou désactiver le module dans les paramètres de la stratégie de Kaspersky Endpoint Security for Windows.

   Procédure d'activation ou de désactivation du module Endpoint Detection and Response dans Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.
   4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
   5. Activez le commutateur **Endpoint Detection and Response ACTIVÉ**.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.



Paramètres d'intégration à EDR

Le module Kaspersky Endpoint Detection and Response est activé. 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 **Endpoint Detection and Response Optimum** ou **Endpoint Detection and Response Expert (cloud)** est ajouté à la liste des modules de Kaspersky Endpoint Security.

4 Activation du transfert de données au Serveur d'administration

Pour activer toutes les fonctionnalités d'Endpoint Detection and Response, le transfert doit être activé pour les types de données suivants :

- Données de fichiers de la quarantaine.

  Ces données sont requises pour obtenir des informations à propos des fichiers mis en quarantaine sur un ordinateur via Web Console. Par exemple, vous pouvez télécharger un fichier de la quarantaine pour l'analyser dans Web Console.

- Données de la chaîne de conception des menaces.

  Ces données sont requises pour obtenir des informations à propos des menaces détectées sur un ordinateur dans Web Console. Vous pouvez consulter les détails de l'alerte et prendre des mesures de réponse dans Web Console.

Comment activer le transfert de données vers le Serveur d'administration dans Web Console ?

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.
5. Dans le groupe **Transfert des données au Serveur d'administration**, cliquez sur le lien **Paramètres avancés**.

6. Dans la fenêtre qui s'ouvre, cochez les cases suivantes :

   - **À propos des fichiers de la Quarantaine**.
   - **À propos d'une chaîne de développement de menaces**.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Recherche d'indicateurs de compromission (tâche standard)

Un *indicateur de compromission (IOC)* est un ensemble de données concernant un objet ou une activité qui indique un accès non autorisé à l'ordinateur (compromission des données). Par exemple, de nombreuses tentatives infructueuses de se connecter au système peuvent constituer un indicateur de compromission. La tâche *Analyse IOC* permet de trouver des indicateurs de compromission sur l'ordinateur et de prendre des mesures de réponse aux menaces.

Kaspersky Endpoint Security recherche les indicateurs de compromission à l'aide des fichiers IOC. Les *fichiers IOC* sont des fichiers contenant les ensembles d'indicateurs que l'application tente de faire correspondre pour compter une détection. Les fichiers IOC doivent être conformes standard OpenIOC.

Mode d'exécution de la tâche Analyse IOC

Kaspersky Endpoint Detection and Response vous permet de créer des tâches standard d'analyse IOC pour détecter les données compromises. La *tâche standard d'analyse IOC* est une tâche de groupe ou locale qui est créée et configurée manuellement dans Web Console. Les tâches sont exécutées à l'aide de fichiers IOC préparés par l'utilisateur. Si vous souhaitez ajouter un indicateur de compromission manuellement, veuillez lire les exigences relatives aux fichiers IOC.

Le fichier que vous pouvez télécharger via le lien ci-dessous contient une table reprenant la liste complète des termes IOC de la norme OpenIOC.

DOWNLOAD THE IOC_TERMS.XLSX FILE

Kaspersky Endpoint Security prend également en charge les tâches autonomes d'analyse IOC lorsque l'application est utilisée dans le cadre de la solution Kaspersky Sandbox.

Création d'un fichier IOC

À compter de Kaspersky Endpoint Security 12.10 for Windows, vous pouvez créer des fichiers IOC directement dans les paramètres de la tâche. Pour créer un fichier IOC, vous devez préparer un fichier TXT avec une liste d'indicateurs de compromission. Vous pouvez ajouter des listes avec les objets suivants en tant qu'indicateurs de compromission :

- Hachages de fichier (MD5/SHA256).

  L'application prépare un fichier IOC avec une zone d'analyse FileItem/Md5sum ou FileItem/Sha256sum.

- Adresses IP (IPv4, IPv6).

  L'application prépare un fichier IOC avec une zone d'analyse PortItem/RemoteIP.

- Noms DNS.

  L'application prépare un fichier IOC avec une zone d'analyse DnsEntryItem/RecordName.

Comment créer un fichier IOC dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Sélectionnez la tâche **Analyse IOC**.

   La fenêtre des propriétés de la tâche s'ouvre. Si nécessaire, créez la tâche **Analyse IOC**.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Analyse des menaces**.

5. Cliquez sur **Redéfinir les fichiers IOC**.

6. Le formulaire de création du fichier IOC s'ouvre :

   a. Sous **Source des fichiers IOC**, sélectionnez **Générer à partir d'un fichier**.

   b. Saisissez le nom du fichier IOC.

   c. Sélectionnez un fichier TXT avec une liste d'indicateurs de compromission.

   d. Sélectionnez le type de fichier IOC : **Noms DNS**, **Hachages de fichiers**, **Adresses IP**.

   e. Cliquez sur **Charger**.

   Kaspersky Endpoint Security ajoute les fichiers IOC à la collection IOC. Le cas échéant, vous pouvez exclure temporairement les fichiers IOC de la zone d'action de la tâche.

7. Enregistrez vos modifications.

Création d'une tâche Analyse IOC

Vous pouvez créer des tâches *Analyse IOC* manuellement :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

- À l'aide de l'Assistant de création d'une tâche.

La tâche de groupe *Analyse IOC* ne peut pas être exécutée si l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou Kaspersky Endpoint Detection and Response Expert (cloud) est configurée sur les ordinateurs analysés. Dans ce cas, nous vous recommandons d'utiliser l'action de réponse *Analyse IOC* pour rechercher des indicateurs de compromission. Pour plus de détails, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.

Pour créer une tâche Analyse IOC, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Analyse IOC**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Passez à l'étape suivante.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

Le compte système (SYSTEM) n'a pas l'autorisation d'exécuter la tâche *Analyse IOC* sur les disques réseau. Si vous voulez exécuter la tâche pour un disque réseau, sélectionnez le compte d'un utilisateur qui a accès à ce disque.

Pour les tâches autonomes d'analyse IOC sur des disques réseau, dans les propriétés de la tâche, vous devez sélectionner manuellement dans les propriétés le compte utilisateur qui a accès à ce lecteur.

6. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Passez à la section **Analyse des menaces**.

10. Chargez les fichiers IOC pour rechercher des indicateurs de compromission.

    Une fois les fichiers IOC chargés, l'application affiche un résumé des informations relatives au fichier, y compris la liste des indicateurs qui n'ont pas réussi la vérification. Après avoir téléchargé les fichiers IOC, vous pouvez modifier les fichiers manuellement dans l'éditeur intégré directement dans les propriétés de la tâche. Kaspersky Endpoint Security prend en charge l'édition des fichiers IOC conformes à la norme OpenIOC 1.1. Il n'est pas possible de modifier le contenu des fichiers IOC conformes à OpenIOC version 1.0.

    Kaspersky Endpoint Security ajoute les fichiers IOC à la collection IOC. Le cas échéant, vous pouvez exclure temporairement les fichiers IOC de la zone d'action de la tâche.

    Il n'est pas recommandé d'ajouter ou de supprimer des fichiers IOC après l'exécution de la tâche. Cela peut entraîner un affichage incorrect des résultats de l'analyse IOC pour les exécutions précédentes de la tâche. Pour rechercher des indicateurs de compromission par nouveaux fichiers IOC, il est recommandé d'ajouter de nouvelles tâches.

11. Le cas échéant, cochez la case **Analyse IOC rétrospective**. *Analyse IOC rétrospective* est un mode de la tâche *Analyse IOC* dans laquelle Kaspersky Endpoint Security recherche des indicateurs de compromission à l'aide des données pendant une certaine période. Ce mode est destiné à la recherche d'indicateurs de compromission à partir des données de télémétrie de l'ordinateur protégé, telles que l'activité réseau, les processus, les fichiers et d'autres données télémétriques. Kaspersky Endpoint Security analyse les données contenues dans les journaux du système d'exploitation et les journaux du navigateur sur l'ordinateur. L'analyse IOC rétrospective analyse les journaux des navigateurs suivants : Google Chrome, Mozilla Firefox, Microsoft Edge (version 79 ou ultérieure).

12. Configurez les actions à effectuer en cas de détection d'IOC :

    - **Isoler l'appareil du réseau**. Si cette option est sélectionnée, Kaspersky Endpoint Security isole l'ordinateur du réseau afin d'empêcher la propagation de la menace. Vous pouvez configurer la durée de l'isolation dans les paramètres du module Endpoint Detection and Response.

      Si cette case est décochée, vous pouvez isoler l'ordinateur du réseau après avoir exécuté la tâche manuellement. Si la tâche *Analyse IOC* détecte un IOC, vous pouvez isoler l'ordinateur du réseau directement à partir de l'IOC (propriétés de la tâche *Analyse IOC* → **Paramètres de l'application** → **Résultats de l'analyse IOC**). Kaspersky Endpoint Security permet également de gérer immédiatement des paramètres supplémentaires : Période de désactivation de l'isolation du réseau et Exclusions d'isolation du réseau.

- **Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer l'objet, Kaspersky Endpoint Security crée une copie de sauvegarde au cas où l'objet devrait être restauré ultérieurement. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.

  Si cette case est décochée, vous pouvez mettre le fichier en quarantaine manuellement après avoir exécuté la tâche manuellement. Si la tâche *Analyse IOC* détecte un fichier qui peut compromettre les données, vous pouvez mettre ce fichier en quarantaine directement à partir des résultats de l'analyse IOC (**Paramètres de l'application** → **Résultats de l'analyse IOC**). Kaspersky Endpoint Security lance alors l'assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

  Si nécessaire, cochez la case **Appliquer aux objets critiques du système**. Les System Critical Object (SCO) incluent les fichiers nécessaires au fonctionnement du système d'exploitation.

  > Il est déconseillé d'appliquer des actions aux fichiers SCO. Cela peut rendre le système d'exploitation instable ou empêcher son démarrage.

- **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

13. Passez à la section **Avancé**.

14. Sélectionnez les types de données (documents IOC) qui doivent être analysés dans le cadre de la tâche.

    > Kaspersky Endpoint Security sélectionne automatiquement les types de données (documents IOC) pour la tâche *Analyse IOC* conformément au contenu des fichiers IOC chargés. Il est déconseillé de désélectionner les types de données.

    Vous pouvez également configurer les zone d'analyse pour les types de données suivants :

    - **Fichiers - FileItem**. Définissez une zone d'analyse IOC sur l'ordinateur à l'aide de zones prédéfinies.

      Par défaut, Kaspersky Endpoint Security recherche les IOC uniquement dans les zones importantes de l'ordinateur comme le dossier Téléchargements, le bureau, le dossier des fichiers temporaires du système d'exploitation, etc. Vous pouvez également ajouter manuellement la zone d'analyse.

    - **Journal des événements Windows – EventLogItem**. Saisissez la période pendant laquelle les événements ont été consignés. Vous pouvez également sélectionner les journaux des événements Windows à utiliser pour l'analyse IOC. Par défaut, les journaux des événements suivants sont sélectionnés : journal des événements des applications, journal des événements du système et journal des événements de sécurité.

      > Pour le terme IOC EventLogItem\source, utilisez la valeur **Nom du fournisseur** du schéma XML de l'événement.

    - **Registre Windows – RegistryItem**. Configurez la zone d'analyse IOC dans le registre.

      Par défaut, Kaspersky Endpoint Security analyse un ensemble de clés de registre.

15. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

16. Programmez l'exécution de la tâche.

> Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

17. Enregistrez vos modifications.

18. Cochez la case en regard de la tâche.

19. Cliquez sur **Démarrer**.

    Ainsi, Kaspersky Endpoint Security lance la recherche d'indicateurs de compromission sur l'ordinateur. Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats**. Vous pouvez consulter les informations relatives aux indicateurs de compromission détectés dans les propriétés de la tâche : **Paramètres de l'application** → **Résultats de l'analyse IOC**. Dans les résultats de l'analyse IOC, vous pouvez aussi manuellement mettre en quarantaine le fichier détecté ou isoler l'ordinateur du réseau.

Kaspersky Endpoint Security recherche les doublons parmi les enregistrements créés pour un même fichier IOC et ne conserve que les enregistrements uniques dans les résultats des tâches. Les doublons sont des enregistrements du même type qui ont les mêmes valeurs dans tous les champs comparés. Il se peut également que l'application ne crée pas d'enregistrement si une ou plusieurs zones ne contiennent pas de valeur (voir le tableau ci-dessous).

Type	Champs comparés	Condition de non-création d'enregistrement
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valeur manquante des champs FullPath, Md5sum et Sha256sum. • Valeur manquante du champ FullPath et valeur identique des champs Md5sum et Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valeur manquante pour au moins un des champs suivants : Hive, KeyPath et ValueName.
ProcessItem	• startTime • PID	Valeurs manquantes des champs startTime ou PID.

> La fenêtre **Détails de l'alerte** peut afficher des enregistrements RegistryItem avec des valeurs de champ identiques. Ces enregistrements ne sont pas des doublons, car ils ont des valeurs différentes dans le champ Texte, qui ne s'affiche pas dans l'interface.

> Les résultats de l'analyse IOC sont conservés pendant 30 jours. À l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens.

Télémétrie étendue pour l'analyse IOC

Nous recommandons d'activer la télémétrie étendue sur l'ordinateur pour analyser les IOC de manière rétrospective. La télémétrie étendue améliore la précision de la détection IOC, mais utilise plus de ressources de l'ordinateur.

La télémétrie étendue inclut la prise en charge des éléments supplémentaires suivants :

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Si la télémétrie étendue est désactivée, Kaspersky Endpoint Security peut alterner les informations relatives aux indicateurs de compromission détectés.

Pour activer la télémétrie étendue, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Cochez la case **Activer la journalisation avancée de l'activité du système**.
6. Enregistrez vos modifications.

Placer le fichier en quarantaine

Lors de la réaction aux menaces, Kaspersky Endpoint Detection and Response peut créer des tâches *Placer le fichier en Quarantaine*. Cette mesure est nécessaire pour minimiser les conséquences de la menace. La *Quarantaine* est un stockage local spécial sur l'ordinateur. L'utilisateur peut mettre en quarantaine les fichiers qu'il considère comme dangereux pour l'ordinateur. Les fichiers mis en quarantaine sont stockés dans un état chiffré et ne menacent pas la sécurité de l'appareil. Kaspersky Endpoint Security utilise la Quarantaine uniquement lorsqu'elle est intégrée aux solutions de détection et de réponse de Kaspersky. Dans d'autres cas, Kaspersky Endpoint Security place le fichier correspondant dans la Sauvegarde. Pour en savoir plus sur la gestion de la Quarantaine dans le cadre des solutions, veuillez consulter l'aide de Kaspersky Sandbox, l'aide de Kaspersky Endpoint Detection and Response Optimum, l'aide de Kaspersky Endpoint Detection and Response Expert, l'aide de Kaspersky Anti Targeted Attack Platform et l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

Vous pouvez créer des tâches *Placer le fichier en Quarantaine* de la manière suivante :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

- À l'aide de l'Assistant de création d'une tâche.

  Vous devez saisir le chemin d'accès au fichier ou le hash (SHA256 ou MD5), ou à la fois le chemin d'accès au fichier et le hash du fichier.

- Dans les paramètres de la tâche *Analyse IOC*.

  Si la tâche *Analyse IOC* détecte un fichier qui peut compromettre les données, vous pouvez mettre ce fichier en quarantaine directement à partir des résultats de l'analyse IOC (**Paramètres de l'application** → **Résultats de l'analyse IOC**). Kaspersky Endpoint Security lance alors l'Assistant de création de la tâche avec les données prédéfinies du fichier détecté. Il vous suffit de gérer les paramètres supplémentaires de la tâche, par exemple, configurer la planification de la tâche.

La tâche *Placer le fichier en Quarantaine* présente les limitations suivantes :

1. La taille du fichier ne doit pas dépasser 100 Mo.
2. Vous ne pouvez pas supprimer les fichiers nécessaires au fonctionnement de Kaspersky Endpoint Security for Windows :
   - Fichiers couverts par la technologie d'Autodéfense de Kaspersky Endpoint Security for Windows
   - Fichiers signés numériquement par Kaspersky
3. Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.
4. Vous ne pouvez pas analyser un objet mis en quarantaine à la suite de la tâche *Placer le fichier en Quarantaine*.

Pour créer une tâche Placer le fichier en Quarantaine, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Placer le fichier en Quarantaine**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Suivant**.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Cliquez sur **Suivant**.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Le cas échéant, cochez la case **Appliquer aux objets critiques du système**.

   Les System Critical Object (SCO) incluent les fichiers nécessaires au fonctionnement du système d'exploitation.

   Il est déconseillé d'appliquer des actions aux fichiers SCO. Cela peut rendre le système d'exploitation instable ou empêcher son démarrage.

10. Dans la liste des fichiers, cliquez sur **Ajouter**.

    L'Assistant d'ajout de fichiers démarre.

11. Pour ajouter le fichier, vous devez saisir le chemin d'accès complet au fichier ou le hachage du fichier ainsi que son chemin d'accès.

    Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

12. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

13. Programmez l'exécution de la tâche.

    Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

14. Enregistrez vos modifications.

15. Cochez la case en regard de la tâche.

16. Cliquez sur **Démarrer**.

Kaspersky Endpoint Security déplace alors des fichiers dans la Quarantaine.

Si le fichier est verrouillé par un autre processus, la tâche s'affiche comme Progression, mais le fichier lui-même n'est placé en quarantaine qu'après le redémarrage de l'ordinateur. Après avoir redémarré l'ordinateur, confirmez que le fichier est supprimé.

Si le fichier est verrouillé par un autre processus, la tâche s'affiche comme *Terminée*, mais le fichier lui-même n'est mis en quarantaine qu'après le redémarrage de l'ordinateur. Après avoir redémarré l'ordinateur, confirmez que le fichier est supprimé.

La tâche *Placer le fichier en Quarantaine* peut se terminer par l'erreur *Accès interdit* si vous essayez de mettre en quarantaine un fichier exécutable en cours d'exécution. Créez une tâche Terminer le processus pour le fichier et réessayez.

La tâche *Placer le fichier en Quarantaine* peut se terminer par l'erreur *Espace insuffisant dans le Stockage en ligne* si vous essayez de mettre en quarantaine un fichier trop volumineux. Videz la Quarantaine ou augmentez l'espace de la Quarantaine. Puis réessayez.

Vous pouvez restaurer un fichier de la Quarantaine ou vider la Quarantaine à l'aide de Web Console. Vous pouvez restaurer les objets localement sur l'ordinateur en utilisant la ligne de commande.

Obtenir le fichier

Vous pouvez obtenir des fichiers à partir des ordinateurs des utilisateurs. Par exemple, vous pouvez configurer l'obtention d'un fichier journal des événements créé par une application tierce. À la suite de l'exécution de la tâche, une copie du fichier est enregistrée dans la quarantaine. La *Quarantaine* est un stockage local spécial sur l'ordinateur. Vous pouvez télécharger ce fichier depuis la Quarantaine vers votre ordinateur à l'aide de Web Console (**Opérations** → **Stockages** → **Quarantaine**). Sur l'ordinateur de l'utilisateur, le fichier reste dans son dossier d'origine.

La taille du fichier ne doit pas dépasser 2 Go.

Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.

Pour créer une tâche Obtention du fichier, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Obtenir le fichier**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Suivant**.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Cliquez sur **Suivant**.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Dans la liste des fichiers, cliquez sur **Ajouter**.

   L'Assistant d'ajout de fichiers démarre.

10. Pour ajouter le fichier, vous devez saisir le chemin d'accès complet au fichier ou le hachage du fichier ainsi que son chemin d'accès.

    Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

    Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security crée une copie du fichier et la place dans la Quarantaine. Vous pouvez télécharger le fichier de la Quarantaine dans Web Console.

Supprimer le fichier

Vous pouvez supprimer des fichiers à distance à l'aide de la tâche *Supprimer le fichier*. Par exemple, vous pouvez supprimer à distance un fichier lorsque vous répondez à des menaces.

Vous ne pouvez pas supprimer les fichiers nécessaires au fonctionnement de Kaspersky Endpoint Security for Windows :

- Fichiers couverts par la technologie d'Autodéfense de Kaspersky Endpoint Security for Windows
- Fichiers signés numériquement par Kaspersky

Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.

Pour créer une tâche Supprimer le fichier, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Supprimer le fichier**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Suivant**.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Cliquez sur **Suivant**.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Pour ajouter le fichier, vous devez saisir le chemin d'accès complet au fichier ou le hachage du fichier ainsi que son chemin d'accès.

   Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

10. Le cas échéant, cochez la case **Appliquer aux objets critiques du système**.

    Les System Critical Object (SCO) incluent les fichiers nécessaires au fonctionnement du système d'exploitation.

    Il est déconseillé d'appliquer des actions aux fichiers SCO. Cela peut rendre le système d'exploitation instable ou empêcher son démarrage.

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

    Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security supprime alors le fichier de l'ordinateur. Si le fichier est verrouillé par un autre processus, la tâche s'affiche comme *Progression*, mais le fichier lui-même n'est supprimé qu'après le redémarrage de l'ordinateur. Après avoir redémarré l'ordinateur, confirmez que le fichier est supprimé.

La tâche *Supprimer le fichier* peut se terminer par l'erreur *Accès interdit ou fichier introuvable* si vous essayez de supprimer un fichier exécutable en cours d'exécution. Créez une tâche Terminer le processus pour le fichier et réessayez.

Démarrage du processus

Vous pouvez lancer des fichiers à distance à l'aide de la tâche *Démarrage du processus*. Par exemple, vous pouvez exécuter à distance un utilitaire qui crée le fichier de configuration de l'ordinateur. Ensuite, vous pouvez utiliser la tâche *Obtenir le fichier* pour recevoir le fichier créé dans Kaspersky Security Center Web Console.

Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.

Pour créer une tâche Démarrage du processus, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Démarrage du processus**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Suivant**.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Cliquez sur **Suivant**.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

8. La fenêtre des propriétés de la tâche s'ouvre.

9. Sélectionnez l'onglet **Paramètres de l'application**.

10. Saisissez la commande de démarrage du processus.

    Imaginons que vous souhaitiez exécuter un utilitaire `utility.exe`) qui enregistre les informations relatives à la configuration de l'ordinateur dans un fichier nommé `conf.txt`, dans le dossier actuel (par défaut). L'utilitaire se trouve dans le dossier `C:\Users\admin\Diagnostic\`. Il faut enregistrer le fichier de configuration dans le dossier `C:\Users\admin\Documents\Configuration`. Saisissez les valeurs suivantes :

    - **Commande exécutable** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Arguments de ligne de commande (facultatif)** – `/R conf.txt`
    - **Chemin d'accès au dossier de travail (facultatif)** – `C:\Users\admin\Documents\Configuration`

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

    Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

13. Enregistrez vos modifications.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

Kaspersky Endpoint Security exécute alors la commande en mode silencieux et lance le processus. Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats d'exécution**.

Terminer le processus

Vous pouvez mettre fin aux processus à distance à l'aide de la tâche *Fin du processus*. Par exemple, vous pouvez mettre fin à distance à un utilitaire de test de vitesse Internet qui a été lancé à l'aide de la tâche *Lancement du processus*.

Si vous souhaitez interdire l'exécution d'un fichier, vous pouvez configurer le module Prévention de l'exécution. Vous pouvez interdire l'exécution de fichiers exécutables, de scripts et de fichiers au format Office.

La tâche *Fin du processus* présente les limitations suivantes :

Vous ne pouvez pas arrêter les processus des fichiers nécessaires au fonctionnement de Kaspersky Endpoint Security for Windows :

- Fichiers couverts par la technologie d'Autodéfense de Kaspersky Endpoint Security for Windows
- Fichiers signés numériquement par Kaspersky

Vous pouvez configurer la tâche pour EDR Optimum dans Web Console et Cloud Console. Les paramètres des tâches pour EDR Expert sont disponibles uniquement dans Cloud Console.

Pour créer une tâche Fin du processus, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez **Kaspersky Endpoint Security for Windows 14.2**.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Fin du processus**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez 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 **Suivant**.

5. Saisissez les informations d'identification du compte de l'utilisateur dont vous souhaitez utiliser les droits pour exécuter la tâche. Cliquez sur **Suivant**.

   Par défaut, Kaspersky Endpoint Security lance la tâche en tant que compte utilisateur du système (SYSTEM).

6. Quittez l'Assistant en cliquant sur le bouton **Terminer**.

   La nouvelle tâche apparaît dans la liste des tâches.

7. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

8. Sélectionnez l'onglet **Paramètres de l'application**.

9. Le cas échéant, cochez la case **Appliquer aux objets critiques du système**.

   Les System Critical Object (SCO) incluent les fichiers nécessaires au fonctionnement du système d'exploitation.

   > Il est déconseillé d'appliquer des actions aux fichiers SCO. Cela peut rendre le système d'exploitation instable ou empêcher son démarrage.

10. Pour terminer le processus, vous devez sélectionner le fichier dont vous voulez arrêter le fonctionnement. Vous pouvez sélectionner un fichier d'une des manières suivantes :

    - Saisissez le nom complet du fichier.
    - Saisissez le hachage du fichier et le chemin d'accès au fichier.
    - Saisissez le PID du processus (uniquement pour les tâches locales).
    - Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

    > Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès au fichier contient une lettre de disque réseau, l'erreur suivante peut s'afficher : *Fichier introuvable*.

11. Dans la fenêtre des propriétés des tâches, sélectionnez l'onglet **Programmation**.

12. Programmez l'exécution de la tâche.

    > Wake-on-LAN n'est pas disponible pour cette tâche. Assurez-vous que l'ordinateur est allumé pour exécuter la tâche.

13. Cliquez sur **Enregistrer**.

14. Cochez la case en regard de la tâche.

15. Cliquez sur **Démarrer**.

    Kaspersky Endpoint Security arrête alors ce processus sur l'ordinateur. Si une application GAME est en cours d'exécution et que vous arrêtez le processus game.exe, l'application s'arrête sans enregistrer les données. Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats**.

Prévention de l'exécution

La prévention de l'exécution permet de gérer l'exécution de fichiers exécutables et de scripts, ainsi que d'ouvrir des fichiers au format Office. Vous pouvez ainsi, par exemple, empêcher l'exécution d'applications que vous considérez dangereuses. Cela permet d'arrêter la propagation de la menace. La prévention de l'exécution prend en charge un ensemble d'extensions de fichier Office et un ensemble d'interpréteurs de scripts.

Règle de prévention de l'exécution

La Prévention de l'exécution gère l'accès de l'utilisateur aux fichiers à l'aide de règles de prévention de l'exécution. La *règle de prévention de l'exécution* est un ensemble de critères que l'application prend en compte lorsqu'elle réagit à l'exécution d'un objet, par exemple lorsqu'elle bloque l'exécution d'un objet. L'application identifie les fichiers par leur chemin d'accès ou leurs sommes de contrôle calculées à l'aide des algorithmes de hachage MD5 et SHA256.

Vous pouvez créer des règles de prévention de l'exécution :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

- À l'aide d'une stratégie de groupe ou des paramètres locaux de l'application.

  Vous devez saisir le chemin d'accès au fichier ou son hash (SHA256 ou MD5), ou le chemin d'accès au dossier et le hash du fichier.

Vous pouvez également gérer la Prévention de l'exécution localement en utilisant la ligne de commande.

La prévention de l'exécution présente les restrictions suivantes :

1. Les règles de prévention ne couvrent pas les fichiers sur les cédéroms ou les images ISO. L'application ne bloque pas l'exécution ou l'ouverture de ces fichiers.

2. Vous ne pouvez pas appliquer de règle de prévention aux fichiers nécessaires au fonctionnement de Kaspersky Endpoint Security for Windows :

   - Fichiers couverts par la technologie d'Autodéfense de Kaspersky Endpoint Security for Windows

   - Fichiers signés numériquement par Kaspersky

3. Il n'est pas recommandé de créer plus de 5 000 règles de prévention de l'exécution, car cela peut entraîner une instabilité du système.

Modes de règles de prévention de l'exécution

Le module Prévention de l'exécution peut fonctionner selon deux modes :

- **Statistiques seulement**

  Dans ce mode, Kaspersky Endpoint Security publie un événement sur les tentatives d'exécution d'objets exécutables ou d'ouverture de documents qui correspondent aux critères de la règle de prévention dans le journal des événements Windows et dans Kaspersky Security Center, mais ne bloque pas la tentative d'exécution ni d'ouverture de l'objet ou du document. Ce mode est sélectionné par défaut.

- **Actif**

  Dans ce mode, l'application bloque l'exécution des objets ou l'ouverture des documents qui correspondent aux critères des règles de prévention. L'application publie également un événement sur les tentatives d'exécution d'objets ou d'ouverture de documents dans le journal des événements Windows et dans le journal des événements de Kaspersky Security Center.

Gestion de la prévention de l'exécution

Vous pouvez configurer les paramètres du module uniquement dans Web Console.

Pour prévenir l'exécution :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Sélectionnez l'onglet **Prévention de l'exécution**.
6. Activez le commutateur **Prévention de l'exécution ACTIVÉE**.
7. Dans le groupe **Action sur l'exécution ou l'ouverture d'un objet interdit**, sélectionnez le mode de fonctionnement du module :

   - **Bloquer et ajouter au journal des événements**. Dans ce mode, l'application bloque l'exécution des objets ou l'ouverture des documents qui correspondent aux critères des règles de prévention. L'application publie également un événement sur les tentatives d'exécution d'objets ou d'ouverture de documents dans le journal des événements Windows et dans le journal des événements de Kaspersky Security Center.

     Si nécessaire, cochez la case **Appliquer aux objets critiques du système**. Les System Critical Object (SCO) incluent les fichiers nécessaires au fonctionnement du système d'exploitation.

Il est déconseillé d'appliquer des actions aux fichiers SCO. Cela peut rendre le système d'exploitation instable ou empêcher son démarrage.

- **Ajouter au journal des événements**. Dans ce mode, Kaspersky Endpoint Security publie un événement sur les tentatives d'exécution d'objets exécutables ou d'ouverture de documents qui correspondent aux critères de la règle de prévention dans le journal des événements Windows et dans Kaspersky Security Center, mais ne bloque pas la tentative d'exécution ni d'ouverture de l'objet ou du document. Ce mode est sélectionné par défaut.

8. Créez une liste de règles de prévention de l'exécution :

   a. Cliquez sur **Ajouter**.

   b. Dans la fenêtre qui s'ouvre, saisissez le nom de la règle de prévention de l'exécution (par exemple *Application A*).

   c. Dans la liste déroulante **Type**, sélectionnez l'objet que vous souhaitez bloquer : **Fichier exécutable**, **Script**, **Document Microsoft Office**.

   Si vous sélectionnez le mauvais type d'objet, Kaspersky Endpoint Security ne bloque pas le fichier ou le script.

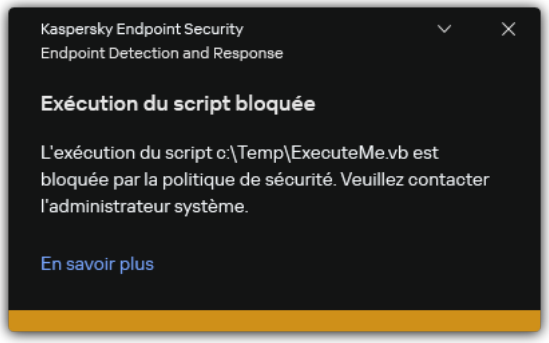
   d. Pour ajouter le fichier, vous devez saisir son hash (SHA256 ou MD5), son chemin d'accès complet, ou son hash et le chemin d'accès au dossier.

   Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier en commençant par `\\`, et non la lettre du disque. Par exemple, `\\server\shared_folder\file.exe`. Si le chemin d'accès contient une lettre de disque réseau, Kaspersky Endpoint Security ne bloque pas le fichier ou le script.

   La prévention de l'exécution prend en charge un ensemble d'extensions de fichier Office et un ensemble d'interpréteurs de scripts.

9. Enregistrez vos modifications.

Kaspersky Endpoint Security interdit alors l'exécution des objets : exécution de fichiers exécutables et de scripts, ouverture de fichiers au format Office. Vous pouvez toutefois ouvrir un fichier de script dans un éditeur de texte, même si l'exécution du script est interdite. Lors de l'interdiction de l'exécution d'un objet, Kaspersky Endpoint Security affiche une notification standard (cf. Illustration ci-dessous) si les notifications sont activées dans les paramètres des applications.



Notification de Prévention de l'exécution

Isolation du réseau pour l'ordinateur

L'isolation de l'ordinateur du réseau permet d'isoler l'ordinateur du réseau automatiquement à la suite d'une détection d'un indicateur de compromission (IOC) – il s'agit du *mode automatique*. Vous pouvez activer l'isolation du réseau manuellement pendant que vous enquêtez sur la menace détectée – il s'agit du *mode manuel*.

Lorsque l'isolation du réseau est activée, l'application coupe toutes les connexions actives et bloque toutes les nouvelles connexions réseau TCP/IP sur l'ordinateur, à l'exception des connexions suivantes :

- Les connexions indiquées dans Exclusions de l'isolation du réseau.
- Les connexions amorcées par les services de Kaspersky Endpoint Security.
- Les connexions amorcées par l'Agent d'administration de Kaspersky Security Center.
- Les connexions à la SVM et au Serveur d'intégration si l'application est utilisée en mode Light Agent.
- Les connexions à KSN lors de l'intégration de l'application à Kaspersky Managed Detection and Response.

Vous pouvez configurer les paramètres du module uniquement dans Web Console.

Mode d'isolation automatique du réseau

Vous pouvez configurer l'activation automatique de l'isolation du réseau suite à une détection IOC. Vous pouvez configurer le mode d'isolation automatique du réseau avec une stratégie de groupe.

Comment configurer l'activation automatique de l'isolation du réseau suite à une détection IOC

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Analyse IOC** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   Si nécessaire, créez la tâche *Analyse IOC*.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Paramètres de réponse**.

5. Dans le groupe **Configurez les actions de réponse en cas de détection IOC**, sélectionnez **Alerter et répondre**, puis cochez la case **Isoler l'appareil du réseau**.

6. Enregistrez vos modifications.

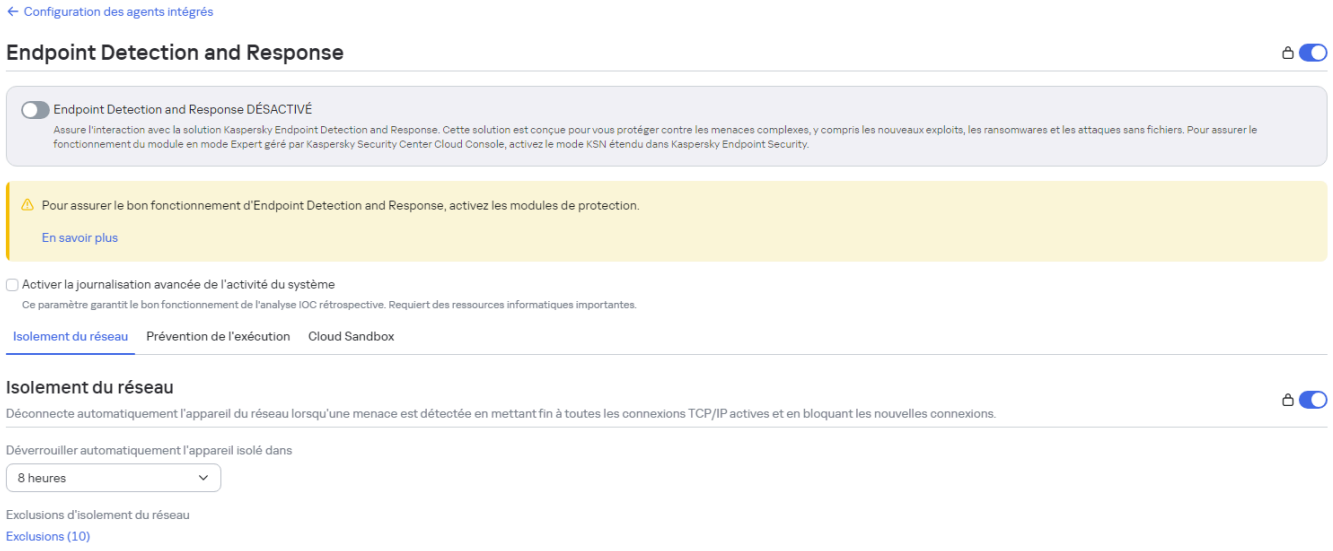
Ainsi, suite à une détection IOC, l'application isole l'ordinateur du réseau afin d'éviter la propagation de la menace.

Vous pouvez configurer la désactivation de l'isolement automatique du réseau après un certain temps. Par défaut, l'application désactiver l'isolation du réseau 8 heures après son activation. Vous pouvez également désactiver l'isolation du réseau manuellement (consultez les instructions ci-dessous). Quand l'isolation du réseau est désactivée, l'ordinateur peut utiliser le réseau sans restriction.

Comment configurer le délai de désactivation de l'isolation du réseau d'un ordinateur en mode automatique

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Sélectionnez l'onglet **Isolement du réseau**.
6. Sélectionnez le délai de désactivation de l'isolement du réseau.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.



Paramètres d'intégration à EDR

Mode d'isolation manuelle du réseau

Vous pouvez activer ou désactiver manuellement l'isolation du réseau. Vous pouvez configurer le mode d'isolation manuelle du réseau à l'aide des propriétés de l'ordinateur dans la console de Kaspersky Security Center.

Vous pouvez activer l'isolation du réseau :

- Dans les détails de l'alerte (uniquement pour EDR Optimum).

  Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

- Utilisation des paramètres locaux de l'application.
- Dans les paramètres de la tâche *Analyse IOC*.

  Si la tâche *Analyse IOC* détecte un IOC, vous pouvez isoler l'ordinateur du réseau directement à partir de l'IOC (propriétés de la tâche *Analyse IOC* → **Paramètres de l'application** → **Résultats de l'analyse IOC**). Kaspersky Endpoint Security permet également de gérer immédiatement des paramètres supplémentaires : Période de désactivation de l'isolation du réseau et Exclusions d'isolation du réseau.

Comment activer manuellement l'isolation du réseau d'un ordinateur

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
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. Sélectionnez l'onglet **Applications**.
4. Cliquez sur **Kaspersky Endpoint Security for Windows 14.2**.

   La fenêtre des paramètres locaux de l'application s'ouvre.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Passez à la section **Detection and Response** → **Endpoint Detection and Response**.
7. Dans le groupe **Isolement du réseau**, cliquez sur **Isoler l'ordinateur du réseau**.

Vous pouvez configurer la désactivation de l'isolement automatique du réseau après un certain temps. Par défaut, l'application désactiver l'isolation du réseau 8 heures après son activation. Quand l'isolation du réseau est désactivée, l'ordinateur peut utiliser le réseau sans restriction.

Comment configurer le délai de désactivation de l'isolation du réseau d'un ordinateur en mode manuel

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
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. Sélectionnez l'onglet **Tâches**.

   La liste des tâches disponibles sur l'ordinateur s'affiche.
4. Sélectionnez la tâche **Isolement du réseau**.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Cette opération ouvre une fenêtre ; dans cette fenêtre, sélectionnez le délai de désactivation de l'isolation du réseau.
7. Enregistrez vos modifications.

Comment désactiver l'isolation du réseau d'un ordinateur manuellement

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
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. Sélectionnez l'onglet **Applications**.

4. Cliquez sur **Kaspersky Endpoint Security for Windows 14.2**.

   La fenêtre des paramètres locaux de l'application s'ouvre.

5. Sélectionnez l'onglet **Paramètres de l'application**.

6. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.

7. Dans le groupe **Isolement du réseau**, cliquez sur **Débloquer l'ordinateur isolé du réseau**.

Vous pouvez également activer ou désactiver l'isolation du réseau localement en utilisant la ligne de commande.

À compter de Kaspersky Endpoint Security 12.10 for Windows, vous pouvez gérer l'isolation du réseau dans les détails de l'alerte. De plus, vous pouvez indiquer dans les détails de l'alerte la période d'isolation du réseau de l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Exclusions d'isolation du réseau

Vous pouvez configurer des exclusions d'isolation du réseau. Les connexions réseau qui correspondent aux règles ne sont pas bloquées sur l'ordinateur lorsque l'isolation du réseau est activée.

Pour configurer les exclusions d'isolation du réseau, vous pouvez utiliser une liste de *profils réseau standard*. Par défaut, les exclusions comprennent les profils réseau contenant des règles qui assurent le fonctionnement ininterrompu des appareils avec les rôles de serveur DNS/DHCP et de client DNS/DHCP. Vous pouvez également modifier les paramètres des profils réseau standard ou définir des exclusions manuellement (cf. Instructions ci-dessous).

Les exclusions définies dans les propriétés de la stratégie sont appliquées uniquement si l'isolation du réseau est activée automatiquement en réponse à une menace détectée. Les exclusions définies dans les propriétés de l'ordinateur sont appliquées uniquement si l'isolation du réseau est activée manuellement dans les propriétés de l'ordinateur dans la console Kaspersky Security Center ou dans les détails de l'alerte.

Une stratégie active n'empêche pas l'application d'exclusions de l'isolation du réseau configurées dans les propriétés de l'ordinateur, car ces paramètres s'utilisent dans des scénarios différents.

Comment ajouter une exclusion d'isolation du réseau en mode automatique

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.

5. Sélectionnez l'onglet **Isolement du réseau**.

6. Dans le groupe **Exclusions d'isolement du réseau**, cliquez sur **Exclusions**.

7. Dans la fenêtre qui s'ouvre, cliquez sur **Ajouter** → **Ajouter à partir du profil** et sélectionnez des profils réseau standard pour configurer les exclusions.

   Les exclusions d'isolation du réseau du profil sont ajoutées à la liste Exclusions d'isolation du réseau. Vous pouvez consulter les propriétés des connexions réseau. Le cas échéant, vous pouvez modifier les paramètres de connexion réseau.

8. Au besoin, ajoutez manuellement une exclusion d'isolation du réseau. Pour ce faire, dans la fenêtre reprenant la liste des exclusions, cliquez sur **Ajouter** → **Ajouter** et modifiez manuellement les paramètres de connexion réseau.

9. Enregistrez vos modifications.

Comment ajouter une exclusion d'isolation du réseau en mode manuel

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

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. Sélectionnez l'onglet **Tâches**.

   La liste des tâches disponibles sur l'ordinateur s'affiche.

4. Sélectionnez la tâche **Isolement du réseau**.

5. Sélectionnez l'onglet **Paramètres de l'application**.

6. Une fenêtre s'ouvre. Dans cette fenêtre, cliquez sur **Exclusions**.

7. Dans la fenêtre qui s'ouvre, cliquez sur **Ajouter à partir du profil** et sélectionnez des profils réseau standard pour configurer les exclusions.

   Les exclusions d'isolation du réseau du profil sont ajoutées à la liste Exclusions d'isolation du réseau. Vous pouvez consulter les propriétés des connexions réseau. Le cas échéant, vous pouvez modifier les paramètres de connexion réseau.

8. Au besoin, ajoutez manuellement une exclusion d'isolation du réseau. Pour ce faire, dans la fenêtre reprenant la liste des exclusions, cliquez sur **Ajouter** et modifiez manuellement les paramètres de connexion réseau.

9. Enregistrez vos modifications.

Vous pouvez également consulter la liste des exclusions d'isolation du réseau localement en utilisant la ligne de commande. Dans ce cas, l'ordinateur doit être isolé.

À compter de Kaspersky Endpoint Security 12.10 for Windows, vous pouvez ajouter les exclusions d'isolation du réseau dans les détails de l'alerte. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Cloud Sandbox

Cloud Sandbox est une technologie qui vous permet de détecter les menaces avancées sur les ordinateurs. Kaspersky Endpoint Security transmet automatiquement les fichiers détectés à Cloud Sandbox pour analyse. Cloud Sandbox exécute ces fichiers dans un environnement isolé pour identifier les activités malveillantes et décider de leur réputation. Les données de ces fichiers sont ensuite envoyées à Kaspersky Security Network. Par conséquent, si Cloud Sandbox a détecté un fichier malveillant, Kaspersky Endpoint Security effectuera l'action appropriée pour éliminer cette menace sur tous les ordinateurs où ce fichier est détecté.

Pour que Cloud Sandbox fonctionne, vous devez activer l'utilisation de Kaspersky Security Network.

Si vous utilisez Kaspersky Private Security Network, la technologie Cloud Sandbox n'est pas disponible.

La technologie Cloud Sandbox est activée en permanence et est disponible pour tous les utilisateurs de Kaspersky Security Network, quel que soit le type de licence qu'ils utilisent. Si vous avez déjà déployé la solution Endpoint Detection and Response Optimum, vous pouvez activer un compteur distinct pour les menaces détectées par Cloud Sandbox. Vous pouvez utiliser ce compteur pour compiler des statistiques lors de l'analyse des menaces détectées. Kaspersky Endpoint Security indique la technologie de détection des menaces Cloud Sandbox dans le *Rapport sur les menaces* de la console Kaspersky Security Center.

Compteurs de menaces

Pour activer le compteur Cloud Sandbox, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response**.
5. Sélectionnez l'onglet **Cloud Sandbox**.
6. Activez le commutateur **Cloud Sandbox ACTIVÉ**.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

En cas de menace, Kaspersky Endpoint Security active le compteur de menaces détectées à l'aide de Cloud Sandbox dans la fenêtre principale de l'application, sous **Technologies de détection des menaces**. Kaspersky Endpoint Security indiquera également la technologie de détection des menaces de Cloud Sandbox dans le *Rapport sur les menaces* et dans la console de Kaspersky Security Center.

Section de la stratégie Endpoint Detection and Response

Guide de migration KEA vers KES pour EDR Optimum

Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Optimum. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser EDR Optimum. Toutes les fonctions de Kaspersky Endpoint Agent seront exécutées par Kaspersky Endpoint Security.

Lorsque vous déployez Kaspersky Endpoint Security sur des ordinateurs sur lesquels Kaspersky Endpoint Agent est installé, la solution Kaspersky Endpoint Detection and Response Optimum continuera à fonctionner avec Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur. Le même comportement dans le système se produira lors de la mise à jour de Kaspersky Endpoint Security vers la version 11.7.0 ou toute version ultérieure.

Kaspersky Endpoint Security n'est pas compatible avec Kaspersky Endpoint Agent. Vous ne pouvez pas installer ces deux applications sur le même ordinateur.

Les conditions suivantes doivent être remplies pour que Kaspersky Endpoint Security fonctionne dans le cadre de Kaspersky Endpoint Detection and Response Optimum :

- Kaspersky Endpoint Detection and Response Optimum version 2.0 ou toute version ultérieure.
- Kaspersky Security Center version 13.2 ou version ultérieure (y compris l'Agent d'administration). Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonction EDR Optimum.
- EDR Optimum peut être géré uniquement à l'aide de Kaspersky Security Center Web Console.

- Le transfert de données au Serveur d'administration est activé. Ces données sont requises pour obtenir des informations à propos des fichiers mis en quarantaine sur un ordinateur via Web Console.

- Une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie. Pour que le module EDR Optimum fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*.

Étapes de migration de la configuration [KES KEA] vers [KES+agent intégré] pour EDR Optimum

1. **Mise à jour du plug-in Internet de Kaspersky Endpoint Security**

   Le module EDR Optimum peut être géré à l'aide du plug-in d'administration Web de Kaspersky Endpoint Security version 11.7.0 ou toute version ultérieure.

2. **Migration des stratégies et des tâches**

   Transférez les paramètres de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows. Pour ce faire, utilisez l'Assistant de migration à partir de Kaspersky Endpoint Agent dans Web Console.

   Migration des paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security dans Web Console

   Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Migration depuis Kaspersky Endpoint Agent**.

   Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

Étape 1. Migration de stratégie

L'Assistant de migration crée une stratégie que fusionne les paramètres des stratégies de Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez fusionner les paramètres avec ceux de la stratégie de Kaspersky Endpoint Security. Cliquez sur une stratégie de Kaspersky Endpoint Agent pour sélectionner la stratégie Kaspersky Endpoint Security avec laquelle vous souhaitez fusionner les paramètres. Confirmez que vous avez sélectionné les bonnes stratégies, puis passez à l'étape suivante.

Étape 2. Migration d'une tâche

L'Assistant de migration crée de nouvelles tâches pour Kaspersky Endpoint Security. Dans la liste de tâches, sélectionnez les tâches de Kaspersky Endpoint Agent que vous souhaitez créer pour une stratégie de Kaspersky Endpoint Security. Passez à l'étape suivante.

Étape 3. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- Crée une stratégie Kaspersky Endpoint Security.

La stratégie fusionne les paramètres de Kaspersky Endpoint Security et Kaspersky Endpoint Agent La stratégie porte le nom *<Nom de stratégie de Kaspersky Endpoint Security> et <Nom de stratégie de Kaspersky Endpoint Agent>*. La nouvelle stratégie porte l'état *Inactive*. Pour continuer, changez l'état des stratégies de Kaspersky Endpoint Agent et Kaspersky Endpoint Security sur *Inactive* et activez la nouvelle stratégie fusionnée.

> Après avoir procédé à la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows, veuillez vous assurer que la fonctionnalité de transfert de données vers le Serveur d'administration (données du fichier de quarantaine et données de la chaîne de développement des menaces) est configurée dans la nouvelle stratégie. Les valeurs des paramètres de transfert de données ne sont pas migrées à partir d'une stratégie de Kaspersky Endpoint Agent.

- Crée de nouvelles tâches de Kaspersky Endpoint Security.

  Les nouvelles tâches sont des copies des tâches de Kaspersky Endpoint Agent. En même temps, l'Assistant laisse les tâches de Kaspersky Endpoint Agent inchangées.

3. **Licence pour la fonctionnalité EDR Optimum**

   Si vous utilisez une licence commune Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Security for Windows et Kaspersky Endpoint Agent, la fonctionnalité EDR Optimum sera activée automatiquement après la mise à jour de l'application vers la version 11.7.0 ou toute version ultérieure. Aucune autre action n'est nécessaire.

   Si vous utilisez une licence autonome de l'extension Kaspersky Endpoint Detection and Response Optimum pour activer la fonctionnalité EDR Optimum, vous devez vous assurer que la clé d'EDR Optimum est ajoutée au stockage de Kaspersky Security Center et que la fonctionnalité de distribution automatique des clés de licence est activée. Une fois que la mise à jour de l'application vers la version 11.7.0 ou toute version ultérieure est effectuée, la fonctionnalité EDR Optimum est activée automatiquement.

   Si vous utilisez une licence Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Agent et une autre licence pour activer Kaspersky Endpoint Security for Windows, vous devez remplacer la clé de Kaspersky Endpoint Security for Windows par la clé commune de Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security. Vous pouvez remplacer la clé à l'aide de la tâche *Ajout d'une clé*.

4. **Installation/Mise à jour de l'application Kaspersky Endpoint Security**

   Pour migrer la fonctionnalité EDR Optimum lors de l'installation ou de la mise à jour d'une application, il est recommandé d'utiliser la tâche d'installation à distance. Lors de la création d'une tâche d'installation à distance, vous devez sélectionner le module EDR Optimum dans les paramètres du paquet d'installation.

   Vous pouvez également mettre à jour l'application en utilisant les méthodes suivantes :

   - À l'aide du service de mise à jour de Kaspersky.
   - Localement à l'aide de l'Assistant d'installation de l'application.

   Kaspersky Endpoint Security prend en charge la sélection automatique des modules lors de la mise à jour de l'application sur un ordinateur sur lequel est installée l'application Kaspersky Endpoint Agent. La sélection automatique des modules dépend des autorisations du compte utilisateur qui met à jour l'application.

   Si vous mettez à jour Kaspersky Endpoint Security en utilisant le fichier EXE ou MSI sous le compte système (SYSTEM), Kaspersky Endpoint Security obtient l'accès aux licences valides des solutions Kaspersky. Par conséquent, si, par exemple, Kaspersky Endpoint Agent est installé et la solution EDR Optimum est activée sur l'ordinateur, le programme d'installation de Kaspersky Endpoint Security configure automatiquement l'ensemble des modules et sélectionne le module EDR Optimum. Cette opération fait passer Kaspersky Endpoint Security à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. L'exécution du programme d'installation MSI sous le compte système (SYSTEM) est généralement effectuée lors de la mise à jour via le service de mise à jour Kaspersky ou lors du déploiement d'un paquet d'installation via Kaspersky Security Center.

Si vous mettez à jour Kaspersky Endpoint Security à l'aide d'un fichier MSI sous un compte utilisateur non privilégié, Kaspersky Endpoint Security n'a pas accès aux licences valides des solutions Kaspersky. Dans ce cas, Kaspersky Endpoint Security sélectionne automatiquement les modules en fonction de la configuration de Kaspersky Endpoint Agent. Après cela, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

Kaspersky Endpoint Security prend en charge la mise à jour sans redémarrage de l'ordinateur. Vous pouvez sélectionner le mode de mise à jour de l'application dans les propriétés de la stratégie.

5. **Vérification du fonctionnement de l'application**

   Si après l'installation ou la mise à jour de l'application, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

   - Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
   - Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous d'avoir activé la fonctionnalité d'agent intégré.
   - Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows inclut un agent intégré permettant l'intégration avec la solution Kaspersky Sandbox. Le module *Sandbox* détecte et bloque automatiquement les menaces avancées sur les ordinateurs. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Sandbox et Kaspersky Anti Targeted Attack Platform.

Intégration de l'agent intégré avec Kaspersky Sandbox

L'ajout du module Sandbox est nécessaire pour assurer l'intégration avec Kaspersky Sandbox. Vous pouvez sélectionner le module Sandbox lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

Pour utiliser le module, les conditions suivantes doivent être remplies :

- Kaspersky Security Center 13.2. Les versions antérieures de Kaspersky Security Center ne permettent pas la création de tâches autonomes d'analyse IOC pour la réponse aux menaces.
- Le module peut être administré uniquement à l'aide de Web Console. Vous ne pouvez pas gérer ce module à l'aide de la Console d'administration (MMC).
- L'application est activée, et la fonctionnalité est couverte par la licence.
- Le transfert de données au Serveur d'administration est activé.

Pour utiliser toutes les fonctionnalités de Kaspersky Sandbox, assurez-vous que le transfert de données des fichiers de quarantaine est activé. Ces données sont requises pour obtenir des informations à propos des fichiers mis en quarantaine sur un ordinateur via Web Console. Par exemple, vous pouvez télécharger un fichier de la quarantaine pour l'analyser dans Web Console.

Comment activer le transfert de données vers le Serveur d'administration dans Web Console ?

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.
5. Dans le groupe **Transfert des données au Serveur d'administration**, cochez la case **À propos des fichiers de la Quarantaine**.
6. Enregistrez vos modifications.

- Une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie

  Pour que Kaspersky Sandbox fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*. Pour en savoir plus sur l'intégration de Kaspersky Security Center avec les autres solutions de Kaspersky, consultez l'aide de Kaspersky Security Center.

  Établissement d'une connexion en arrière-plan dans Web Console

  1. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Intégration**.
  2. Passez à la section **Intégration**.
  3. Activez le commutateur **Connexion en arrière-plan pour l'intégration Activé**.
  4. Enregistrez vos modifications.

  En l'absence de connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration, il est impossible de créer des tâches d'analyse IOC autonome dans le cadre de la réponse aux menaces.

- Pour configurer une connexion de confiance avec le serveur Sandbox, vous devez préparer un certificat TLS. Il faut ensuite ajouter le certificat à l'ordinateur à l'aide d'une stratégie. Vous devez également ajouter le certificat au serveur Sandbox.

  > L'authentification bidirectionnelle à l'aide d'un conteneur chiffré n'est pas disponible pour Kaspersky Sandbox.

  Vous pouvez également ajouter un certificat TLS à Web Console ou localement en utilisant la ligne de commande.

- Le module Kaspersky Sandbox est activé.

- Les modules de l'application qui garantissent le fonctionnement de Sandbox sont activés et opérationnels. Les modules suivants assurent le fonctionnement de Sandbox :
  - Protection contre les fichiers malicieux.
  - Prévention des intrusions.
  - Pare-feu.
  - Protection AMSI.
  - Analyse en arrière-plan.

Pour activer ou désactiver l'intégration avec Kaspersky Sandbox, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Sandbox**.
5. Utilisez le commutateur **Intégration avec Sandbox ACTIVÉE** pour activer ou désactiver le module.
6. Dans le groupe **Mode d'intégration**, sélectionnez le mode de fonctionnement du module : **Kaspersky Sandbox**.
7. Cliquez sur le lien **Paramètres de connexion**.

   La fenêtre des paramètres de connexion du serveur Sandbox s'ouvre.
8. Dans le groupe **Certificat TLS du serveur**, cliquez sur **Charger** et sélectionnez le fichier du certificat TLS.

   Kaspersky Endpoint Security ne peut avoir qu'un seul certificat TLS pour un serveur Sandbox. Si vous avez ajouté un certificat TLS auparavant, ce certificat est révoqué. Seul le dernier certificat ajouté est utilisé.
9. Configurez les paramètres de connexion avancés pour les serveurs Sandbox :
   - **Délai d'attente (ms.)**. Délai d'attente de la connexion avec le serveur Sandbox. Une fois le délai d'attente configuré écoulé, Kaspersky Endpoint Security envoie une requête au serveur suivant. Vous pouvez augmenter le délai d'attente de la connexion avec le serveur si votre vitesse de connexion est faible ou si la connexion est instable. Le délai d'attente recommandé pour les demandes est de 0.5 seconde ou moins.
   - **File d'attente des requêtes**. Taille du dossier de la file d'attente des requêtes. Lors de l'envoi de plusieurs objets à l'analyse dans Sandbox, Kaspersky Endpoint Security crée une file d'attente des requêtes. Par défaut, la taille du dossier de la file d'attente des requêtes est limitée à 100 Mo. Lorsque la taille maximale est atteinte, Sandbox cesse d'ajouter de nouvelles requêtes à la file d'attente et envoie l'événement correspondant à Kaspersky Security Center. Vous pouvez configurer la taille du dossier de la file d'attente des requêtes en fonction de la configuration de votre serveur.
10. Cliquez sur le bouton **Ajouter** dans le groupe **Connexion aux serveurs Sandbox**.

11. Une fenêtre s'ouvre. Dans cette fenêtre, saisissez l'adresse du serveur Sandbox (IPv4, IPv6, DNS) ainsi que le port.

    Pour en savoir plus sur le déploiement des images virtuelles et la configuration des serveurs Sandbox, consultez l'aide de Kaspersky Sandbox.

12. Enregistrez vos modifications.

Kaspersky Endpoint Security vérifie alors le certificat TLS. Si le certificat est validé, Kaspersky Endpoint Security charge le fichier du certificat sur l'ordinateur lors de la prochaine synchronisation avec Kaspersky Security Center. Si vous avez ajouté deux certificats TLS, Kaspersky Sandbox utilisera le dernier certificat pour établir une connexion de confiance. 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 **Sandbox** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Vous pouvez activer ou désactiver l'intégration avec Kaspersky Sandbox dans Web Console ou localement en utilisant la ligne de commande.

Kaspersky Endpoint Security enregistre les informations relatives au fonctionnement du module Kaspersky Sandbox dans un rapport. Le rapport contient également des informations sur les erreurs. Si une erreur s'affiche dont la description correspond au format `Error code: XXX` (par exemple, `0xa67b01f4`), contactez le Support Technique.

Recherche d'indicateurs de compromission (tâche autonome)

Un *indicateur de compromission (IOC)* est un ensemble de données concernant un objet ou une activité qui indique un accès non autorisé à l'ordinateur (compromission des données). Par exemple, de nombreuses tentatives infructueuses de se connecter au système peuvent constituer un indicateur de compromission. La tâche *Analyse IOC* permet de trouver des indicateurs de compromission sur l'ordinateur et de prendre des mesures de réponse aux menaces.

Kaspersky Endpoint Security recherche les indicateurs de compromission à l'aide des fichiers IOC. Les *fichiers IOC* sont des fichiers contenant les ensembles d'indicateurs que l'application tente de faire correspondre pour compter une détection. Les fichiers IOC doivent être conformes standard OpenIOC. Kaspersky Endpoint Security génère automatiquement des fichiers IOC pour Kaspersky Sandbox.

Mode d'exécution de la tâche Analyse IOC

L'application crée des tâches autonomes d'analyse IOC pour Kaspersky Sandbox. La *tâche autonome d'analyse IOC* est une tâche de groupe qui est automatiquement créée lors de la réaction à une menace détectée par Kaspersky Sandbox. Kaspersky Endpoint Security génère automatiquement le fichier IOC. Les fichiers IOC personnalisés ne sont pas pris en charge. Les tâches sont automatiquement supprimées 30 jours après leur création. Pour en savoir plus sur les tâches autonomes d'analyse IOC, consultez l'aide de Kaspersky Sandbox.

Paramètres de la tâche Analyse IOC

Kaspersky Sandbox peut créer et exécuter des tâches *Analyse IOC* automatiquement lorsqu'il réagit aux menaces.

Vous pouvez configurer les paramètres uniquement dans Web Console.

Vous avez besoin de Kaspersky Security Center 13.2 pour que les tâches autonomes d'analyse IOC de Kaspersky Sandbox fonctionnent.

Pour modifier les paramètres de la tâche Analyse IOC, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur la tâche **Analyse IOC** pour Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres de l'analyse IOC**.

5. Configurez les actions à effectuer en cas de détection d'IOC :

   - **Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer l'objet, Kaspersky Endpoint Security crée une copie de sauvegarde au cas où l'objet devrait être restauré ultérieurement. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.

   - **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

   - **Exécuter uniquement lorsque l'ordinateur est inactif**. Début différé de la tâche 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. Si vous avez interrompu l'exécution de la tâche, par exemple en déverrouillant l'ordinateur, Kaspersky Endpoint Security exécute automatiquement la tâche, en reprenant à partir du point où elle a été interrompue. Cette option de planification vous permet de préserver les ressources de l'ordinateur lorsque celui-ci est utilisé.

6. Enregistrez vos modifications.

   Vous pouvez consulter les résultats de la tâche dans les propriétés de la tâche dans la section **Résultats**. Vous pouvez consulter les informations relatives aux indicateurs de compromission détectés dans les propriétés de la tâche : **Paramètres de l'application** → **Résultats de l'analyse IOC**.

Les résultats de l'analyse IOC sont conservés pendant 30 jours. À l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens.

Guide de migration KEA vers KES pour Kaspersky Sandbox

Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Sandbox. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser Kaspersky Sandbox. Toutes les fonctions de Kaspersky Endpoint Agent seront exécutées par Kaspersky Endpoint Security.

Lorsque vous déployez Kaspersky Endpoint Security sur des ordinateurs sur lesquels Kaspersky Endpoint Agent est installé, la solution Kaspersky Sandbox continuera à fonctionner avec Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur. Le même comportement dans le système se produira lors de la mise à jour de Kaspersky Endpoint Security vers la version 11.7.0 ou toute version ultérieure.

> Kaspersky Endpoint Security n'est pas compatible avec Kaspersky Endpoint Agent. Vous ne pouvez pas installer ces deux applications sur le même ordinateur.

Les conditions suivantes doivent être remplies pour que Kaspersky Endpoint Security fonctionne dans le cadre de Kaspersky Sandbox :

- Kaspersky Sandbox version 2.0 ou toute version ultérieure.
- Kaspersky Security Center version 13.2 ou version ultérieure (y compris l'Agent d'administration). Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonction Kaspersky Sandbox.
- Kaspersky Sandbox peut être administré uniquement à l'aide de Kaspersky Security Center Web Console.
- Le transfert de données au Serveur d'administration est activé. Ces données sont requises pour obtenir des informations à propos des fichiers mis en quarantaine sur un ordinateur via Web Console.
- Une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie. Pour que Kaspersky Sandbox fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*.

Étapes de migration de la configuration [KES KEA] vers [KES+agent intégré] pour Kaspersky Sandbox

1. **Mise à jour du plug-in Internet de Kaspersky Endpoint Security**

   Le module Kaspersky Sandbox peut être géré à l'aide du plug-in d'administration Web de Kaspersky Endpoint Security version 11.7.0 ou toute version ultérieure.

2. **Migration des stratégies et des tâches**

   Transférez les paramètres de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows. Pour ce faire, utilisez l'Assistant de migration à partir de Kaspersky Endpoint Agent dans Web Console.

   Migration des paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security dans Web Console

   Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Migration depuis Kaspersky Endpoint Agent**.

   Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

Étape 1. Migration de stratégie

L'Assistant de migration crée une stratégie que fusionne les paramètres des stratégies de Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez fusionner les paramètres avec ceux de la stratégie de Kaspersky Endpoint Security. Cliquez sur une stratégie de Kaspersky Endpoint Agent pour sélectionner la stratégie Kaspersky Endpoint Security avec laquelle vous souhaitez fusionner les paramètres. Confirmez que vous avez sélectionné les bonnes stratégies, puis passez à l'étape suivante.

Étape 2. Migration d'une tâche

L'Assistant de migration crée de nouvelles tâches pour Kaspersky Endpoint Security. Dans la liste de tâches, sélectionnez les tâches de Kaspersky Endpoint Agent que vous souhaitez créer pour une stratégie de Kaspersky Endpoint Security. Passez à l'étape suivante.

Étape 3. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- Crée une stratégie Kaspersky Endpoint Security.

  La stratégie fusionne les paramètres de Kaspersky Endpoint Security et Kaspersky Endpoint Agent La stratégie porte le nom *<Nom de stratégie de Kaspersky Endpoint Security> et <Nom de stratégie de Kaspersky Endpoint Agent>*. La nouvelle stratégie porte l'état *Inactive*. Pour continuer, changez l'état des stratégies de Kaspersky Endpoint Agent et Kaspersky Endpoint Security sur *Inactive* et activez la nouvelle stratégie fusionnée.

  > Après avoir procédé à la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows, veuillez vous assurer que la fonctionnalité de transfert de données vers le Serveur d'administration (données du fichier de quarantaine et données de la chaîne de développement des menaces) est configurée dans la nouvelle stratégie. Les valeurs des paramètres de transfert de données ne sont pas migrées à partir d'une stratégie de Kaspersky Endpoint Agent.

- Crée de nouvelles tâches de Kaspersky Endpoint Security.

  Les nouvelles tâches sont des copies des tâches de Kaspersky Endpoint Agent. En même temps, l'Assistant laisse les tâches de Kaspersky Endpoint Agent inchangées.

3. **Licence de la fonctionnalité Kaspersky Sandbox**

   Pour activer Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Sandbox, vous avez besoin d'une licence distincte pour le module complémentaire Kaspersky Sandbox. Vous pouvez ajouter la clé à l'aide de la tâche *Ajout d'une clé*. En conséquence, deux clés seront ajoutées à l'application : *Kaspersky Endpoint Security* et *Kaspersky Sandbox*.

4. **Installation/Mise à jour de l'application Kaspersky Endpoint Security**

   Pour migrer la fonctionnalité Kaspersky Sandbox lors de l'installation ou de la mise à jour d'une application, il est recommandé d'utiliser la tâche d'installation à distance. Lors de la création d'une tâche d'installation à distance, vous devez sélectionner le module Kaspersky Sandbox dans les paramètres du paquet d'installation.

Vous pouvez également mettre à jour l'application en utilisant les méthodes suivantes :

- À l'aide du service de mise à jour de Kaspersky.
- Localement à l'aide de l'Assistant d'installation de l'application.

Kaspersky Endpoint Security prend en charge la sélection automatique des modules lors de la mise à jour de l'application sur un ordinateur sur lequel est installée l'application Kaspersky Endpoint Agent. La sélection automatique des modules dépend des autorisations du compte utilisateur qui met à jour l'application.

Si vous mettez à jour Kaspersky Endpoint Security en utilisant le fichier EXE ou MSI sous le compte système (SYSTEM), Kaspersky Endpoint Security obtient l'accès aux licences valides des solutions Kaspersky. Par conséquent, si, par exemple, Kaspersky Endpoint Agent est installé et la solution Kaspersky Sandbox est activée sur l'ordinateur, le programme d'installation de Kaspersky Endpoint Security configure automatiquement l'ensemble des modules et sélectionne le module Kaspersky Sandbox. Cette opération fait passer Kaspersky Endpoint Security à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. L'exécution du programme d'installation MSI sous le compte système (SYSTEM) est généralement effectuée lors de la mise à jour via le service de mise à jour Kaspersky ou lors du déploiement d'un paquet d'installation via Kaspersky Security Center.

Si vous mettez à jour Kaspersky Endpoint Security à l'aide d'un fichier MSI sous un compte utilisateur non privilégié, Kaspersky Endpoint Security n'a pas accès aux licences valides des solutions Kaspersky. Dans ce cas, Kaspersky Endpoint Security sélectionne automatiquement les modules en fonction de la configuration de Kaspersky Endpoint Agent. Après cela, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

Kaspersky Endpoint Security prend en charge la mise à jour sans redémarrage de l'ordinateur. Vous pouvez sélectionner le mode de mise à jour de l'application dans les propriétés de la stratégie.

5 **Vérification du fonctionnement de l'application**

Si après l'installation ou la mise à jour de l'application, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

- Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
- Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous d'avoir activé la fonctionnalité d'agent intégré.
- Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows prend en charge l'utilisation de la solution 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 trois unités fonctionnelles :

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Vous pouvez acheter l'ensemble des unités fonctionnelles ou des unités fonctionnelles individuelles séparément. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform. L'application inclut des agents intégrés pour les modules EDR et NDR. L'application prend également en charge l'utilisation du module Sandbox, qui fait partie de KATA.

Outils de Threat Intelligence

Kaspersky Endpoint Detection and Response utilise les outils Threat Intelligence suivants :

- L'intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations concernant la réputation des fichiers et des adresses Internet.
- La base de données Kaspersky Threats.
- L'infrastructure du service Cloud Kaspersky Security Network (ci-après également appelé "KSN"), qui donne accès à des informations en temps réel sur la réputation des fichiers, des sites Internet et des logiciels à partir de la base de connaissances de Kaspersky. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de protection et réduit la possibilité de faux positifs.

Principe de fonctionnement de la solution

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les informations relatives aux événements survenus sur l'ordinateur (données de télémétrie) sont envoyées au serveur Kaspersky Anti Targeted Attack Platform. Dans ce cas, Kaspersky Endpoint Security envoie également au serveur Kaspersky Anti Targeted Attack Platform des informations relatives aux menaces découvertes par l'application ainsi que des informations relatives aux résultats du traitement de ces menaces.

L'intégration de EDR (KATA) et NDR (KATA) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la console Kaspersky Anti Targeted Attack Platform, y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Configurations de Kaspersky Endpoint Security pour utiliser EDR / NDR (KATA)

Les configurations suivantes peuvent être appliquées pour utiliser EDR / NDR (KATA) :

- **[KES+agent intégré]**. Dans cette configuration, Kaspersky Endpoint Security agit à la fois comme une application assurant la sécurité de l'ordinateur et comme une application permettant d'utiliser EDR / NDR (KATA). L'agent intégré pour EDR (KATA) est disponible dans Kaspersky Endpoint Security 12.1 for Windows et toute version ultérieure. L'agent intégré pour NDR (KATA) est disponible dans Kaspersky Endpoint Security 12.7 for Windows et toute version ultérieure.

- **[PPE tierce+EDR Agent]**. Dans cette configuration, la sécurité de l'infrastructure informatique est assurée par la plateforme de protection des terminaux (PPE) tierce. L'interaction avec EDR / NDR (KATA) est assurée par Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent (EDR Agent). Dans cette configuration, EDR Agent est compatible avec les applications PPE tierces. EDR Agent pour EDR (KATA) est disponible dans Kaspersky Endpoint Security 12.3 for Windows et toute version ultérieure. EDR Agent pour NDR (KATA) est disponible dans Kaspersky Endpoint Security 12.7 for Windows et toute version ultérieure.

Prise en charge des versions précédentes de Kaspersky Endpoint Security

Si vous utilisez Kaspersky Endpoint Security 11.2.0 – 11.8.0 pour l'interopérabilité avec Kaspersky Anti Targeted Attack Platform (EDR), l'application comprend Kaspersky Endpoint Agent. Vous pouvez installer Kaspersky Endpoint Agent en même temps que Kaspersky Endpoint Security.

Si vous utilisez Kaspersky Endpoint Security 11.9.0 – 12.0, vous devez installer Kaspersky Endpoint Agent séparément, car à partir de Kaspersky Endpoint Security 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution de Kaspersky Endpoint Security.

Intégration de l'agent intégré avec EDR / NDR (KATA)

Pour l'intégration avec EDR / NDR (KATA), il faut ajouter le module correspondant : Endpoint Detection and Response (KATA) ou Network Detection and Response (KATA). Vous pouvez sélectionner les modules d'intégration avec EDR / NDR (KATA) lors de l'installation ou de la mise à jour de l'application ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

À partir de la version 12.11 de Kaspersky Endpoint Security for Windows, le module EDR (KATA) a été renommé en **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)**. Dans cette version de l'application, le module est compatible avec Kaspersky Anti Targeted Attack Platform 7.1 et les versions antérieures, ainsi qu'avec Kaspersky Endpoint Detection and Response Expert (on-premises).

Les modules Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises) ne sont pas compatibles entre eux.

Pour utiliser EDR / NDR (KATA), les conditions suivantes doivent être remplies :

- EDR (KATA) : Kaspersky Anti Targeted Attack Platform versions 5.0–7.1.
- NDR (KATA) : Kaspersky Anti Targeted Attack Platform version 7.0 ou toute version ultérieure.
- EDR (KATA) : Kaspersky Endpoint Security for Windows 12.1 ou version ultérieure. Pour en savoir plus sur la compatibilité de KATA avec les différentes versions de Kaspersky Endpoint Security, consultez la documentation Aide de Kaspersky Anti Targeted Attack Platform.
- NDR (KATA) : Kaspersky Endpoint Security for Windows 12.7 ou version ultérieure.
- Kaspersky Security Center version 14.2 ou toute version ultérieure. Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonction EDR / NDR (KATA).
- L'application est activée, et la fonctionnalité est couverte par la licence.
- Les modules Endpoint Detection and Response (KATA) et Network Detection and Response (KATA) sont activés.
- Les modules de l'application qui garantissent le fonctionnement d'EDR/NDR (KATA) sont activés et opérationnels. Les modules suivants assurent le fonctionnement d'EDR / NDR (KATA) :
  - Protection contre les fichiers malicieux.
  - Protection contre les menaces Internet.
  - Protection contre les menaces par emails.
  - Protection contre les Exploits.
  - Détection comportementale.
  - Prévention des intrusions.
  - Protection AMSI.

- Analyse en arrière-plan.
- Kaspersky Security Network.

https://www.youtube.com/watch?v=cZzgtBoeC7k

https://www.youtube.com/watch?v=gd-rySv0ThQ

L'intégration avec Endpoint Detection and Response (KATA) comprend les étapes suivantes :

1. **Installation des modules Endpoint Detection and Response (KATA) et Network Detection and Response (KATA)**

   Vous pouvez sélectionner les modules EDR (KATA) et NDR (KATA) lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   > Vous devez redémarrer votre ordinateur pour terminer la mise à jour de l'application avec les nouveaux modules.

2. **Activation d'Endpoint Detection and Response (KATA) et de Network Detection and Response (KATA)**

   Vous devez acheter une licence distincte pour EDR (KATA) et NDR (KATA) (par exemple, module complémentaire de Kaspersky Endpoint Detection and Response (KATA)).

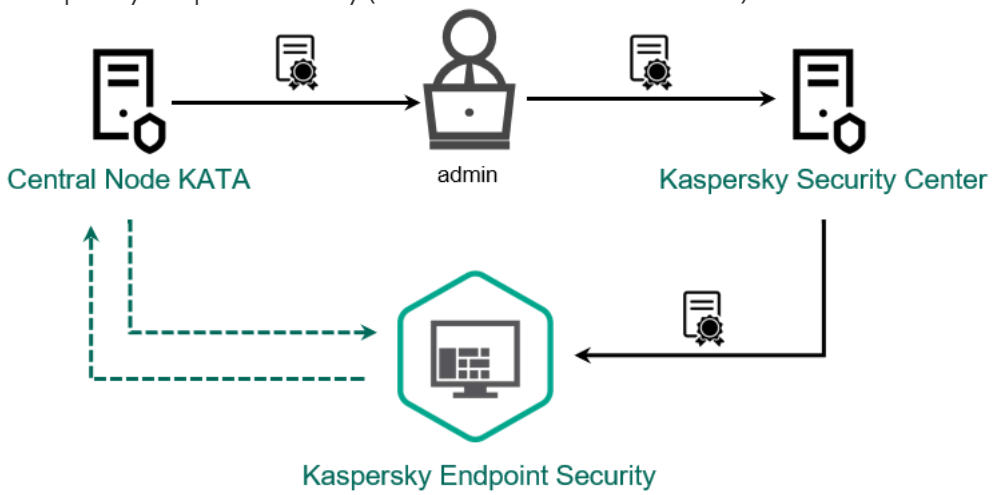
   La fonctionnalité est disponible après l'ajout d'une clé distincte qui couvre les fonctionnalités EDR (KATA) et NDR (KATA). Par conséquent, plusieurs clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et des clés pour Kaspersky Endpoint Detection and Response (KATA) et Network Detection and Response (KATA).

   Les licences de fonctionnalité autonome EDR (KATA) et NDR (KATA) sont les mêmes que celles de Kaspersky Endpoint Security.

Assurez-vous que les fonctionnalités EDR (KATA) et NDR (KATA) sont incluses dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

3 Connexion au module Central Node

Kaspersky Anti Targeted Attack Platform requiert l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le module Central Node. Pour configurer une connexion sécurisée, vous devez utiliser un certificat TLS. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).



Ajouter un certificat TLS à Kaspersky Endpoint Security

Par défaut, Kaspersky Endpoint Security vérifie uniquement le certificat TLS du module Central Node. Pour rendre la connexion plus sécurisée, vous pouvez en outre activer la vérification de l'ordinateur sur le module Central Node (authentification bidirectionnelle). Pour activer cette vérification, vous devez activer l'authentification bidirectionnelle dans les paramètres du module Central Node et de Kaspersky Endpoint Security. Pour utiliser l'authentification bidirectionnelle, vous aurez également besoin d'un conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** et sélectionnez le module que vous souhaitez configurer : **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.
5. Cochez la case correspondante : **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** ou **Network Detection and Response (KATA)**.
6. Cliquez sur **Paramètres de connexion au serveur**.

7. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.

   - **Certificat TLS du serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

     Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

8. Cliquez sur **OK**.

9. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

   Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

10. En cas de nécessité, configurez la télémétrie.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment connecter un ordinateur Kaspersky Endpoint Security au module Central Node à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Accédez à la section **Configuration des agents intégrés** et sélectionnez le module que vous souhaitez configurer : **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.

5. Activez le commutateur correspondant : **Endpoint Detection and Response Expert (on-premises) ACTIVÉ** ou **Network Detection and Response (KATA) ACTIVÉ**.

6. Pour configurer EDR (KATA), sélectionnez **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** dans la liste des solutions.

7. Cliquez sur **Paramètres de connexion**.

8. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node.

   - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform).

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

     Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

9. Cliquez sur **OK**.

10. Ajoutez des serveurs Central Node. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

    Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

11. En cas de nécessité, configurez la télémétrie.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Vous pouvez également ajouter un certificat TLS localement en utilisant la ligne de commande.

Par conséquent, l'ordinateur est ajouté à la console Kaspersky Anti Targeted Attack Platform. Vérifiez l'état de fonctionnement des modules en consultant le *Rapport sur l'état des modules de l'application*. Vous pouvez également consulter l'état de fonctionnement des modules dans les rapports de l'interface locale de Kaspersky Endpoint Security. Les modules **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)** et **Network Detection and Response (KATA)** seront ajoutés à la liste des modules de Kaspersky Endpoint Security.

Vous pouvez vérifier l'état des modules de la console de Kaspersky Security Center dans les propriétés de l'ordinateur, dans la section **Modules**. Tenez compte des aspects suivants lorsque vous vérifiez l'état du module dans la console. Si le module n'est pas installé et si la fonctionnalité n'est pas comprise dans votre licence, la console présente l'état **Non pris en charge par la licence** au lieu de l'état **Non installé(e)**.

À partir de Kaspersky Endpoint Security 12.6 for Windows, vous pouvez surveiller l'état du module EDR (KATA) dans la Console d'administration (MMC) de Kaspersky Security Center. L'état actuel du module s'affiche dans les propriétés de l'ordinateur dans la colonne **État de Endpoint Sensor** (*En cours d'exécution*, *En cours de démarrage*, *Arrêté(e)*, *Suspendu(e)*, *Échec*, *Inconnu*). La Web Console n'affiche pas l'état de l'Endpoint Sensor.

Configuration de la télémétrie EDR (KATA)

Télémétrie est une liste d'événements qui se sont produits sur l'ordinateur protégé. Kaspersky Endpoint Security analyse les données de télémétrie et les envoie à Kaspersky Anti Targeted Attack Platform lors de la synchronisation. Les événements de télémétrie arrivent presque continuellement sur le serveur. Kaspersky Endpoint Security lance la synchronisation avec le serveur lorsque l'une des conditions suivantes est remplie :

- L'intervalle de synchronisation est écoulé.
- Le nombre d'événements dans la mémoire tampon dépasse la limite supérieure.

Par conséquent, par défaut, l'application se synchronise toutes les 30 secondes ou chaque fois que la mémoire tampon contient 1 024 événements. Vous pouvez configurer le comportement de synchronisation dans la stratégie de Kaspersky Endpoint Security et sélectionner les valeurs optimales en fonction de la charge de votre réseau (voir les instructions ci-dessous).

S'il n'y a pas de connexion entre Kaspersky Endpoint Security et le serveur, l'application met les nouveaux événements en file d'attente. Lorsque la connexion est rétablie, Kaspersky Endpoint Security envoie les événements de la file d'attente au serveur dans le bon ordre. Pour éviter de surcharger le serveur, Kaspersky Endpoint Security peut ignorer certains événements. Pour cela, vous pouvez optimiser les paramètres de transmission des événements, par exemple, pour définir une valeur maximale d'événements par heure (voir les instructions ci-dessous).

Si vous utilisez Kaspersky Anti Targeted Attack Platform avec une autre solution qui utilise également la télémétrie, vous pouvez désactiver la télémétrie pour KATA (EDR) (voir les instructions ci-dessous). Cela vous permet d'optimiser la charge du serveur pour ces solutions. Par exemple, si vous avez déployé la solution Managed Detection and Response et KATA (EDR), vous pouvez utiliser la télémétrie MDR et créer des tâches Threat Response dans KATA (EDR).

Configuration de la télémétrie dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Detection and Response** et sélectionnez le module que vous souhaitez configurer : **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.
5. Configurez le paramètre **Envoyer une demande de synchronisation au serveur KATA toutes les (min.)**. Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.
6. Assurez-vous que la case **Envoyer la télémétrie à KATA** est cochée.

7. Si nécessaire, configurez la synchronisation avec les paramètres du serveur dans le groupe **Paramètres de transmission des données** :

   - **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.

   - **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.

8. Si nécessaire, cochez la case **Activer la limitation des demandes** dans le groupe **Limitation des demandes**.

   Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.

9. Configurez les paramètres d'optimisation pour l'envoi d'événements au serveur :

   - **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.

   - **Pourcentage de la limite d'événement excédentaire**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

10. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer la télémétrie dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.

5. Pour configurer EDR (KATA), sélectionnez **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** dans la liste des solutions.

6. Assurez-vous que la case **Envoyer la télémétrie aux serveurs KATA** est cochée dans le groupe **Paramètres de transmission des données**.

7. Configurez le paramètre **Envoyer une demande de synchronisation au serveur toutes les (min.)**. Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.

8. Assurez-vous que la case **Envoyer la télémétrie aux serveurs KATA** est cochée.

9. Si nécessaire, configurez la synchronisation avec les paramètres du serveur dans le groupe **Paramètres de transmission des données** :

   - **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.

   - **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.

10. Si nécessaire, cochez la case **Activer la limitation des demandes** dans le groupe **Limitation des demandes**.

    Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.

11. Configurez les paramètres d'optimisation pour l'envoi d'événements au serveur :

    - **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.

    - **Pourcentage de la limite d'événement excédentaire**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Accédez à la section **Intégration KATA** → **Exclusions de la télémétrie**.

5. Sous **Paramètres de transmission des données**, cochez la case **Utiliser les exclusions**.

6. Cliquez sur **Ajouter** et configurez les exclusions :

Les critères sont combinés avec la logique *ET*.

- **Chemin d'accès**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Pour que l'exclusion fonctionne, le chemin d'accès au fichier doit être précisé.
- **Ligne de commande**. Commande utilisée pour exécuter l'objet.
- **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo).

  Pour en savoir plus sur la ressource VersionInfo, consultez le site de Microsoft.
- **Nom du fichier d'origine**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo).
- **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo).
- **MD5**. hash MD5 du fichier.
- **SHA256**. hash SHA256 du fichier.
- **Types d'événements**. Pour que l'exclusion fonctionne, vous devez sélectionner au moins un type d'événement.

7. Enregistrez vos modifications.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur **Nouvelle tâche**.

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

Étape 1. Sélection du type de tâche

1. Choisissez **Kaspersky Endpoint Security for Windows (14.2)** → **Annulation de la mise à jour**.

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

Configurez la planification de la tâche, par exemple, manuellement.

Étape 4. Définition du nom de la tâche

Saisissez un nom pour la tâche.

Étape 7. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Exclusions de télémétrie EDR (KATA)

Pour améliorer les performances et optimiser la transmission des données vers le serveur de télémétrie, vous pouvez configurer des exclusions de télémétrie. Par exemple, vous pouvez choisir de ne pas envoyer les données de communication réseau pour certaines applications.

Comment créer une exclusion de télémétrie dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la télémétrie** → **Télémétrie EDR (KATA) / NDR (KATA)**.
5. Dans la fenêtre qui s'ouvre, configurez les exclusions de télémétrie (cf. tableau ci-après).

   L'application associe des conditions d'exclusion à l'opérateur logique ET Pour créer une règle, vous devez définir une valeur dans le champ **Chemin complet** et sélectionner au moins un type d'événement dans la liste **Utiliser pour les types d'événements suivants**.
6. Enregistrez vos modifications.

Création d'une exclusion de télémétrie dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie EDR (KATA) / NDR (KATA)**.

6. Dans la fenêtre qui s'ouvre, configurez les exclusions de télémétrie (cf. tableau ci-après).

   L'application associe des conditions d'exclusion à l'opérateur logique ET Pour créer une règle, vous devez définir une valeur dans le champ **Chemin complet** et sélectionner au moins un type d'événement.

7. Enregistrez vos modifications.

Paramètres d'exclusion de télémétrie

Paramètre	Description
Processus exclus	**Optimiser la taille de la télémétrie à envoyer**. Kaspersky Endpoint Security permet d'optimiser le volume de données transmises et d'exclure de la télémétrie les événements présentant certains codes : code 102 (communications de base) et 8 (activité réseau du processus) pour le protocole Microsoft SMB, le service WinRM et le processus klnagent.exe de l'Agent d'administration et des informations détaillées sur les types de paquets réseau pour tous les types de protocoles réseau. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation. **Utiliser pour les types d'événements suivants** : • **Modification du fichier**. • **Événements du réseau**. • **Processus : entrée interactive de la console**. • **Module chargé**. • **Registre modifié**. • **Journaux DNS**. • **Accès au processus**. • **Injection de code**. • **Requête WMI**. • **Canal**. • **LDAP**. • **AMSI**.

Paramètre	Description
Communications des réseaux exclus	**Nom de la règle**. **Direction**. **Protocole**. **Socket raw**. **Numéro de protocole**. **Certificat TLS**. **Port local ou plage**. **Port distant ou plage**. **Adresse locale**. L'adresse réseau de l'ordinateur pour lequel Kaspersky Endpoint Security exclut la télémétrie du trafic réseau. **Adresse distante**. L'adresse réseau de l'ordinateur pour lequel Kaspersky Endpoint Security exclut la télémétrie du trafic réseau. Seul le format IPv4 est pris en charge pour les adresses IP. **Applications**. Liste des fichiers exécutables des applications pour lesquelles Kaspersky Endpoint Security exclut la télémétrie EDR du trafic réseau.
Opérations sur les fichiers exclus	**Nom de la règle**. **Nom du fichier ou masque**. Nom ou masque du fichier ou du dossier. Kaspersky Endpoint Security applique la règle d'exclusion lors de l'accès à ce fichier ou à ce dossier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. **Type de fonctionnement**. **Chemin précédent**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.

Paramètre	Description
Opérations DNS exclues	**Nom de la règle**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation. **DNS** : • **Adresse IP du serveur DNS**. • **Options de requête**. • **État**. • **Nom de domaine**. • **Identifiant du type de paramètres**. • **Données de réponse**.
Opérations LDAP exclues	**Nom de la règle**. **Zone de recherche LDAP**. **Filtre**. **Nom unique pour la recherche d'objets LDAP**. **Attributs d'objets**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.

Paramètre	Description
Requêtes d'accès aux processus exclues	**Nom de la règle**. **Type de fonctionnement**. **Accès demandé au processus**. **Trace de la pile d'exécution**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus**, **Processus parent**, **Fichier du processus cible**, **Gérer le processus source** et **Gérer le processus cible**. • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Précisez les critères de déclenchement de la règle et les types d'événements pour lesquels cette règle doit être utilisée**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.
Injections de code exclues	**Nom de la règle**. **Méthode d'accès**. **Pile d'exécution**. **Ligne de commande modifiée**. **Adresse d'injection**. **Nom DLL injecté**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.

Paramètre	Description
Requêtes WMI exclues	**Nom de la règle**. **Type d'opérations WMI**. **Requête à distance**. **Nom de l'ordinateur qui a exécuté une commande WMI**. **Compte utilisateur WMI**. **Commande WMI exécutée**. **Espace de noms WMI**. **Filtre du consommateur d'événements WMI**. **Nom du consommateur d'événements WMI créé**. **Code source d'un consommateur d'événements WMI**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.
Opérations sur les canaux exclues	**Nom de la règle**. **Nom du canal**. **Type de fonctionnement**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.

Paramètre	Description
Modifications exclues du registre	**Nom de la règle**. **Type de fonctionnement**. **Chemin**. **Nom de la valeur**. **Valeur**. **Nom complet d'un fichier du registre**. Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. **Processus** et **Processus parent**: • **Chemin complet**. Chemin d'accès complet au fichier, y compris son nom et son extension. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. • **Texte de la ligne de commande**. Commande utilisée pour exécuter le fichier. • **Description**. Valeur du paramètre FileDescription d'une ressource RT_VERSION (VersionInfo). • **Nom d'origine du fichier**. Valeur du paramètre OriginalFilename d'une ressource RT_VERSION (VersionInfo). • **Version**. Valeur du paramètre FileVersion d'une ressource RT_VERSION (VersionInfo). • **Sommes de contrôle des fichiers**. MD5 et SHA256. Vous pouvez aussi sélectionner un fichier manuellement, et l'application remplira automatiquement les champs à partir du fichier sélectionné. Sous les systèmes d'exploitation 64 bits, vous devez saisir manuellement les paramètres de la version 64 bits du fichier exécutable du processus à partir du dossier `C:\windows\system32`, car l'application remplit les champs des paramètres du fichier exécutable avec les données des propriétés du fichier exécutable de la version 32 bits du même fichier exécutable dans le dossier `C:\windows\syswow64`. Par exemple, si vous sélectionnez `C:\windows\system32\cmd.exe`, le plug-in affiche les paramètres de `C:\windows\syswow64\cmd.exe`. Un tel comportement est dicté par les particularités du système d'exploitation.
Opérations exclues avec les appareils	**Nom de la règle**. **Type d'appareil**. **Identifiant d'appareil**. **Nom de l'appareil**.

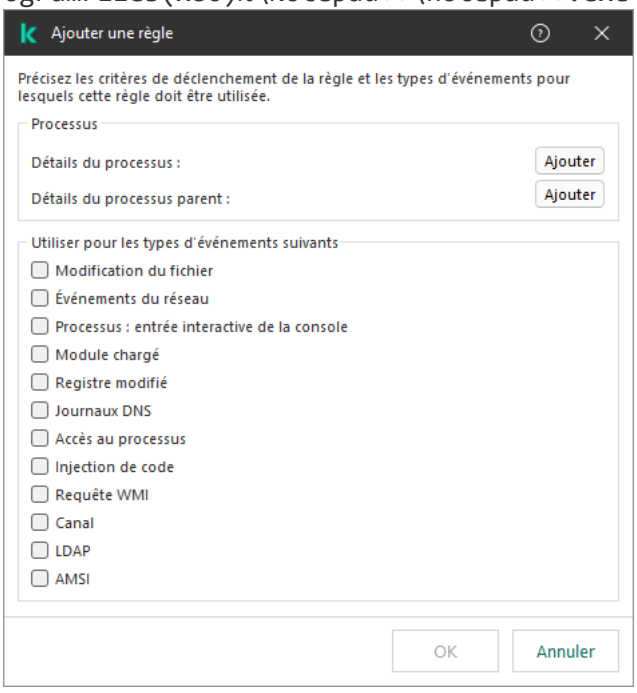
Exemple 1. Processus exclus

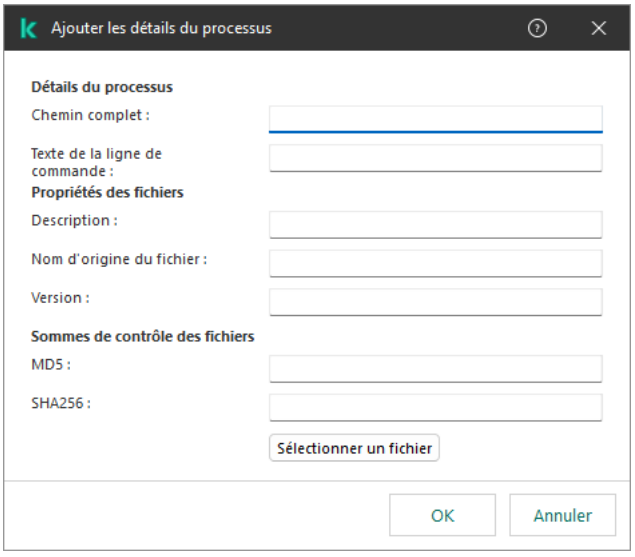
Pour exclure les événements des applications (processus) tierces de la télémétrie, ouvrez la fenêtre d'exclusions de la télémétrie EDR dans l'onglet **Processus exclus** et ajoutez le fichier exécutable de l'application.

Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique.

Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Par exemple :

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`





Exclusion d'un processus

Exemple 1. Modification du fichier

Si vous modifiez souvent des scripts dans l'application Notepad++ et que vous voulez exclure les événements de modification pour les scripts correspondants, ajoutez le fichier exécutable Notepad++ aux exclusions de télémétrie.

Définissez les paramètres comme suit :

- **Chemin complet** : `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256** : 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Utiliser pour les types d'événements suivants** : Modification du fichier.

Exemple 2. Événements du réseau

Si vous utilisez l'application WinSCP pour gérer des fichiers sur un serveur distant et que vous souhaitez exclure les événements réseau, ajoutez le fichier exécutable WinSCP aux exclusions de télémétrie.

Définissez les paramètres comme suit :

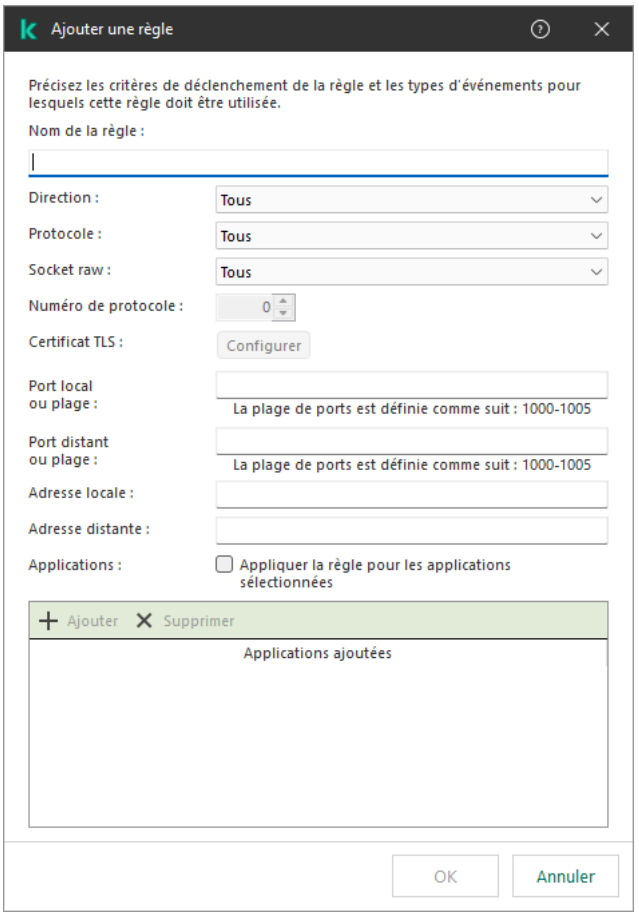
- **Chemin complet** : `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256** : 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (facultatif).
- **Utiliser pour les types d'événements suivants** : Événements du réseau.

Exemple 2. Communications des réseaux exclus

Pour exclure les événements de connexion à un service distant de la télémétrie, ouvrez la fenêtre d'exclusions de la télémétrie EDR dans l'onglet **Communications des réseaux exclus** et ajoutez les paramètres de connexion : protocole, port, direction, adresse IP, certificat TLS et autres.

Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique.

> Vous ne pouvez pas indiquer d'adresse de sous-réseau (par exemple, 10.28.0.0/24). L'application permet d'indiquer une seule adresse IP (par exemple, 10.28.0.105).



Exclusion de communications réseau

Si vous utilisez un serveur Internet d'entreprise et que vous souhaitez exclure les événements du navigateur lors de la connexion à ce serveur Internet, ajoutez l'adresse IP de l'utilisateur et le fichier exécutable du navigateur aux exclusions de télémétrie.

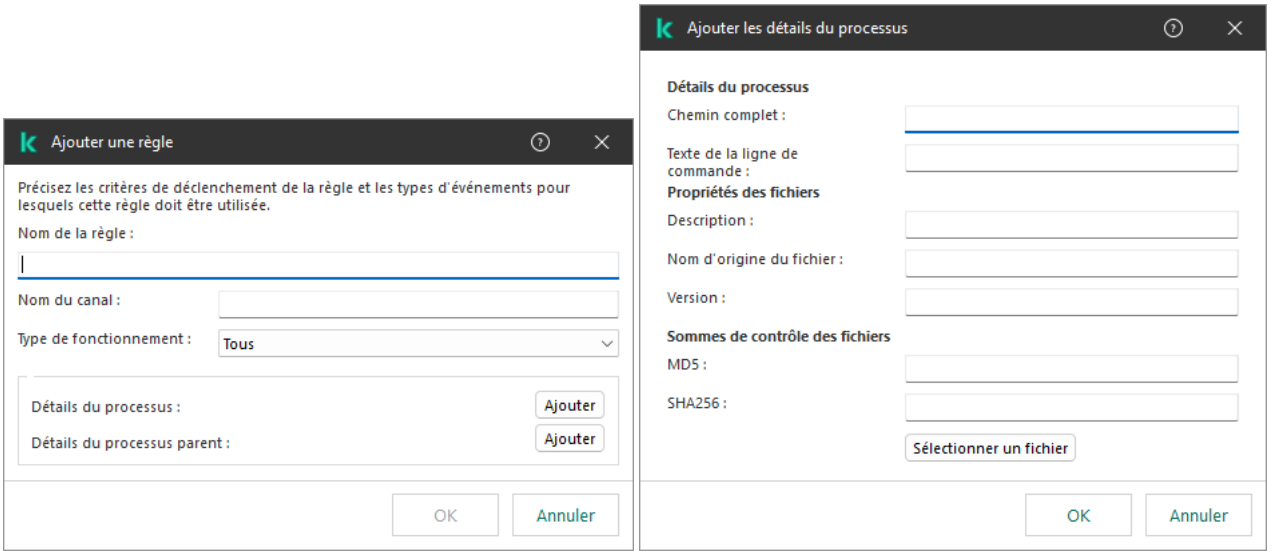
Définissez les paramètres comme suit :

- **Protocole** : TCP.
- **Port distant ou plage** : 443.
- **Adresse distante** : 10.28.0.105.
- **Applications** : `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe` ; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Exemple 3. Opérations sur les fichiers exclus

Pour exclure de la télémétrie les événements impliquant des opérations avec des fichiers de confiance, ouvrez la fenêtre d'exclusions de la télémétrie EDR dans l'onglet **Opérations sur les fichiers exclus** et ajoutez le fichier de confiance.

Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique.



Exclusion des opérations sur les fichiers

Si une application enregistre dans un journal et que vous souhaitez exclure les événements de modification du fichier journal, ajoutez le fichier journal et le fichier exécutable de l'application à la télémétrie.

Définissez les paramètres comme suit :

- **Nom du fichier ou masque** : `C:\Apache24\logs\error.log`.
- **Type de fonctionnement** : Modification du fichier.
- **Chemin complet** : `C:\Apache24\bin\httpd.exe`.
- **SHA256** : 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Exemple 4. Modifications du registre exclues

Pour exclure les événements de modification du registre de la télémétrie, ouvrez la fenêtre d'exclusions de la télémétrie EDR dans l'onglet **Modifications exclues du registre** et ajoutez une clé de registre.

Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique.

Si une application modifie fréquemment les valeurs de son registre et que vous souhaitez exclure ces événements de modification du registre de la télémétrie, ajoutez la clé de registre et le fichier exécutable de l'application aux exclusions de la télémétrie.

Définissez les paramètres comme suit :

- **Type de fonctionnement** : Modification.
- **Chemin** : HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Chemin complet** : `C:\Program Files\PuTTY\putty.exe`.
- **SHA256** : 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform inclut le module Sandbox (KATA Sandbox). *Sandbox* est une technologie qui vous permet de détecter les menaces avancées sur un ordinateur. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

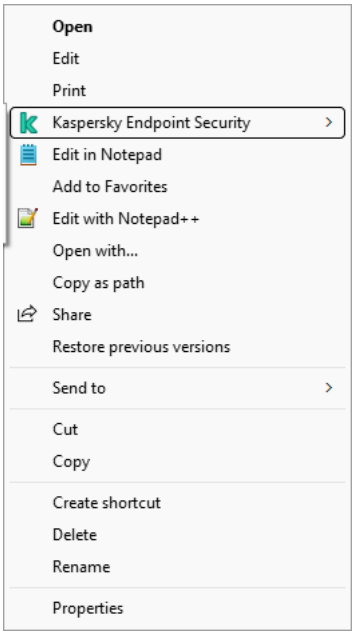
> Pour activer KATA Sandbox, vous avez besoin d'une clé de licence qui inclut les fonctionnalités KATA ou KEDR. Pour en savoir plus sur les fonctionnalités disponibles, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

KATA Sandbox permet d'analyser les fichiers dans les modes suivants :

- *Manuellement*. L'utilisateur envoie manuellement le fichier pour analyse à l'aide du menu contextuel (**Envoyer à la Sandbox**). Lors de l'envoi d'un fichier dans l'application Sandbox, l'application l'analyse à l'aide des bases antivirus.
- *Automatiquement*. L'application détecte automatiquement les objets et les envoie à la Sandbox pour analyse.

Une fois que le fichier est envoyé à Sandbox, il reste accessible à l'utilisateur. Kaspersky Endpoint Security enregistre l'événement correspondant dans le journal, puis le transmet à Kaspersky Security Center et à la console de Kaspersky Anti Targeted Attack Platform. Si Sandbox détecte une activité malveillante, Kaspersky Endpoint Security exécute automatiquement une action de réponse aux menaces (par exemple, il supprime l'objet et lance une analyse des zones critiques).

Pour que KATA Sandbox fonctionne en mode manuel, Kaspersky Anti Targeted Attack Platform 7.0 ou une version ultérieure doit être déployée. Pour que KATA Sandbox fonctionne en mode automatique, Kaspersky Anti Targeted Attack Platform 8.0 ou une version ultérieure doit être déployée.



Analyse dans KATA Sandbox à partir du menu contextuel

Intégration de l'agent intégré avec KATA Sandbox

L'ajout du module Sandbox est nécessaire pour assurer l'intégration avec KATA Sandbox. Vous pouvez sélectionner le module Sandbox lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

Pour envoyer des fichiers à l'analyse, vous devez activer l'intégration avec KATA Sandbox et ajouter un serveur Central Node qui est déployé au sein de la solution. Le module peut être administré uniquement à l'aide de Kaspersky Security Center Web Console. Vous ne pouvez pas gérer ce module à l'aide de la Console d'administration (MMC).

Pour activer ou désactiver l'intégration avec KATA Sandbox, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Sandbox**.
5. Utilisez le commutateur **Intégration avec Sandbox ACTIVÉE** pour activer ou désactiver le module.

6. Sélectionnez le mode de fonctionnement de KATA Sandbox :

   - **Manuel**. L'utilisateur envoie manuellement le fichier pour analyse à l'aide du menu contextuel (**Envoyer à la Sandbox**).

   - **Automatique**. L'application détecte automatiquement les objets et les envoie à la Sandbox pour analyse.

   - **Combiné**.

7. Cliquez sur le lien **Paramètres de connexion**.

8. Configurez les paramètres de connexion au serveur Central Node :

   - **Délai d'attente (ms.)**. Délai d'attente de la connexion avec le serveur Central Node. Une fois le délai d'attente configuré écoulé, Kaspersky Endpoint Security envoie une requête au serveur suivant. Vous pouvez augmenter le délai d'attente de la connexion avec le serveur si votre vitesse de connexion est faible ou si la connexion est instable. Le délai d'attente recommandé pour les demandes est de 0.5 seconde ou moins.

   - **File d'attente des requêtes**. Taille du dossier de la file d'attente des requêtes. Lors de l'envoi de plusieurs objets à l'analyse dans Sandbox, Kaspersky Endpoint Security crée une file d'attente des requêtes. Par défaut, la taille du dossier de la file d'attente des requêtes est limitée à 100 Mo. Lorsque la taille maximale est atteinte, Sandbox cesse d'ajouter de nouvelles requêtes à la file d'attente et envoie l'événement correspondant à Kaspersky Security Center. Vous pouvez configurer la taille du dossier de la file d'attente des requêtes en fonction de la configuration de votre serveur.

   - **Certificat TLS du serveur**. Pour configurer une connexion de confiance avec le serveur Central Node, vous devez préparer un certificat TLS. Il faut ensuite ajouter le certificat à l'ordinateur à l'aide d'une stratégie. Vous devez également ajouter le certificat au serveur Central Node.

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.

9. Cliquez sur le bouton **Ajouter** dans le groupe **Connexion aux serveurs Sandbox**.

10. Une fenêtre s'ouvre. Dans cette fenêtre, saisissez l'adresse du serveur Central Node (IPv4, IPv6, DNS) ainsi que le port.

    Pour en savoir plus sur le déploiement des images virtuelles et la configuration des serveurs Central Node, consultez l'aide de Kaspersky Anti Targeted Attack Platform .

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Ainsi, le module Sandbox est activé. 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 **Sandbox** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Configuration des actions de réponse aux menaces

Si Sandbox détecte une activité malveillante, Kaspersky Endpoint Security exécute automatiquement une action de réponse aux menaces (par exemple, il supprime l'objet et lance une analyse des zones critiques).

Pour configurer les actions de réponse aux menaces, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Sandbox**.

5. Sélectionnez l'action appropriée dans le groupe **Action en cas de détection d'une menace** :

   - **Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer l'objet, Kaspersky Endpoint Security crée une copie de sauvegarde au cas où l'objet devrait être restauré ultérieurement. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.

   - **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

   - **Créer la tâche Analyse IOC**. Si cette option est sélectionnée, Kaspersky Endpoint Security crée automatiquement la tâche *Analyse IOC (tâche autonome d'analyse IOC)*. Pour cette tâche, vous pouvez configurer le mode d'exécution, la zone d'analyse et l'action en cas de détection d'un IOC (*Placer la copie en Quarantaine, supprimer l'objet* ou *Lancer l'Analyse des zones critiques*). Pour modifier les autres paramètres de la tâche *Analyse IOC*, accédez aux paramètres de la tâche.

6. Si nécessaire, configurez les paramètres de la tâche *Analyse IOC* dans le groupe **Zone de l'analyse IOC**.

   - **Zones de fichiers critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security effectue une analyse IOC uniquement dans les zones de fichiers critiques de l'ordinateur : la mémoire du noyau et les secteurs d'amorçage.

   - **Zones de fichiers sur le disque système de l'ordinateur**. Si cette option est sélectionnée, Kaspersky Endpoint Security effectue une analyse IOC sur le disque système de l'ordinateur.

7. Si nécessaire, configurez les paramètres de la tâche *Analyse IOC* dans le groupe **Exécuter la tâche Analyse IOC**.

   - **Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer la tâche *Analyse IOC* manuellement à tout moment.

   - **Automatiquement**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute automatiquement la tâche *Analyse IOC* après la détection d'une menace.

   - **Exécuter uniquement lorsque l'ordinateur est inactif**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute la tâche *Analyse IOC* si l'écran de veille est actif ou si l'écran est verrouillé. Si l'utilisateur déverrouille l'ordinateur, Kaspersky Endpoint Security interrompt la tâche. Cela signifie que la tâche peut prendre plusieurs jours.

8. Configurez les paramètres de tâche avancés pour *Analyse IOC*.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Guide de migration KEA vers KES pour EDR (KATA)

À partir de la version 12.1, Kaspersky Endpoint Security for Windows inclut désormais un agent intégré pour la gestion du module Kaspersky Endpoint Detection and Response dans le cadre de la solution Kaspersky Anti Targeted Attack Platform. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser EDR (KATA). Toutes les fonctions de Kaspersky Endpoint Agent seront exécutées par Kaspersky Endpoint Security. La charge sur les serveurs de Kaspersky Anti Targeted Attack Platform restera la même.

Lorsque vous déployez Kaspersky Endpoint Security sur des ordinateurs sur lesquels Kaspersky Endpoint Agent est installé, la solution Kaspersky Anti Targeted Attack Platform (EDR) continuera à fonctionner avec Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur. Le même comportement dans le système se produira lors de la mise à jour de Kaspersky Endpoint Security vers la version 12.1 ou toute version ultérieure.

> Kaspersky Endpoint Security n'est pas compatible avec Kaspersky Endpoint Agent. Vous ne pouvez pas installer ces deux applications sur le même ordinateur.

Les conditions suivantes doivent être remplies pour que Kaspersky Endpoint Security fonctionne dans le cadre de Endpoint Detection and Response (KATA) :

- Kaspersky Anti Targeted Attack Platform version 5.0 ou toute version ultérieure.

- Kaspersky Security Center version 14.2 ou version ultérieure (y compris l'Agent d'administration). Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonctionnalité Endpoint Detection and Response (KATA).

Étapes de migration de la configuration [KES KEA] vers [KES+agent intégré] pour EDR (KATA)

1. **Mise à jour du plug-in d'administration de Kaspersky Endpoint Security**

   Le module EDR (KATA) peut être géré à l'aide du plug-in d'administration de Kaspersky Endpoint Security version 12.1 ou version ultérieure. Selon le type de console Kaspersky Security Center que vous utilisez, mettez à jour le plug-in d'administration dans la Console d'administration (MMC) ou le plug-in Internet dans Web Console.

2 **Migration des stratégies et des tâches**

Transférez les paramètres de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security for Windows. Les options suivantes existent :

- Un Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security. L'Assistant de migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security fonctionne uniquement dans Web Console

  Migration des paramètres de stratégies et de tâches depuis Kaspersky Endpoint Agent vers Kaspersky Endpoint Security dans Web Console

  Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Migration depuis Kaspersky Endpoint Agent**.

  Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

  Étape 1. Migration de stratégie

  L'Assistant de migration crée une stratégie que fusionne les paramètres des stratégies de Kaspersky Endpoint Security et Kaspersky Endpoint Agent. Dans la liste de stratégies, sélectionnez les stratégies de Kaspersky Endpoint Agent dont vous souhaitez fusionner les paramètres avec ceux de la stratégie de Kaspersky Endpoint Security. Cliquez sur une stratégie de Kaspersky Endpoint Agent pour sélectionner la stratégie Kaspersky Endpoint Security avec laquelle vous souhaitez fusionner les paramètres. Confirmez que vous avez sélectionné les bonnes stratégies, puis passez à l'étape suivante.

  Étape 2. Migration d'une tâche

  L'Assistant de migration ne prend pas en charge les tâches EDR (KATA). Ignorez cette étape.

  Étape 3. Fin de l'Assistant

  Quittez l'Assistant. À la suite de l'Assistant, une nouvelle stratégie de Kaspersky Endpoint Security sera créée. La stratégie fusionne les paramètres de Kaspersky Endpoint Security et Kaspersky Endpoint Agent La stratégie porte le nom *<Nom de stratégie de Kaspersky Endpoint Security> et <Nom de stratégie de Kaspersky Endpoint Agent>*. La nouvelle stratégie porte l'état *Inactive*. Pour continuer, changez l'état des stratégies de Kaspersky Endpoint Agent et Kaspersky Endpoint Security sur *Inactive* et activez la nouvelle stratégie fusionnée.

  L'Assistant de migration de Web Console ignore les paramètres de stratégie suivants et ne les migre pas :

  - Interdiction de modification des paramètres **Paramètres de connexion** (« cadenas »).

    Par défaut, les paramètres peuvent être modifiés (le « cadenas » est ouvert). Par conséquent, les paramètres ne sont pas appliqués sur l'ordinateur. Vous devez interdire la modification des paramètres et fermer le « cadenas ».

  - Conteneur crypto.

    Si vous utilisez l'authentification bidirectionnelle pour vous connecter aux serveurs de Central Node, vous devez rajouter le conteneur crypto.

Comme l'Assistant de migration ne migre pas ces paramètres, vous pouvez rencontrer des erreurs lors de la connexion de l'ordinateur aux serveurs de Central Node. Pour corriger les erreurs, vous devez accéder aux propriétés de la stratégie et configurer les paramètres de connexion.

- Un Assistant standard de conversion de masse des stratégies et des tâches L'Assistant de conversion de masse des stratégies et des tâches est uniquement disponible dans la Console d'administration (MMC). Pour en savoir plus sur l'Assistant de conversion de masse des stratégies et des tâches, consultez l'aide de Kaspersky Security Center.

Pour assurer le bon fonctionnement de Kaspersky Endpoint Security sur les serveurs, il est recommandé d'ajouter à la zone de confiance les fichiers importants pour le fonctionnement du serveur. Pour les serveurs SQL, vous devez ajouter des fichiers de base de données MDF et LDF. Pour les serveurs Microsoft Exchange, vous devez ajouter des fichiers CHK, EDB, JRS, LOG et JSL. Vous pouvez utiliser des masques, par exemple, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

Les exclusions de télémétrie EDR ne migrent pas de la politique de Kaspersky Endpoint Agent vers la politique de Kaspersky Endpoint Security. Kaspersky Endpoint Security dispose de ses propres outils d'exclusion - applications de confiance. Le fonctionnement de Kaspersky Endpoint Security est optimisé afin que l'absence d'exclusions de télémétrie EDR individuelles n'entraîne aucune charge supplémentaire sur votre ordinateur par rapport à Kaspersky Endpoint Agent. Kaspersky Endpoint Security utilise les données télémétriques non seulement pour EDR (KATA), mais également pour le fonctionnement des modules de protection des applications. Par conséquent, il n'est pas nécessaire de transférer les exclusions de télémétrie EDR individuelles. Si les performances de l'ordinateur diminuent, vérifiez le fonctionnement de l'application (voir étape 7 Vérification des performances).

3 Licence pour la fonctionnalité EDR (KATA)

Pour activer Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Anti Targeted Attack Platform, vous avez besoin d'une licence distincte pour le module complémentaire Kaspersky Endpoint Detection and Response (KATA). Vous pouvez ajouter la clé à l'aide de la tâche *Ajout d'une clé*. En conséquence, deux clés seront ajoutées à l'application : *Kaspersky Endpoint Security* et *Kaspersky Endpoint Detection and Response (KATA)*.

L'activation d'une licence pour le module complémentaire Kaspersky Endpoint Detection and Response (KATA) sur des ordinateurs disposant de fonctionnalités EDR Optimum ou EDR Expert préalablement activées implique les considérations spéciales suivantes :

- Si vous utilisez un *fichier clé* pour la licence de Kaspersky Endpoint Security avec les fonctionnalités EDR Optimum ou EDR Expert, vous ne pouvez pas ajouter une clé séparée pour le module complémentaire Kaspersky Endpoint Detection and Response (KATA). Vous pouvez soit passer à l'utilisation d'un code d'activation pour la licence, soit contacter votre fournisseur de services pour obtenir un nouveau fichier clé pour l'activation de Kaspersky Endpoint Security et des fonctionnalités EDR. Le fournisseur de services fournira un ou plusieurs fichiers clés pour l'octroi de licences.

- Si vous utilisez un *fichier clé* pour obtenir une licence Kaspersky Endpoint Security sans les fonctionnalités EDR Optimum ou EDR Expert, vous pouvez ajouter une clé séparée pour le module complémentaire Kaspersky Endpoint Detection and Response (KATA) sans que les fichiers clés ne soient réémis.

- Si vous utilisez un *code d'activation* pour les licences, le serveur d'activation de Kaspersky réémettra automatiquement les clés, et les fonctionnalités EDR (KATA) seront disponibles automatiquement. Dans ce cas, EDR Optimum et EDR Expert seront désactivés.

- Kaspersky Endpoint Security vous permet d'ajouter jusqu'à deux clés actives : la clé Kaspersky Endpoint Security et la clé de type module complémentaire. Vous pouvez également ajouter jusqu'à deux clés de réserve. Une clé de réserve Kaspersky Endpoint Security et une clé de réserve de type module complémentaire.

4. **Installation/Mise à jour de l'application Kaspersky Endpoint Security**

Pour migrer la fonctionnalité EDR (KATA) lors de l'installation ou de la mise à jour d'une application, il est recommandé d'utiliser la tâche d'installation à distance. Lors de la création d'une tâche d'installation à distance, vous devez sélectionner le module EDR (KATA) dans les paramètres du paquet d'installation.

Vous pouvez également mettre à jour l'application en utilisant les méthodes suivantes :

- À l'aide du service de mise à jour de Kaspersky.

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

Kaspersky Endpoint Security prend en charge la sélection automatique des modules lors de la mise à jour de l'application sur un ordinateur sur lequel est installée l'application Kaspersky Endpoint Agent. La sélection automatique des modules dépend des autorisations du compte utilisateur qui met à jour l'application.

Si vous mettez à jour Kaspersky Endpoint Security en utilisant le fichier EXE ou MSI sous le compte système (SYSTEM), Kaspersky Endpoint Security obtient l'accès aux licences valides des solutions Kaspersky. Par conséquent, si Kaspersky Endpoint Agent est installé et la solution EDR (KATA) est activée sur l'ordinateur, le programme d'installation de Kaspersky Endpoint Security configure automatiquement l'ensemble des modules et sélectionne le module EDR (KATA). Cette opération fait passer Kaspersky Endpoint Security à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent. L'exécution du programme d'installation MSI sous le compte système (SYSTEM) est généralement effectuée lors de la mise à jour via le service de mise à jour Kaspersky ou lors du déploiement d'un paquet d'installation via Kaspersky Security Center.

Si vous mettez à jour Kaspersky Endpoint Security à l'aide d'un fichier MSI sous un compte utilisateur non privilégié, Kaspersky Endpoint Security n'a pas accès aux licences valides des solutions Kaspersky. Dans ce cas, Kaspersky Endpoint Security sélectionne automatiquement les modules en fonction d'un ensemble de modules de Kaspersky Endpoint Agent. Après cela, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

Kaspersky Endpoint Security prend en charge la mise à jour sans redémarrage de l'ordinateur. Vous pouvez sélectionner le mode de mise à jour de l'application dans les propriétés de la stratégie.

5. **Vérification du fonctionnement de l'application**

Si après l'installation ou la mise à jour de l'application, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

- Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.

- Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous d'avoir activé la fonctionnalité d'agent intégré.

- Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

6. **Vérification de la connexion au serveur de Kaspersky Anti Targeted Attack Platform**

Vérifiez la connexion au serveur Kaspersky Anti Targeted Attack Platform. Pour ce faire, procédez comme suit :

1. Vérifiez que vous disposez d'un certificat valide.
2. Vérifiez les paramètres de connexion au serveur.
3. Vérifiez le journal des événements.

   Si une connexion au serveur est établie, l'application envoie l'événement *Connexion réussie au serveur EDR Expert*. S'il n'y a pas d'événement de connexion réussie et qu'il n'y a pas d'événements avec des erreurs de connexion, vérifiez les paramètres du journal des événements et activez l'envoi d'événements pour Endpoint Detection and Response (KATA).

L'état de la connexion au serveur n'affecte pas l'état de l'ordinateur dans la console Kaspersky Security Center. Par conséquent, s'il n'y a pas de connexion au serveur, l'ordinateur peut toujours avoir l'état *OK*. Consultez le journal des événements pour vérifier la connexion au serveur.

7 **Vérification des performances**

Si les performances de votre ordinateur ont ralenti après l'installation ou la mise à jour d'une application, vous pouvez optimiser le transfert de données. Pour ce faire, procédez comme suit :

1. Désactivez le module EDR (KATA) et vérifiez que la dégradation des performances est due à EDR (KATA).
2. Pour les applications de confiance, désactivez la collecte de données télémétriques sur les opérations d'entrée de console (activé par défaut).
3. Ajoutez des applications qui réduisent les performances de l'ordinateur à la liste des applications de confiance.
4. Contactez le support technique de Kaspersky. Les experts du support vous aideront à configurer le filtrage des données télémétriques dans Kaspersky Anti Targeted Attack Platform. La quantité de trafic sera réduite. Si les performances de votre ordinateur sont compromises par une application en particulier, joignez le paquet de distribution de l'application en question à votre demande.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows prend en charge l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* est une solution de cybersécurité d'entreprise qui comprend des applications Kaspersky permettant à une organisation de se défendre contre la plupart des types de cyber-risques et de faire face aux scénarios de propagation des menaces les plus importants. Les modules EDR Expert (on-premises) sont déployés sur Open Single Management Platform (OSMP). Cette plateforme exécute des scénarios multiplateformes dans une interface unique et permet d'intégrer des applications Kaspersky avec des applications tierces dans un système de sécurité complet.

L'un des éléments centraux de la solution est *SIEM*. Le SIEM suit les événements provenant de tous les modules et les met en corrélation les uns avec les autres à l'aide de règles définies par le fournisseur et l'utilisateur. EDR Expert (on-premises) examine les données télémétriques et les journaux reçus de l'infrastructure de l'entreprise pour détecter automatiquement les attaques et permet d'enquêter sur les incidents à l'aide d'un graphique d'enquête unifié qui combine tous les événements collectés dans EDR Expert (on-premises), y compris les événements provenant des applications Kaspersky et des produits de sécurité informatique tiers.

Pour la réponse aux incidents avancés, EDR Expert (on-premises) utilise des scénarios prédéfinis et définis par l'utilisateur. Vous pouvez également utiliser des actions de réponse à partir d'applications tierces et des scénarios de réponse qui impliquent plusieurs applications.

Outils de Threat Intelligence

Kaspersky Endpoint Detection and Response utilise les outils Threat Intelligence suivants :

- L'intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations concernant la réputation des fichiers et des adresses Internet.
- La base de données Kaspersky Threats.
- L'infrastructure du service Cloud Kaspersky Security Network (ci-après également appelé "KSN"), qui donne accès à des informations en temps réel sur la réputation des fichiers, des sites Internet et des logiciels à partir de la base de connaissances de Kaspersky. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de protection et réduit la possibilité de faux positifs.

Principe de fonctionnement de la solution

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification.

> Lorsqu'il est installé en mode standard dans l'infrastructure VDI, Kaspersky Endpoint Security prend en charge l'intégration avec EDR Expert (on-premises). Cependant, le fonctionnement des autres fonctionnalités de l'application n'est pas garanti. Pour protéger les machines virtuelles dans l'infrastructure VDI, nous vous recommandons d'utiliser Kaspersky Endpoint Security en mode Light Agent.

Les informations (télémétrie) sur les événements survenus sur l'ordinateur sont envoyées au serveur EDR Expert (on-premises). Dans ce cas, Kaspersky Endpoint Security envoie également aux serveurs de collecte de données télémétriques des informations sur les menaces détectées par l'application, ainsi que des informations sur les résultats du traitement de ces menaces.

L'intégration de EDR Expert (on-premises) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la plateforme Open Single Management Platform (OSMP), y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Configurations de Kaspersky Endpoint Security pour utiliser EDR Expert (on-premises)

Les configurations suivantes peuvent être appliquées pour utiliser EDR Expert (on-premises) :

- **[KES+agent intégré]**. Dans cette configuration, Kaspersky Endpoint Security agit à la fois comme une application assurant la sécurité de l'ordinateur et comme une application permettant d'utiliser EDR Expert (on-premises). L'agent intégré pour EDR Expert (on-premises) est disponible dans Kaspersky Endpoint Security 12.11 for Windows et toute version ultérieure.

- **[PPE tierce+EDR Agent]**. Dans cette configuration, la sécurité de l'infrastructure informatique est assurée par la Endpoint Protection Platform (PPE) tierce. L'interaction avec EDR Expert (on-premises) est assurée par Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent (EDR Agent). Dans cette configuration, EDR Agent est compatible avec les applications PPE tierces. EDR Agent pour EDR Expert (on-premises) est disponible dans Kaspersky Endpoint Security 12.11 for Windows et toute version ultérieure.

Intégration de l'agent intégré avec EDR Expert (on-premises)

Pour intégrer la solution Kaspersky Endpoint Detection and Response Expert (on-premises), vous devez ajouter le module Endpoint Detection and Response Expert (on-premises) et configurer Kaspersky Endpoint Security.

> Les modules Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises) ne sont pas compatibles entre eux.

Les conditions suivantes doivent être remplies pour que Endpoint Detection and Response Expert (on-premises) fonctionne :

- La plateforme OSMP (Open Single Management Platform) est installée.

- L'application est activée, et la fonctionnalité est couverte par la licence.

- Le module Endpoint Detection and Response Expert (on-premises) est activé.

- Les modules de l'application qui garantissent le fonctionnement d'EDR Expert (on-premises) sont activés et opérationnels. Les modules suivants assurent le fonctionnement d'EDR Expert (on-premises) :

  - Protection contre les fichiers malicieux.

  - Protection contre les menaces Internet.

  - Protection contre les menaces par emails.

  - Protection contre les Exploits.

  - Détection comportementale.

  - Prévention des intrusions.

  - Réparation des actions malicieuses.

  - Contrôle évolutif des anomalies.

La configuration de l'Intégration EDR Expert (on-premises) comprend les étapes suivantes :

1. **Installation du module EDR Expert (on-premises)**

   Vous pouvez sélectionner le module EDR Expert (on-premises) lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   Vous devez redémarrer votre ordinateur pour terminer la mise à jour de l'application avec le nouveau module.

2. **Activation de Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Vous devez acheter une licence distincte pour EDR Expert (on-premises) (module complémentaire de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response Expert (on-premises). Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour Kaspersky Endpoint Detection and Response Expert (on-premises).

   La licence de la fonctionnalité autonome Endpoint Detection and Response Expert (on-premises) est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité EDR Expert (on-premises) est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

3. **Connexion au serveur de collecte de données télémétriques et au serveur de réponse**

   Kaspersky Endpoint Detection and Response Expert (on-premises) nécessite une connexion de confiance entre Kaspersky Endpoint Security et deux serveurs :

   - Un *serveur de collection de télémétrie* est un serveur qui fait partie d'une solution SIEM et qui collecte, normalise, corrèle, analyse et stocke les informations relatives aux événements qui se produisent sur l'ordinateur.
   - Un *serveur de réponse* est un serveur pour la réception et l'analyse des données, l'étude du comportement d'objets et la publication des résultats.

   Pour configurer une connexion sécurisée, vous devez utiliser un certificat TLS. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).

   Par défaut, Kaspersky Endpoint Security vérifie uniquement le certificat TLS des serveurs. Pour rendre la connexion plus sécurisée, vous pouvez en outre activer la vérification de l'ordinateur sur le serveur (authentification bidirectionnelle). Pour activer cette vérification, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur et de Kaspersky Endpoint Security. Pour utiliser l'authentification bidirectionnelle, vous aurez également besoin d'un conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Comment connecter un ordinateur Kaspersky Endpoint Security au module EDR Expert (on-premises) à l'aide de Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.

5. Activez le commutateur **Endpoint Detection and Response Expert (on-premises) ACTIVÉ**.

6. Pour configurer EDR Expert (on-premises), sélectionnez **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)** dans la liste des solutions.

7. Configurez la connexion au *serveur de collecte de données télémétriques* :

   a. Dans le groupe **Connexion aux serveurs de collecte de données télémétriques**, cliquez sur le lien **Paramètres de connexion**.

   b. Configurez la connexion au serveur de collecte de données télémétriques :

      - **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.

      - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe.

        Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   c. Cliquez sur **OK**.

   d. Ajoutez des serveurs de collecte de données télémétriques. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

      Vous pouvez ajouter plusieurs adresses de serveur de collecte de données télémétriques. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

   e. En cas de nécessité, configurez la télémétrie.

8. Configurez la connexion des *serveurs de réponse* :

   a. Configurez le paramètre **Envoyer une demande de synchronisation au serveur toutes les (min.)** dans le groupe **Connexion aux serveurs de réponse**. Fréquence des requêtes de synchronisation envoyées au serveur. Pendant la synchronisation, Kaspersky Endpoint Security reçoit les tâches de réponse aux menaces et envoie les résultats des tâches.

   b. Cliquez sur le lien **Paramètres de connexion**.

   c. Configurez la connexion des serveurs de réponse :

      - **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.

      - **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe.

        Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   d. Cliquez sur **OK**.

   e. Ajoutez des serveurs de réponse. Pour ce faire, indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au serveur.

      Vous pouvez ajouter plusieurs adresses de serveur de réponse. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Vous pouvez vérifier l'état du module à l'aide de *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 **Endpoint Detection and Response Expert (on-premises)** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Configuration des paramètres de la télémétrie EDR Expert (on-premises)

Télémétrie est une liste d'événements qui se sont produits sur l'ordinateur protégé. Kaspersky Endpoint Security analyse les données de télémétrie et les envoie aux serveurs de collecte de données télémétriques lors de la synchronisation. Pour en savoir plus sur les événements de télémétrie transmis, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

Les événements de télémétrie arrivent presque continuellement sur le serveur. Kaspersky Endpoint Security lance la synchronisation avec le serveur lorsque l'une des conditions suivantes est remplie :

- L'intervalle de synchronisation est écoulé.
- Le nombre d'événements dans la mémoire tampon dépasse la limite supérieure.

Par conséquent, par défaut, l'application se synchronise toutes les 30 secondes ou chaque fois que la mémoire tampon contient 1 024 événements. Vous pouvez configurer le comportement de synchronisation dans la stratégie de Kaspersky Endpoint Security et sélectionner les valeurs optimales en fonction de la charge de votre réseau (voir les instructions ci-dessous).

S'il n'y a pas de connexion entre Kaspersky Endpoint Security et le serveur, l'application met les nouveaux événements en file d'attente. Lorsque la connexion est rétablie, Kaspersky Endpoint Security envoie les événements de la file d'attente au serveur dans le bon ordre. Pour éviter de surcharger le serveur, Kaspersky Endpoint Security peut ignorer certains événements. Pour cela, vous pouvez optimiser les paramètres de transmission des événements, par exemple, pour définir une valeur maximale d'événements par heure (voir les instructions ci-dessous).

Pour configurer les paramètres de télémétrie, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.
5. Pour configurer EDR Expert (on-premises), sélectionnez **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)** dans la liste des solutions.
6. Assurez-vous que la case **Envoyer les données télémétriques aux serveurs de collecte de données télémétriques** est cochée dans le groupe **Paramètres de transmission des données**.
7. Le cas échéant, cochez la case **Envoyer la télémétrie avec l'IOA uniquement**. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements.

8. Si nécessaire, configurez la synchronisation avec les paramètres du serveur dans le groupe **Paramètres de transmission des données** :

   - **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.

   - **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.

9. Si nécessaire, décochez la case **Activer la limitation des demandes** dans le groupe **Limitation des demandes**.

   Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Cette option est activée par défaut.

10. Configurez les paramètres d'optimisation pour l'envoi d'événements au serveur :

    - **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.

    - **Pourcentage de la limite d'événement excédentaire**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

11. Dans le bloc **Connexion aux serveurs de réponse**, saisissez une valeur pour le paramètre **Envoyer une demande de synchronisation au serveur toutes les (min.)**.

12. Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.

13. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Exclusions de la télémétrie EDR Expert (on-premises)

Pour améliorer les performances et optimiser la transmission des données vers le serveur de collecte de données télémétriques, vous pouvez ajouter des exclusions de télémétrie. Par exemple, vous pouvez choisir de ne pas envoyer les données de communication réseau pour certaines applications.

> L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte de données télémétriques et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Pour créer une exclusion de télémétrie dans Web Console et Cloud Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
5. Sélectionnez l'onglet **Télémétrie EDR Expert (on-premises)**.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions générales**.
   La fenêtre **Ajouter une règle d'exclusion** s'ouvre.
7. Si nécessaire, modifiez l'état de la règle. Par défaut, la règle est activée.
8. Saisissez un nom pour la règle.
9. Sélectionnez l'action à effectuer lorsque la règle est déclenchée :
   - **Ne pas collecter**. L'événement filtré sera exclu des données télémétriques envoyées.
   - **Exclure l'IOA**. L'événement déclencheur de la règle IOA sera exclu des données télémétriques envoyées.
10. Si l'option **Exclure l'IOA** est sélectionnée, indiquez les règles IOA à ajouter aux exclusions :
    - **Tout exclure**. Quand la condition indiquée est remplie, l'application exclut de la télémétrie les événements générés sur la base de toutes les règles IOA.
    - **Exclure par GUID**. Spécifiez le GUID de la règle IOA. Vous pouvez spécifier plusieurs GUID en utilisant le séparateur « `,` ». Pour en savoir plus sur les règles IOA, veuillez consulter l'aide relative à EDR Expert (on-premises).
11. Indiquez la condition de filtrage :
    a. Sélectionnez le nom du champ à utiliser pour le filtrage.
    b. Sélectionnez un opérateur (cf. le tableau ci-dessous) et indiquez la valeur à laquelle la valeur de champ de l'événement sera comparée.

Liste des opérateurs conditionnels

Opérateur	Description
<	Si la valeur du champ est inférieure à la valeur indiquée dans la condition, l'événement est filtré.
≤	Si la valeur du champ est inférieure ou égale à la valeur indiquée dans la condition, l'événement est filtré.
=	Si la valeur du champ est égale à la valeur indiquée dans la condition, l'événement est filtré.
≥	Si la valeur du champ est supérieure ou égale à la valeur spécifiée dans la condition, l'événement est filtré.
>	Si la valeur du champ est supérieure à la valeur spécifiée dans la condition, l'événement est filtré.
≠	Si la valeur du champ est différente de la valeur indiquée dans la condition, l'événement est filtré.
ressemble à	Si la valeur du champ correspond au masque spécifié dans la condition, l'événement est filtré. L'application prend en charge les caractères `*` et `?` lors de la saisie d'un masque :

Opérateur	Description
différent	Si la valeur du champ ne correspond pas au masque spécifié dans la condition, l'événement est filtré. L'application prend en charge les caractères `*` et `?` lors de la saisie d'un masque :
un des	Si la valeur du champ correspond à l'une des valeurs de la liste spécifiée dans la condition, l'événement est considéré comme filtré.
aucun des	Si la valeur du champ ne correspond à aucune des valeurs de la liste spécifiée dans la condition, l'événement est considéré comme filtré.
est comme un des	Si la valeur du champ correspond à l'un des masques spécifiés dans la condition, l'événement est filtré. L'application prend en charge les caractères * et ? lors de la saisie d'un masque.
n'est pas comme un des	Si la valeur du champ ne correspond à aucun des masques spécifiés dans la condition, l'événement est filtré. L'application prend en charge les caractères * et ? lors de la saisie d'un masque.
existe	Si le champ spécifié dans la condition est présent dans l'événement, l'événement est filtré.
n'existe pas	Si le champ spécifié dans la condition n'est pas présent dans l'événement, l'événement est filtré.
contient	Si la valeur spécifiée dans la condition figure dans le champ valeur, l'événement est filtré.
est égal à	Si la valeur du champ est égale à la valeur indiquée dans la condition, l'événement est filtré. L'analyse ne respecte pas la casse.
ET bit à bit	Si le résultat de l'opération ET binaire (&) entre la valeur du champ et la valeur spécifiée dans la condition est égal à 1, l'événement est filtré.

12. Si nécessaire, vous pouvez créer des critères de filtrage complexes en ajoutant plusieurs conditions de filtrage et des groupes de conditions. Vous pouvez également ajouter des conditions imbriquées et des groupes de conditions à un groupe de conditions. Vous pouvez utiliser les opérateurs suivants :

    - **ET** signifie que le filtre sélectionne les événements qui remplissent toutes les conditions spécifiées.
    - **OU** signifie que le filtre sélectionne les événements qui remplissent une des conditions spécifiées.
    - **NON** (pour utiliser cet opérateur, il faut sélectionner l'option **Ajouter NON devant**) signifie que le filtre sélectionne les événements qui ne remplissent aucune des conditions spécifiées.

    Les conditions et les groupes de conditions de premier niveau sont combinés avec l'opérateur **ET**.

13. Si votre ordinateur utilise la plateforme Open Single Management Platform (OSMP), vous pouvez analyser la règle de filtrage que vous avez créée. Pour lancer l'analyse, cliquez sur le bouton **Vérifier la règle**.

    Dans la fenêtre qui s'ouvre, un tableau des événements filtrés en fonction de la règle créée s'affiche. Pour en savoir plus, veuillez consulter l'Aide relative à EDR Expert (on-premises).

14. Le cas échéant, sous **Tous les types d'événements**, ajoutez des exclusions de télémétrie par type d'événement.

    a. Cliquez sur le nom du type d'événement.

    b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Configurer manuellement**.

    c. Configurez, si nécessaire, la transmission télémétrique pour le type d'événement sélectionné à l'aide du commutateur **Envoyer l'événement**. Par défaut, la transmission télémétrique est activée pour tous les types d'événements.

    d. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'exclusion**.

    La fenêtre **Ajouter une règle d'exclusion** s'ouvre.

    e. Exécutez les actions décrites aux étapes 7 à 13 pour chaque règle ajoutée.

15. Pour certains types d'événements, vous pouvez également ajouter des règles d'inclusion pour étendre la télémétrie collectée :

    a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'inclusion**.

       La fenêtre **Ajouter des règles d'inclusion** s'ouvre.

    b. Saisissez un nom pour la règle.

    c. Sous **Condition**, saisissez les valeurs des champs affichés. Le type de champs disponibles dépend de l'événement sélectionné.

> Les règles d'exclusion ont la priorité sur les règles d'inclusion.

16. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Exportation et importation de filtres d'événements EDR Expert (on-premises)

Vous pouvez exporter la liste des exclusions dans un fichier JSON. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'identifiants d'événements. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder les filtres d'événements ou pour migrer la liste vers un autre serveur.

> L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte de données télémétriques et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Comment exporter et importer des filtres d'événements dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la télémétrie** → **Télémétrie EDR Expert (on-premises)**.

6. Pour exporter les filtres d'événements, procédez comme suit :

    a. Cliquez sur **Exporter**.

       Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

    b. Enregistrez le fichier.

       Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.

7. Pour importer les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

   c. Ouvrez le fichier.

      Si des règles de filtrage des événements existent déjà sur l'ordinateur, Kaspersky Endpoint Security les remplace lors de l'importation.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exporter et importer des filtres d'événements dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie EDR Expert (on-premises)**.

6. Pour exporter les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Exporter**.

   b. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   c. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.

7. Pour importer les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

   c. Sélectionnez la méthode d'importation des règles de filtrage des événements : en les ajoutant aux règles existantes ou en supprimant les règles existantes et en les remplaçant par de nouvelles.

   d. Ouvrez le fichier.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Vous pouvez également exporter ou importer des filtres d'événements à partir de la ligne de commande.

Points à prendre en compte lors de l'utilisation de profils de stratégie pour configurer l'intégration avec EDR Expert (on-premises) et EDR (KATA)

Pour configurer l'intégration avec EDR (KATA) pour certains groupes d'administration et avec EDR Expert (on-premises) pour d'autres dans le cadre d'une même stratégie, vous devez utiliser des profils de stratégie. Vous devez configurer les paramètres d'intégration avec EDR (KATA) dans les propriétés de la stratégie, tandis que l'intégration avec EDR Expert (on-premises) pour les groupes d'administration sélectionnés doit être configurée dans les propriétés du profil de stratégie.

L'utilisation de profils de stratégie pour configurer l'intégration avec EDR Expert (on-premises) présente les limitations suivantes :

- Si vous configurez l'intégration avec EDR Expert (on-premises) dans les propriétés de la stratégie, ces paramètres s'appliquent à tous les groupes d'administration ; les paramètres d'intégration des profils de stratégie ne seront pas appliqués.
- Lorsque vous utilisez des profils de stratégie pour configurer l'intégration avec EDR Expert (on-premises), vous ne pouvez pas utiliser la Console d'administration (MMC) pour administrer les stratégies. Lorsque vous ouvrez les propriétés de la stratégie dans la Console d'administration, les paramètres d'intégration avec EDR Expert (on-premises) dans les profils de stratégie sont remplacés par les paramètres de la stratégie, ce qui entraîne le dysfonctionnement du module. Vous devez réinitialiser les paramètres du module Endpoint Detection and Response Expert (on-premises) conformément aux instructions ci-dessous.
- Lorsque vous utilisez des profils de stratégie pour configurer l'intégration avec EDR Expert (on-premises), vous ne pouvez pas utiliser de stratégies enfants.

Si une stratégie est déjà configurée dans une version précédente du plug-in Internet, vous devez réinitialiser les paramètres du module Endpoint Detection and Response Expert (on-premises) afin d'appliquer aux appareils administrés les paramètres d'intégration avec EDR Expert (on-premises) provenant des profils de stratégie.

Pour réinitialiser les paramètres du module :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premises)**.
5. Changez le mode de fonctionnement de **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)** à **Mode Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)**.
6. Revenez à **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)**.
7. Enregistrez vos modifications.

Endpoint Detection and Response Expert (cloud)

L'intégration de Kaspersky Endpoint Security à Kaspersky Endpoint Detection and Response Expert (cloud) est temporairement indisponible. Il est prévu que cette fonctionnalité soit prise en charge d'ici fin 2026. Consultez régulièrement nos notes de mise à jour pour vous tenir informé des mises à jour des applications et des nouvelles fonctionnalités.

Kaspersky Endpoint Security prend en charge l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* est une solution de cybersécurité d'entreprise basée sur le cloud qui comprend des applications Kaspersky permettant à une organisation de se défendre contre la plupart des types de cyberrisques et de faire face aux scénarios de propagation des menaces les plus importants. Les modules EDR Expert (cloud) sont déployés sur le Open Single Management Platform (OSMP). Cette plateforme exécute des scénarios multiplateformes dans une interface unique et permet d'intégrer des applications Kaspersky avec des applications tierces dans un système de sécurité complet.

L'un des éléments centraux de la solution est *SIEM*. Le SIEM suit les événements provenant de tous les modules et les met en corrélation les uns avec les autres à l'aide de règles définies par le fournisseur et l'utilisateur. EDR Expert (cloud) examine les données télémétriques et les journaux reçus de l'infrastructure de l'entreprise pour détecter automatiquement les attaques et permet d'enquêter sur les incidents à l'aide d'un graphique d'enquête unifié qui combine tous les événements collectés dans EDR Expert (cloud), y compris les événements provenant des applications Kaspersky et des produits de sécurité informatique tiers.

Pour la réponse aux incidents avancés, EDR Expert (cloud) utilise des scénarios prédéfinis et définis par l'utilisateur. Vous pouvez également utiliser des actions de réponse à partir d'applications tierces et des scénarios de réponse qui impliquent plusieurs applications.

Outils de Threat Intelligence

Kaspersky Endpoint Detection and Response utilise les outils Threat Intelligence suivants :

- L'intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations concernant la réputation des fichiers et des adresses Internet.
- La base de données Kaspersky Threats.
- L'infrastructure du service Cloud Kaspersky Security Network (ci-après également appelé "KSN"), qui donne accès à des informations en temps réel sur la réputation des fichiers, des sites Internet et des logiciels à partir de la base de connaissances de Kaspersky. L'utilisation des données de Kaspersky Security Network permet aux applications de Kaspersky de réagir plus rapidement aux menaces, augmente l'efficacité de fonctionnement de certains modules de protection et réduit la possibilité de faux positifs.

Principe de fonctionnement de la solution

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification.

Les informations (télémétrie) sur les événements survenus sur l'ordinateur sont envoyées au serveur EDR Expert (cloud). Dans ce cas, Kaspersky Endpoint Security envoie également aux serveurs de collecte de données télémétriques des informations sur les menaces détectées par l'application, ainsi que des informations sur les résultats du traitement de ces menaces.

L'intégration de EDR Expert (cloud) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la plateforme Open Single Management Platform (OSMP), y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Intégration de l'agent intégré avec EDR Expert (cloud)

Pour configurer l'intégration avec la solution Kaspersky Endpoint Detection and Response (cloud), vous devez installer le module Endpoint Detection and Response Expert (cloud) et configurer Kaspersky Endpoint Security.

Les modules Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) et Endpoint Detection and Response Expert (on-premises) ne sont pas compatibles entre eux.

Conditions de fonctionnement d'EDR Expert (cloud)

Pour qu'EDR Expert (cloud) fonctionne, les conditions suivantes doivent être remplies :

- L'infrastructure Kaspersky Endpoint Detection and Response Expert (cloud) est disponible dans votre région. Pour en savoir plus sur la disponibilité de l'infrastructure EDR Expert (cloud) dans votre région, veuillez contacter le Support technique.
- La plateforme OSMP (Open Single Management Platform) est installée.
- Kaspersky Endpoint Security installé en mode standard.
- Kaspersky Endpoint Security est activé, et la fonctionnalité est couverte par la licence.
- Vous avez accepté les conditions du Contrat de traitement des données de Kaspersky Endpoint Detection and Response Expert (cloud).
- Le module Endpoint Detection and Response Expert (cloud) est activé.
- Les modules de l'application qui garantissent le fonctionnement d'EDR Expert (cloud) sont activés et opérationnels :
  - Protection contre les fichiers malicieux.
  - Protection contre les menaces Internet.
  - Protection contre les menaces par emails.
  - Protection contre les Exploits.
  - Détection comportementale.
  - Prévention des intrusions.

- Réparation des actions malicieuses.
- Contrôle évolutif des anomalies.

Étapes de l'intégration à EDR Expert (cloud)

La configuration de l'Intégration EDR Expert (cloud) comprend les étapes suivantes :

1. **Installation du module Endpoint Detection and Response Expert (cloud)**

   Vous pouvez sélectionner le module Endpoint Detection and Response Expert (cloud) lors de l'installation ou de la mise à jour ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   > Vous devez redémarrer votre ordinateur pour terminer la mise à jour de l'application avec le nouveau module.

2. **Activation de Kaspersky Endpoint Detection and Response Expert (cloud)**

   Vous devez acheter une licence distincte pour Kaspersky Endpoint Detection and Response Expert (cloud).

   La fonctionnalité devient disponible après l'ajout d'une clé distincte pour Kaspersky Endpoint Detection and Response Expert (cloud). Par conséquent, deux clés sont ajoutées à l'ordinateur : une clé pour Kaspersky Endpoint Security et une clé pour Kaspersky Endpoint Detection and Response Expert (cloud).

   La licence de la fonctionnalité autonome Endpoint Detection and Response Expert (cloud) est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité EDR Expert (cloud) est incluse dans la licence et qu'elle est exécutée dans l'interface locale de l'application.

3. **Connexion au serveur de collecte de données télémétriques et au serveur de réponse**

   Kaspersky Endpoint Detection and Response Expert (cloud) nécessite une connexion de confiance entre Kaspersky Endpoint Security et deux serveurs :

   - Un *serveur de collection de télémétrie* est un serveur qui fait partie d'une solution SIEM et qui collecte, normalise, corrèle, analyse et stocke les informations relatives aux événements qui se produisent sur l'ordinateur.
   - Un *serveur de réponse* est un serveur pour la réception et l'analyse des données, l'étude du comportement d'objets et la publication des résultats.

   Comment connecter un ordinateur Kaspersky Endpoint Security au module EDR Expert (cloud) à l'aide de Web Console

   1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
   2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

      La fenêtre des propriétés de la stratégie s'ouvre.
   3. Sélectionnez l'onglet **Paramètres de l'application**.
   4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (cloud)**.

5. Activez le module à l'aide du commutateur **Endpoint Detection and Response Expert (cloud) DÉSACTIVÉ**.

6. Si la stratégie actuelle est une stratégie enfant et que la stratégie parent interdit la modification des paramètres d'intégration d'EDR Expert (cloud) (« cadenas » fermé), vous pouvez configurer l'héritage des paramètres dans la section **Héritage** :

   - **Hériter des paramètres de connexion de la stratégie** (valeur par défaut). Les paramètres de connexion sont hérités de la stratégie parent. Vous ne pourrez pas modifier les paramètres.

   - **Utiliser des paramètres de connexion personnalisés**. Vous pouvez configurer les paramètres de connexion manuellement.

7. L'onglet **Serveur de réponse** affiche le nom de domaine complet et le port du serveur de réponse, qui sont récupérés automatiquement. Si la stratégie de sécurité de votre infrastructure ne vous permet pas de vous connecter directement aux serveurs d'EDR Experts (cloud), vous pouvez établir une connexion via un tunnel TCP :

   a. Cochez la case **Utiliser un tunnel TCP pour la réponse**.

   b. Indiquez l'adresse du serveur (IPv4, IPv6) et le port de connexion au tunnel.

8. Si nécessaire, définissez la fréquence d'envoi des demandes de synchronisation au serveur dans le champ **Envoyer une demande de synchronisation au serveur toutes les (min.)**. Pendant la synchronisation, Kaspersky Endpoint Security reçoit les tâches de réponse aux menaces et envoie les résultats des tâches.

9. Rendez-vous dans l'onglet **Serveur de collecte de données télémétriques**.

10. Configurez les paramètres de connexion au serveur de collecte des données de télémétrie :

    a. Cliquez sur le lien **Modifier**.

    b. Dans la fenêtre qui s'ouvre, sélectionnez le serveur de collecte de données télémétriques dans la liste. Le collecteur KUMA sert de serveur de collecte de données télémétriques dans EDR Expert (cloud). Pour en savoir plus, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

    Si une erreur se produit lors de la connexion au serveur de collecte de données télémétriques, sélectionnez un autre serveur. Si vous ne parvenez pas à vous connecter au serveur de collecte de données télémétriques, veuillez contacter le Support technique.

    c. Si nécessaire, vous pouvez configurer une connexion au serveur de collecte de données télémétriques via un tunnel TCP, comme vous le feriez pour le serveur de réponse.

11. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Vous pouvez vérifier l'état du module à l'aide de *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 **Endpoint Detection and Response Expert (cloud)** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Configuration des paramètres de la télémétrie EDR Expert (cloud)

Télémétrie est une liste d'événements qui se sont produits sur l'ordinateur protégé. Kaspersky Endpoint Security analyse les données de télémétrie et les envoie aux serveurs de collecte de données télémétriques lors de la synchronisation. Les événements de télémétrie arrivent presque continuellement sur le serveur. Kaspersky Endpoint Security lance la synchronisation avec le serveur lorsque l'une des conditions suivantes est remplie :

- L'intervalle de synchronisation est écoulé.
- Le nombre d'événements dans la mémoire tampon dépasse la limite supérieure.

Par conséquent, par défaut, l'application se synchronise toutes les 30 secondes ou chaque fois que la mémoire tampon contient 1 024 événements. Vous pouvez configurer le comportement de synchronisation dans la stratégie de Kaspersky Endpoint Security et sélectionner les valeurs optimales en fonction de la charge de votre réseau (voir les instructions ci-dessous).

S'il n'y a pas de connexion entre Kaspersky Endpoint Security et le serveur, l'application met les nouveaux événements en file d'attente. Lorsque la connexion est rétablie, Kaspersky Endpoint Security envoie les événements de la file d'attente au serveur dans le bon ordre. Pour éviter de surcharger le serveur, Kaspersky Endpoint Security peut ignorer certains événements. Pour cela, vous pouvez optimiser les paramètres de transmission des événements, par exemple, pour définir une valeur maximale d'événements par heure (voir les instructions ci-dessous).

Pour configurer les paramètres de télémétrie, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (cloud)**.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres de transmission des données**.
6. Assurez-vous que la case **Envoi des données télémétriques ACTIVÉ** est cochée.
7. Si nécessaire, activez la fonctionnalité **Envoyer la télémétrie avec l'IOA uniquement**. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements. Par défaut, la fonctionnalité est désactivée.

8. Si nécessaire, configurez les paramètres de synchronisation du serveur :

   - **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.

   - **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.

9. Rendez-vous dans l'onglet **Limitation des demandes**.

10. Si nécessaire, désactivez la limitation des demandes à l'aide du commutateur **Limitation des demandes ACTIVÉE**.

    Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Cette option est activée par défaut.

11. Configurez les paramètres d'optimisation pour l'envoi d'événements au serveur :

    - **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.

    - **Pourcentage de la limite d'événement excédentaire (%)**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

12. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas 🔒 et enregistrez vos modifications.

Exclusions de la télémétrie EDR Expert (cloud)

Pour améliorer les performances et optimiser la transmission des données vers le serveur de collecte de données télémétriques, vous pouvez ajouter des exclusions de télémétrie. Par exemple, vous pouvez choisir de ne pas envoyer les données de communication réseau pour certaines applications.

> L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte de données télémétriques et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Pour créer une exclusion de télémétrie dans Web Console et Cloud Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.

6. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions générales**.
   La fenêtre **Ajouter une règle d'exclusion** s'ouvre.

7. Si nécessaire, modifiez l'état de la règle. Par défaut, la règle est activée.

8. Saisissez un nom pour la règle.

9. Sélectionnez l'action à effectuer lorsque la règle est déclenchée :

   - **Ne pas collecter**. L'événement filtré sera exclu des données télémétriques envoyées.

   - **Exclure l'IOA**. L'événement déclencheur de la règle IOA sera exclu des données télémétriques envoyées.

10. Si l'option **Exclure l'IOA** est sélectionnée, indiquez les règles IOA à ajouter aux exclusions :

    - **Tout exclure**. Quand la condition indiquée est remplie, l'application exclut de la télémétrie les événements générés sur la base de toutes les règles IOA.

    - **Exclure par GUID**. Spécifiez le GUID de la règle IOA. Vous pouvez spécifier plusieurs GUID en utilisant le séparateur « `,` ». Pour en savoir plus sur les règles IOA, veuillez consulter l'aide relative à EDR Expert (cloud).

11. Indiquez la condition de filtrage :

    a. Sélectionnez le nom du champ à utiliser pour le filtrage.

    b. Sélectionnez un opérateur (cf. le tableau ci-dessous) et indiquez la valeur à laquelle la valeur de champ de l'événement sera comparée.

Liste des opérateurs conditionnels

Opérateur	Description
<	Si la valeur du champ est inférieure à la valeur indiquée dans la condition, l'événement est filtré.
≤	Si la valeur du champ est inférieure ou égale à la valeur indiquée dans la condition, l'événement est filtré.
=	Si la valeur du champ est égale à la valeur indiquée dans la condition, l'événement est filtré.
≥	Si la valeur du champ est supérieure ou égale à la valeur spécifiée dans la condition, l'événement est filtré.
>	Si la valeur du champ est supérieure à la valeur spécifiée dans la condition, l'événement est filtré.
≠	Si la valeur du champ est différente de la valeur indiquée dans la condition, l'événement est filtré.
ressemble à	Si la valeur du champ correspond au masque spécifié dans la condition, l'événement est filtré. L'application prend en charge les caractères `*` et `?` lors de la saisie d'un masque :
différent	Si la valeur du champ ne correspond pas au masque spécifié dans la condition, l'événement est filtré. L'application prend en charge les caractères `*` et `?` lors de la saisie d'un masque :
un des	Si la valeur du champ correspond à l'une des valeurs de la liste spécifiée dans la condition, l'événement est considéré comme filtré.
aucun des	Si la valeur du champ ne correspond à aucune des valeurs de la liste spécifiée dans la condition, l'événement est considéré comme filtré.
est comme un des	Si la valeur du champ correspond à l'un des masques spécifiés dans la condition, l'événement est filtré. L'application prend en charge les caractères * et ? lors de la saisie d'un masque.
n'est pas comme un des	Si la valeur du champ ne correspond à aucun des masques spécifiés dans la condition, l'événement est filtré. L'application prend en charge les caractères * et ? lors de la saisie d'un masque.

Opérateur	Description
existe	Si le champ spécifié dans la condition est présent dans l'événement, l'événement est filtré.
n'existe pas	Si le champ spécifié dans la condition n'est pas présent dans l'événement, l'événement est filtré.
contient	Si la valeur spécifiée dans la condition figure dans le champ valeur, l'événement est filtré.
est égal à	Si la valeur du champ est égale à la valeur indiquée dans la condition, l'événement est filtré. L'analyse ne respecte pas la casse.
ET bit à bit	Si le résultat de l'opération ET binaire (&) entre la valeur du champ et la valeur spécifiée dans la condition est égal à 1, l'événement est filtré.

12. Si nécessaire, vous pouvez créer des critères de filtrage complexes en ajoutant plusieurs conditions de filtrage et des groupes de conditions. Vous pouvez également ajouter des conditions imbriquées et des groupes de conditions à un groupe de conditions. Vous pouvez utiliser les opérateurs suivants :

    - **ET** signifie que le filtre sélectionne les événements qui remplissent toutes les conditions spécifiées.
    - **OU** signifie que le filtre sélectionne les événements qui remplissent une des conditions spécifiées.
    - **NON** (pour utiliser cet opérateur, il faut sélectionner l'option **Ajouter NON devant**) signifie que le filtre sélectionne les événements qui ne remplissent aucune des conditions spécifiées.

    Les conditions et les groupes de conditions de premier niveau sont combinés avec l'opérateur **ET**.

13. Pour analyser la règle de filtrage que vous avez créée, cliquez sur le bouton **Vérifier la règle**.

    Dans la fenêtre qui s'ouvre, un tableau des événements filtrés en fonction de la règle créée s'affiche. Pour en savoir plus, veuillez consulter l'aide relative à EDR Expert (cloud).

14. Le cas échéant, sous **Tous les types d'événements**, ajoutez des exclusions de télémétrie par type d'événement.

    a. Cliquez sur le nom du type d'événement.

    b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Configurer manuellement**.

    c. Configurez, si nécessaire, la transmission télémétrique pour le type d'événement sélectionné à l'aide du commutateur **Envoyer l'événement**. Par défaut, la transmission télémétrique est activée pour tous les types d'événements.

    d. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'exclusion**.

    La fenêtre **Ajouter une règle d'exclusion** s'ouvre.

    e. Exécutez les actions décrites aux étapes 7 à 13 pour chaque règle ajoutée.

15. Pour certains types d'événements, vous pouvez également ajouter des règles d'inclusion pour étendre la télémétrie collectée :

    a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'inclusion**.

    La fenêtre **Ajouter des règles d'inclusion** s'ouvre.

    b. Saisissez un nom pour la règle.

    c. Sous **Condition**, saisissez les valeurs des champs affichés. Le type de champs disponibles dépend de l'événement sélectionné.

Les règles d'exclusion ont la priorité sur les règles d'inclusion.

16. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

Comment exporter ou importer les filtres d'événements EDR Expert (cloud)

Vous pouvez exporter la liste des exclusions dans un fichier JSON. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'identifiants d'événements. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder les filtres d'événements ou pour migrer la liste vers un autre serveur.

L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur de collecte de données télémétriques et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Pour exporter et importer les filtres d'événements dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.
6. Pour exporter les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Exporter**.

   b. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   c. Enregistrez le fichier.

   Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.
7. Pour importer les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

c. Sélectionnez la méthode d'importation des règles de filtrage des événements : en les ajoutant aux règles existantes ou en supprimant les règles existantes et en les remplaçant par de nouvelles.

d. Ouvrez le fichier.

8. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie EDR Expert (cloud)**.

6. Pour exporter les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Exporter**.

   b. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   c. Enregistrez le fichier.

      Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.

7. Pour importer les filtres d'événements, procédez comme suit :

   a. Cliquez sur **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

   c. Sélectionnez la méthode d'importation des règles de filtrage des événements : en les ajoutant aux règles existantes ou en supprimant les règles existantes et en les remplaçant par de nouvelles.

   d. Ouvrez le fichier.

8. Pour appliquer la stratégie aux ordinateurs, assurez-vous que les cadenas sont fermés (🔒) et enregistrez vos modifications.

Gestion de la quarantaine

La *Quarantaine* est un stockage local spécial sur l'ordinateur. L'utilisateur peut mettre en quarantaine les fichiers qu'il considère comme dangereux pour l'ordinateur. Les fichiers mis en quarantaine sont stockés dans un état chiffré et ne menacent pas la sécurité de l'appareil. Kaspersky Endpoint Security utilise la Quarantaine uniquement lorsqu'elle est intégrée aux solutions de détection et de réponse de Kaspersky. Dans d'autres cas, Kaspersky Endpoint Security place le fichier correspondant dans la Sauvegarde. Pour en savoir plus sur la gestion de la Quarantaine dans le cadre des solutions, veuillez consulter l'aide de Kaspersky Sandbox, l'aide de Kaspersky Endpoint Detection and Response Optimum, l'aide de Kaspersky Endpoint Detection and Response Expert, l'aide de Kaspersky Anti Targeted Attack Platform et l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security utilise le compte système (SYSTEM) pour mettre les fichiers en quarantaine.

Vous ne pouvez configurer les paramètres de quarantaine que dans Kaspersky Security Center Console. Vous pouvez également utiliser Kaspersky Security Center Console pour gérer les objets mis en quarantaine (restauration, suppression, ajout, etc.). Localement, sur l'ordinateur, vous ne pouvez restaurer l'objet qu'en utilisant la ligne de commande.

Configuration de la taille maximale de la quarantaine

Par défaut, la taille de la quarantaine est limitée à 1024 Mo. Lorsque la quarantaine atteint la taille maximale, Kaspersky Endpoint Security arrête l'envoi des fichiers et génère l'événement *Espace insuffisant dans le Stockage en ligne*. Pour éviter que la quarantaine ne manque d'espace sur le disque, vous pouvez définir un seuil à partir duquel Kaspersky Endpoint Security génère un événement *L'espace de la Quarantaine est presque insuffisant*. Vous ne pouvez pas configurer de période de conservation pour les fichiers mis en quarantaine de manière à ce qu'ils soient automatiquement supprimés.

Si la solution Kaspersky Anti Targeted Attack Platform (EDR) est déployée dans votre organisation, nous vous recommandons d'augmenter la taille de la Quarantaine. Lors d'une analyse YARA, l'application peut rencontrer un vidage mémoire important. Si la taille du vidage mémoire dépasse la taille de la Quarantaine, l'analyse YARA se termine par une erreur et le vidage mémoire n'est pas mis en quarantaine. Nous vous recommandons de définir une taille de la Quarantaine égale à la taille totale de la mémoire vive de l'ordinateur (par exemple, 8 Go) ou de désactiver la limite de taille de la Quarantaine.

Configuration de la taille maximale de la quarantaine dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.

4. Dans le groupe **Quarantaine**, configurez la taille de la quarantaine :

   - **Limiter la taille de la Quarantaine à X Mo**. Si la case est cochée, la taille maximale de la Quarantaine est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 1 024 Mo. Lorsque la Quarantaine atteint sa taille maximale, Kaspersky Endpoint Security envoie l'événement *Espace insuffisant dans le Stockage en ligne* à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application arrête de mettre en quarantaine les nouveaux objets. Vous devez vider la Quarantaine manuellement.

     Si la case est décochée, la taille de la Quarantaine est limitée par l'espace libre du disque.

   - **Avertir lorsque le stockage de la Quarantaine atteint X pour cent**. Valeur seuil de la Quarantaine. Par exemple, vous pouvez fixer le seuil de la Quarantaine à 50 %. Lorsque la Quarantaine atteint le seuil, Kaspersky Endpoint Security envoie l'événement correspondant à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application continue de mettre en quarantaine les nouveaux objets.

     Si cette case est décochée, l'application ne génère pas d'événements lorsque le seuil de quarantaine est atteint.

5. Enregistrez vos modifications.

Configuration de la taille maximale de la Quarantaine dans Web Console et Cloud Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Rapports et stockage**.

5. Dans le groupe **Quarantaine**, configurez la taille de la quarantaine :

   - **Limiter la taille de la Quarantaine**. Si la case est cochée, la taille de la Quarantaine est limitée par la valeur définie. Si la case est décochée, la taille de la Quarantaine est limitée par l'espace libre du disque. Cette option peut être nécessaire pour l'analyse YARA, car l'application peut enregistrer un fichier de vidage mémoire volumineux.

   - **Taille maximale de la Quarantaine (Mo)**. Si la case est cochée, la taille maximale de la Quarantaine est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 1 024 Mo. Lorsque la Quarantaine atteint sa taille maximale, Kaspersky Endpoint Security envoie l'événement *Espace insuffisant dans le Stockage en ligne* à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application arrête de mettre en quarantaine les nouveaux objets. Vous devez vider la Quarantaine manuellement.

     Si la case est décochée, la taille de la Quarantaine est limitée par l'espace libre du disque.

   - **Avertir lorsque le stockage de la Quarantaine atteint (%)**. Valeur seuil de la Quarantaine. Par exemple, vous pouvez fixer le seuil de la Quarantaine à 50 %. Lorsque la Quarantaine atteint le seuil, Kaspersky Endpoint Security envoie l'événement correspondant à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application continue de mettre en quarantaine les nouveaux objets.

6. Enregistrez vos modifications.

Envoi de données concernant les fichiers en quarantaine à Kaspersky Security Center

Pour effectuer des actions avec des objets en quarantaine dans Web Console, vous devez activer l'envoi des données des fichiers en quarantaine au Serveur d'administration. Par exemple, vous pouvez télécharger un fichier de la quarantaine pour l'analyser dans Web Console. L'envoi des données des fichiers en quarantaine doit être activé pour que toutes les fonctionnalités de Kaspersky Sandbox et de Kaspersky Endpoint Detection and Response fonctionnent.

Activation du transfert des données des fichiers en quarantaine dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Rapports et stockage**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Transfert des données au Serveur d'administration**.
5. Dans la fenêtre qui s'ouvre, cochez la case **Fichiers de quarantaine**.
6. Enregistrez vos modifications.

Activation du transfert des données des fichiers en quarantaine dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Intégration KSC**.
5. Dans le groupe **Transfert des données au Serveur d'administration**, cochez la case **À propos des fichiers de la Quarantaine**.
6. Enregistrez vos modifications.

Par conséquent, vous pouvez afficher une liste des fichiers mis en quarantaine sur votre ordinateur dans Kaspersky Security Center Console. Vous pouvez utiliser Kaspersky Security Center Console pour administrer les objets mis en quarantaine (restauration, suppression, ajout, etc.). Pour plus de détails sur l'utilisation de la quarantaine, consultez l'aide de Kaspersky Security Center.

Restauration des fichiers depuis la quarantaine

Par défaut, Kaspersky Endpoint Security restaure les fichiers dans leur dossier d'origine. Si le dossier de destination a été supprimé ou si l'utilisateur ne dispose pas de droits d'accès à ce dossier, l'application place le fichier dans le dossier `%DataRoot%\QB\Restored`. Ensuite, vous devez déplacer manuellement le fichier vers le dossier cible.

Pour restaurer les fichiers de la quarantaine :

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages** → **Quarantaine**.

2. La liste des fichiers présents dans la Quarantaine s'ouvre ; dans cette liste, sélectionnez les fichiers que vous voulez restaurer et cliquez sur **Restaurer**.

   Kaspersky Endpoint Security restaure le fichier. Si le dossier de destination contient déjà un fichier portant le même nom, l'application annule la restauration du fichier. L'application enregistre une copie du fichier en quarantaine après sa restauration. Pour supprimer le fichier, vous devez vider manuellement la quarantaine.

Surveillance des actions EDR

Kaspersky Endpoint Security for Windows 12.9 introduit le centre de surveillance des actions EDR. Le *centre de surveillance des actions EDR* est une console où vous pouvez consulter l'historique des réponses aux menaces pour toutes les solutions Kaspersky Detection and Response. Si plusieurs systèmes Detection and Response sont déployés dans votre organisation (par exemple, EDR Optimum et MDR), Kaspersky Endpoint Security affiche l'historique de réponse aux menaces pour toutes les solutions. Cette information vous permet d'analyser les performances des solutions Detection and Response sur un ordinateur distinct et d'optimiser les paramètres de ces solutions.

Le centre de surveillance fournit les informations suivantes :

- Informations sur les tâches de réponse aux menaces (par exemple, la tâche *Fin du processus*)

- Modifications des règles d'isolement du réseau et de prévention de l'exécution

Si la réponse aux menaces rencontre une erreur liée à l'accès à un partage réseau, cette erreur est omise de l'historique de réponse aux menaces affiché.

Pour accéder au centre de surveillance des actions EDR :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.

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. Sélectionnez l'onglet **Applications**.

4. Cliquez sur **Kaspersky Endpoint Security for Windows 14.2**.

   La fenêtre des paramètres locaux de l'application s'ouvre.

5. Sélectionnez l'onglet **Paramètres de l'application**.

6. Passez à la section **Detection and Response** → **Historique des réponses**.

   Cette action ouvre la console du centre de surveillance des actions EDR. Vous pouvez utiliser la console pour afficher les états des tâches de réponse aux menaces, la durée de la tâche, les modifications des règles et les détails sur l'initiateur.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Kaspersky Endpoint Security for Windows prend en charge la solution Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* est une solution de gestion de la sécurité des informations et des événements (SIEM) pour l'infrastructure informatique des organisations. KUMA permet de détecter, d'analyser et d'atténuer les menaces à la sécurité avant qu'elles ne causent des dommages.

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les informations relatives aux événements survenus sur l'ordinateur (télémétrie) sont envoyées au serveur Kaspersky Unified Monitoring and Analysis Platform (KUMA). Dans sa console, KUMA affiche les événements sous la forme d'une liste sans annotation, semblable au journal des événements Windows.

Kaspersky Endpoint Security ne fournit pas toutes les fonctionnalités d'un agent pour KUMA. L'application envoie les événements sans annotations à KUMA uniquement. Pour accéder à toutes les fonctionnalités de KUMA, vous devez acheter une licence et déployer la solution conformément aux Manuel de l'administrateur KUMA.

Intégration de Kaspersky Endpoint Security à KUMA

La configuration de l'intégration de KES à KUMA comprend les étapes suivantes :

1. Dans la console KUMA, ajoutez un collecteur.
2. Dans la console KUMA, configurez un connecteur pour que le collecteur reçoive les événements de KES.
3. Dans la console KUMA, activez l'authentification bidirectionnelle (facultatif).
4. Dans la stratégie de Kaspersky Endpoint Security for Windows, configurez les paramètres de connexion de KES à KUMA.
5. Dans la console KUMA, assurez-vous que les événements de KES parviennent au locataire approprié et sont traités par les règles de corrélation appropriées.

Préparation de l'intégration de KES à KUMA

Pour utiliser KUMA, les conditions suivantes doivent être remplies :

- Kaspersky Security Center version 14.2 ou toute version ultérieure. Dans les versions antérieures de Kaspersky Security Center, il est impossible d'activer la fonction d'intégration KUMA.
- L'application est activée, et la fonctionnalité est couverte par la licence.
- Le module d'intégration KUMA est activé.

La préparation de l'intégration de KES à KUMA comprend les étapes suivantes :

1. **Installation du module d'intégration KUMA**

   Vous pouvez sélectionner le module d'intégration KUMA lors de l'installation ou de la mise à jour de l'application ainsi qu'à l'aide de la tâche *Modification de la sélection des modules de l'application*.

   Vous devez redémarrer votre ordinateur pour terminer la mise à jour de l'application avec le nouveau module.

2. **Activation KUMA**

   En plus de la licence d'application de Kaspersky Endpoint Security (par exemple, Kaspersky Endpoint Security for Business Standard), vous avez besoin d'une licence distincte pour l'intégration de Kaspersky Endpoint Security avec KUMA (module complémentaire d'intégration KUMA pour Kaspersky Endpoint Security for Windows).

   Si vous installez l'application en mode EDR Agent, vous avez besoin d'une licence pour l'intégration de Kaspersky Endpoint Security avec KUMA et d'une licence Kaspersky Anti Targeted Attack Platform (KATA) ou d'une licence Kaspersky Managed Detection and Response (MDR). Vous ne pouvez pas déployer EDR Agent pour KUMA uniquement.

   Cette fonctionnalité n'est disponible qu'après l'ajout de la clé KUMA séparée. Une autre clé active sera donc présente sur l'ordinateur pour assurer l'intégration de Kaspersky Endpoint Security avec KUMA.

   La licence de la fonctionnalité autonome KUMA est la même que celle de Kaspersky Endpoint Security.

   Assurez-vous que la fonctionnalité KUMA est incluse dans la licence et qu'elle fonctionne dans l'interface locale de l'application.

Connexion de KES à KUMA

Pour connecter l'ordinateur doté de l'application Kaspersky Endpoint Security à la solution KUMA, procédez comme suit :

1. Dans la console KUMA, ajoutez un collecteur avec des connecteurs de type **tcp**, **udp** ou **http**, puis définissez les paramètres réseau de base de la connexion. Pour en savoir plus sur la gestion des connecteurs, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

2. Dans la stratégie de Kaspersky Endpoint Security, ajoutez les adresses des collecteurs KUMA et définissez les paramètres réseau de la connexion.

Comment connecter un ordinateur Kaspersky Endpoint Security au module KUMA à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Intégration KUMA**.

5. Cochez la case **Intégration KUMA**.

6. Dans le groupe **Paramètres d'intégration**, cochez la case **Activer la transmission des événements Windows vers un serveur KUMA**.

7. Ajoutez des serveurs KUMA :

   a. Cliquez sur **Ajouter**.

   Cette action ouvre le formulaire dans lequel vous pouvez ajouter des serveurs KUMA.

   b. Sélectionnez le protocole de connexion au serveur KUMA : **HTTP/HTTPS**, **TCP** ou **UDP**.

   Le protocole de connexion au collecteur dans Kaspersky Endpoint Security doit correspondre au type de connecteur dans KUMA : **http**, **tcp** ou **udp**.

   > Lors de l'utilisation du protocole UDP, des données peuvent être perdues en raison de la perte de trafic inhérente à ce protocole.

   c. Indiquez l'adresse du serveur (IPv4, IPv6, FQDN) et le port de connexion au serveur (le port 443 est indiqué par défaut).

   Lorsque vous saisissez l'adresse du serveur, tenez compte des points suivants :

   - **TCP** :
     - **Sans TLS**. Vous pouvez indiquer l'adresse IP ou le FQDN du serveur.
     - **Avec TLS**. Vous devez indiquer uniquement le FQDN du serveur.
   - **HTTP/HTTPS** :
     - **Sans TLS**. Vous devez indiquer explicitement le protocole HTTP dans l'adresse du serveur (par exemple, `http://server.com` ou `http://10.10.10.100`).
     - **Avec TLS**. Vous n'avez pas besoin d'indiquer le protocole (par exemple, `https://server.com` ou `server.com`).
   - **UDP**. Le protocole UDP ne prend pas en charge le chiffrement TLS. Vous pouvez indiquer l'adresse IP ou le FQDN du serveur.

   Vous pouvez consulter l'adresse du serveur dans les propriétés du connecteur dans la console KUMA. Pour en savoir plus sur les connecteurs KUMA, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

   d. Cliquez sur **OK**.

   Kaspersky Endpoint Security se connecte au premier serveur KUMA de la liste. En cas d'échec de la connexion, Kaspersky Endpoint Security se connecte au deuxième serveur KUMA de la liste et ainsi de suite.

8. Si nécessaire, configurez le paramètre **Délai maximal de transmission des événements (s.)** dans le groupe **Paramètres de transmission des données**. Lorsque le délai spécifié est écoulé, Kaspersky Endpoint Security tente de se connecter au même collecteur ou se connecte au collecteur suivant dans la liste s'il y a plusieurs collecteurs. Le paramètre par défaut est de 30 secondes.

9. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment connecter un ordinateur Kaspersky Endpoint Security au module KUMA à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Configuration des agents intégrés** → **Intégration KUMA**.
5. Activez le commutateur **Intégration KUMA ACTIVÉE**.
6. Ajoutez des serveurs KUMA :

   a. Cliquez sur **Ajouter**.

   Cette action ouvre le formulaire dans lequel vous pouvez ajouter des serveurs KUMA.

   b. Sélectionnez le protocole de connexion au serveur KUMA : **HTTP/HTTPS**, **TCP** ou **UDP**.

   Le protocole de connexion au collecteur dans Kaspersky Endpoint Security doit correspondre au type de connecteur dans KUMA : **http**, **tcp** ou **udp**.

   > Lors de l'utilisation du protocole UDP, des données peuvent être perdues en raison de la perte de trafic inhérente à ce protocole.

   c. Indiquez l'adresse du serveur (IPv4, IPv6, FQDN) et le port de connexion au serveur (le port 443 est indiqué par défaut).

   Lorsque vous saisissez l'adresse du serveur, tenez compte des points suivants :

   - **TCP** :
     - **Sans TLS**. Vous pouvez indiquer l'adresse IP ou le FQDN du serveur.
     - **Avec TLS**. Vous devez indiquer uniquement le FQDN du serveur.
   - **HTTP/HTTPS** :
     - **Sans TLS**. Vous devez indiquer explicitement le protocole HTTP dans l'adresse du serveur (par exemple, `http://server.com` ou `http://10.10.10.100`).
     - **Avec TLS**. Vous n'avez pas besoin d'indiquer le protocole (par exemple, `https://server.com` ou `server.com`).
   - **UDP**. Le protocole UDP ne prend pas en charge le chiffrement TLS. Vous pouvez indiquer l'adresse IP ou le FQDN du serveur.

   Vous pouvez consulter l'adresse du serveur dans les propriétés du connecteur dans la console KUMA. Pour en savoir plus sur les connecteurs KUMA, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

   d. Cliquez sur **OK**.

Kaspersky Endpoint Security se connecte au premier serveur KUMA de la liste. En cas d'échec de la connexion, Kaspersky Endpoint Security se connecte au deuxième serveur KUMA de la liste et ainsi de suite.

7. Si nécessaire, configurez le paramètre **Durée d'attente maximale pour l'envoi des événements (sec)** dans le groupe **Paramètres de connexion au serveur**. Lorsque le délai spécifié est écoulé, Kaspersky Endpoint Security tente de se connecter au même collecteur ou se connecte au collecteur suivant dans la liste s'il y a plusieurs collecteurs. Le paramètre par défaut est de 30 secondes.

8. Enregistrez vos modifications.

Vous pouvez vérifier que l'intégration KUMA est correctement configurée dans la console KUMA (pour en savoir plus, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform). Vérifiez l'état de fonctionnement du module en consultant le *Rapport sur l'état des modules de l'application* dans la console Kaspersky Security Center. Vous pouvez également consulter l'état de fonctionnement d'un module dans les rapports de l'interface locale de Kaspersky Endpoint Security. Le module **Intégration KUMA** sera ajouté à la liste des modules de Kaspersky Endpoint Security.

Établissement d'une connexion de confiance entre KES et KUMA

Vous pouvez établir une connexion de confiance entre Kaspersky Endpoint Security et un collecteur KUMA doté d'un connecteur de type tcp ou http. Il est impossible d'établir une connexion de confiance avec un connecteur de type udp.

Pour établir une connexion de confiance, vous devez configurer un mode TLS dans les paramètres du connecteur. Les modes TLS suivants sont disponibles :

- **Disabled** : n'utilise pas le chiffrement TLS. Cette option est sélectionnée par défaut.
- **Enabled** : utilise le chiffrement TLS, mais sans vérification du certificat.
- **Custom PFX with client authentication** : utilise le chiffrement TLS avec un secret PFX. Dans ce mode, le client est authentifié à l'aide d'un certificat.

Kaspersky Endpoint Security ne prend pas en charge le mode TLS **Custom PFX**. Lors de l'intégration de KES à KUMA à l'aide d'un fichier PFX, l'authentification de l'utilisateur par mot de passe est requise.

Pour configurer une connexion de confiance, vous avez besoin d'un certificat TLS, à savoir le *certificat de l'autorité de certification du microservice*. Vous pouvez obtenir un certificat TLS dans la console KUMA. Pour en savoir plus sur le téléchargement des certificats TLS, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform. Ensuite, vous devez ajouter le certificat TLS à Kaspersky Endpoint Security (voir les instructions ci-dessous).

Pour rendre la connexion plus sécurisée, vous pouvez également activer l'authentification de l'ordinateur dans KUMA (authentification bidirectionnelle). Pour activer cette authentification, vous devez créer un conteneur crypto auprès d'une autorité de certification externe. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée au format PKCS#12. Vous devez ensuite activer l'authentification bidirectionnelle dans les paramètres de KUMA (mode TLS **Custom PFX with client authentication**), activer l'authentification bidirectionnelle dans Kaspersky Endpoint Security et ajouter une archive PFX dans la console KUMA et dans Kaspersky Endpoint Security.

Configuration d'une connexion de confiance entre KES et KUMA dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Stratégies**.
3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
4. Dans la fenêtre de la stratégie, sélectionnez **Intégration KUMA**.
5. Cochez la case **Intégration KUMA**.
6. Dans le groupe **Paramètres de connexion aux serveurs KUMA**, cochez la case **Utiliser le chiffrement TLS**.
7. Configurez la connexion de confiance :
   a. Cliquez sur **Paramètres de connexion aux serveurs KUMA**.
   b. Configurez la connexion au serveur :
      - **Délai d'attente (s.)**. Délai maximal d'attente d'une réponse du serveur KUMA (la valeur par défaut est de 5 secondes). À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur KUMA.
      - **Certificat TLS du serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur KUMA. Vous pouvez obtenir un certificat TLS dans la console de Kaspersky Unified Monitoring and Analysis Platform (consultez les instructions dans l'aide de Kaspersky Unified Monitoring and Analysis Platform).

        Pour établir une connexion de confiance, vous devez sélectionner le mode TLS **Enabled** dans la console KUMA.
      - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre KES et KUMA. Pour utiliser l'authentification bidirectionnelle, vous devez sélectionner le mode TLS **Custom PFX with client authentication** dans les paramètres du connecteur de la console KUMA (consultez les paramètres du connecteur dans l'aide de Kaspersky Unified Monitoring and Analysis Platform). Ensuite, vous devez télécharger un certificat de serveur et définir un mot de passe pour protéger le conteneur crypto.

        > Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   c. Cliquez sur **OK**.
8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Configuration d'une connexion de confiance entre KES et KUMA dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Configuration des agents intégrés** → **Intégration KUMA**.

5. Activez le commutateur **Intégration KUMA ACTIVÉE**.

6. Sous **Paramètres de connexion au serveur**, désactivez le commutateur **Utiliser le chiffrement TLS**.

7. Configurez la connexion de confiance :

   a. Cliquez sur **Paramètres de connexion**.

   b. Configurez la connexion au serveur :

   - **Délai d'attente (s.)**. Délai maximal d'attente d'une réponse du serveur KUMA (la valeur par défaut est de 5 secondes). À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur KUMA.

   - **Certificat TLS du serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur KUMA. Vous pouvez obtenir un certificat TLS dans la console de Kaspersky Unified Monitoring and Analysis Platform (consultez les instructions dans l'aide de Kaspersky Unified Monitoring and Analysis Platform).

     Pour établir une connexion de confiance, vous devez sélectionner le mode TLS **Enabled** dans la console KUMA.

   - **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre KES et KUMA. Pour utiliser l'authentification bidirectionnelle, vous devez sélectionner le mode TLS **Custom PFX with client authentication** dans les paramètres du connecteur de la console KUMA (consultez les paramètres du connecteur dans l'aide de Kaspersky Unified Monitoring and Analysis Platform). Ensuite, vous devez télécharger un certificat de serveur et définir un mot de passe pour protéger le conteneur crypto.

     > Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

   c. Cliquez sur **OK**.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Activation de l'envoi des données télémétriques au serveur KUMA

Par défaut, l'envoi d'événements au serveur KUMA est désactivé. Pour garantir le bon fonctionnement de KUMA, vous devez activer l'envoi de données télémétriques. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*.

Comment activer l'envoi de données télémétriques à KUMA dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la télémétrie** → **Télémétrie KUMA**.

6. Sélectionnez les journaux des événements que vous souhaitez utiliser comme sources des événements : *Application*, *Security* ou *System*.

   En plus des journaux standard, vous pouvez spécifier un journal d'une application tierce.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer l'envoi de données télémétriques à KUMA dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie KUMA**.

6. Sélectionnez les journaux des événements que vous souhaitez utiliser comme sources des événements : *Application*, *Security* ou *System*.

   En plus des journaux standard, vous pouvez spécifier un journal d'une application tierce.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Filtrage des événements à envoyer à KUMA

Par défaut, l'envoi d'événements au serveur KUMA est désactivé. Pour garantir le bon fonctionnement de KUMA, vous devez activer l'envoi de données télémétriques. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Pour améliorer les performances et optimiser la transmission des données vers le serveur KUMA, vous pouvez ajouter ou exclure manuellement des événements individuels de la télémétrie. Par exemple, vous pouvez exclure les événements Sysmon.

Comment créer une liste d'événements à envoyer à KUMA dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la télémétrie** → **Télémétrie KUMA**.

6. Dans la fenêtre qui s'affiche, configurez les filtres d'événements à envoyer à KUMA.

Vous pouvez configurer le filtrage des événements pour les journaux standard *Application*, *Security*, *System* ou ajouter manuellement un autre journal :

a. Ouvrez les propriétés du journal ou cliquez sur le bouton **Ajouter** et saisissez le nom du journal.

b. Sélectionnez un mode d'envoi d'événement :

- **Envoyer tous les événements**. Dans ce mode, l'application envoie tous les événements du journal Windows à l'exception des événements ajoutés aux règles d'exclusion.
- **Envoyer uniquement les événements sélectionnés**. Dans ce mode, l'application envoie uniquement les événements ajoutés dans les règles d'inclusion.

c. Créer des listes de règles d'exclusion ou d'inclusion pour le mode d'envoi d'événements concerné.

Pour ajouter des règles, vous devez indiquer l'identifiant de l'événement dans le journal des événements Windows. Vous pouvez inclure plusieurs identifiants d'événement dans une règle. Pour indiquer plusieurs identifiants d'événement, utilisez la virgule (`,`).

d. Le cas échéant, activez la journalisation des événements à l'aide de la case à côté du nom du journal.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment créer une liste d'événements à envoyer à KUMA dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.
5. Sélectionnez l'onglet **Télémétrie KUMA**.
6. Dans la fenêtre qui s'affiche, configurez les filtres d'événements à envoyer à KUMA.

Vous pouvez configurer le filtrage des événements pour les journaux standard *Application*, *Security*, *System* ou ajouter manuellement un autre journal :

a. Ouvrez les propriétés du journal ou cliquez sur le bouton **Ajouter** et saisissez le nom du journal.

b. Sélectionnez un mode d'envoi d'événement :

- **Envoyer tous les événements**. Dans ce mode, l'application envoie tous les événements du journal Windows à l'exception des événements ajoutés aux règles d'exclusion.
- **Envoyer uniquement les événements sélectionnés**. Dans ce mode, l'application envoie uniquement les événements ajoutés dans les règles d'inclusion.

c. Créer des listes de règles d'exclusion ou d'inclusion pour le mode d'envoi d'événements concerné.

Pour ajouter des règles, vous devez indiquer l'identifiant de l'événement dans le journal des événements Windows. Vous pouvez inclure plusieurs identifiants d'événement dans une règle. Pour indiquer plusieurs identifiants d'événement, utilisez la virgule (**,**).

d. Si nécessaire, activez la journalisation des événements à l'aide du commutateur à côté du nom du journal.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Exportation et importation de filtres d'événements KUMA

Vous pouvez exporter la liste des exclusions dans un fichier JSON. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'identifiants d'événements. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder les filtres d'événements ou pour migrer la liste vers un autre serveur.

L'utilisation d'un trop grand nombre de règles peut augmenter la charge sur le serveur KUMA et réduire les performances de l'ordinateur. Nous recommandons d'ajouter uniquement les règles indispensables.

Comment exporter et importer des filtres d'événements dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Exclusions et types d'objets**.

5. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de la télémétrie** → **Télémétrie KUMA**.

6. Pour exporter les filtres d'événements, procédez comme suit :

   a. Sélectionnez les journaux d'événements avec filtres que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   d. Enregistrez le fichier.

   Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.

7. Pour importer les filtres d'événements, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

c. Ouvrez le fichier.

Si des règles de filtrage des événements existent déjà sur l'ordinateur, Kaspersky Endpoint Security les remplace lors de l'importation.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment exporter et importer des filtres d'événements dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → onglet **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Paramètres généraux** → **Paramètres de la télémétrie**.

5. Sélectionnez l'onglet **Télémétrie KUMA**.

6. Pour exporter les filtres d'événements, procédez comme suit :

   a. Sélectionnez les journaux d'événements avec filtres que vous souhaitez exporter.

   b. Appuyez sur le bouton → **Exporter**.

   c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format JSON dans lequel vous voulez exporter les filtres d'événements et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

   d. Enregistrez le fichier.

   Kaspersky Endpoint Security exporte les filtres d'événements dans un fichier JSON.

7. Pour importer les filtres d'événements, procédez comme suit :

   a. Appuyez sur le bouton → **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier JSON à partir duquel vous souhaitez importer les filtres d'événements.

   c. Ouvrez le fichier.

   Si des règles de filtrage des événements existent déjà sur l'ordinateur, Kaspersky Endpoint Security les remplace lors de l'importation.

8. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Vous pouvez également exporter ou importer des filtres d'événements à partir de la ligne de commande.

Guide de migration de KSWS vers KES

À partir de la version 11.8.0, Kaspersky Endpoint Security for Windows prend en charge les fonctionnalités de base de la solution Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* protège les serveurs tournant sous le système d'exploitation Microsoft Windows et les systèmes de stockage en réseau contre les virus et d'autres menaces de sécurité informatique auxquels les serveurs et les systèmes de stockage en réseau sont exposés lors de l'échange de fichiers. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Security for Windows Server. À partir de Kaspersky Endpoint Security 11.8.0, vous pouvez migrer de Kaspersky Security for Windows Server vers Kaspersky Endpoint Security for Windows et utiliser la même solution pour protéger les postes de travail et les serveurs.

Configuration logicielle

Avant de commencer la migration de KSWS vers KES, assurez-vous que votre serveur répond à la configuration matérielle et logicielle requise par Kaspersky Endpoint Security for Windows. Les listes des versions du système d'exploitation prises en charge sont différentes pour KES et KSWS. Par exemple, KES ne prend pas en charge les serveurs fonctionnant sous Windows Server 2003.

Configuration logicielle minimale pour procéder à la migration de KSWS vers KES :

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Si vous avez installé une version antérieure de Kaspersky Security for Windows Server, nous vous recommandons de mettre à jour l'application vers la dernière version. L'Assistant de conversion des stratégies et des tâches ne prend pas en charge les versions antérieures de Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Si une version antérieure de Kaspersky Security Center est installée, mettez-la à jour vers la version 14.2 ou une version ultérieure. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet de migrer les stratégies vers un profil plutôt que vers une stratégie. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet également de migrer un plus large éventail de paramètres de stratégie.
- Kaspersky Endpoint Agent 3.10.

  Si une version antérieure de Kaspersky Endpoint Agent est installée, nous vous recommandons de mettre à jour l'application vers la dernière version. Kaspersky Endpoint Security prend en charge la migration d'une configuration [KSWS+KEA] vers [KES+agent intégré] à partir de Kaspersky Endpoint Agent 3.10.

Recommandations de migration

Lors de la migration de KSWS vers KES, respectez les recommandations suivantes :

- Planifiez le temps de migration de KSWS vers KES. Choisissez un moment où les serveurs fonctionnent avec la charge la plus faible, par exemple pendant le week-end.
- Après la migration, activez progressivement les modules de l'application. C'est-à-dire, par exemple, commencez par activer le module Protection contre les fichiers malicieux seul, puis activez d'autres modules de protection, puis activez les modules de surveillance, etc. À chaque étape, vous devez vous assurer que l'application fonctionne correctement et surveiller les performances du serveur. L'architecture de KES diffère de KSWS, par conséquent, le système d'exploitation peut également se comporter différemment.
- Effectuez la migration progressivement. Migrez d'abord un seul serveur, puis plusieurs serveurs, puis effectuez la migration sur tous les serveurs de l'organisation.
- Migrez différents types de serveurs séparément. C'est-à-dire, par exemple, migrez d'abord les serveurs de base de données, puis les serveurs de messagerie, etc.
- La migration sur des serveurs à forte charge présente certaines particularités.

Étapes de migration

La migration de KSWS vers KES est effectuée de manière semi-automatique. Cette démarche est nécessaire en raison des architectures différentes des applications. Pour migrer les paramètres de stratégie, vous devez exécuter l'Assistant de conversion de masse des stratégies et des tâches (l'Assistant de migration). Après la migration des paramètres de stratégie, vous devez configurer manuellement les paramètres que l'Assistant de migration ne peut pas migrer automatiquement (par exemple, les paramètres de protection par mot de passe). Après la migration, il est également recommandé de vérifier si l'Assistant de migration a correctement migré tous les paramètres.

Procédez à la migration de KSWS vers KES dans l'ordre suivant :

1. **Migrer les tâches et les stratégies de KSWS**

   Après la migration des stratégies et des tâches, vous devez effectuer des étapes de configuration supplémentaires. Nous vous recommandons également de vous assurer que Kaspersky Endpoint Security fournit le niveau de sécurité nécessaire après la migration à partir de KSWS.

   > L'Assistant de conversion de masse des stratégies et des tâches pour Kaspersky Security for Windows Server est uniquement disponible dans la Console d'administration (MMC). Les paramètres de stratégie et de tâche ne peuvent pas être migrés dans Web Console et Kaspersky Security Center Cloud Console.

2. **Installer Kaspersky Endpoint Security**

Vous pouvez installer Kaspersky Endpoint Security des manières suivantes :

- Installation de KES après la suppression de KSWS (recommandé).

  L'utilitaire kavremover ne prend pas en charge la gestion de KSWS.

- Installation de KES par-dessus KSWS.

3. Activer KES avec une clé KSWS

4. **Confirmer que l'application fonctionne correctement après la migration**

   Une fois que vous avez procédé à la migration de KSWS vers KES, assurez-vous que l'application fonctionne correctement. Vérifiez l'état du serveur dans la console (l'état devrait être *OK*). Assurez-vous qu'aucune erreur n'est signalée pour l'application, vérifiez également l'heure de la dernière connexion au Serveur d'administration, l'heure de la dernière mise à jour de la base de données et l'état de la protection du serveur.

   Portez une attention particulière à la migration des listes d'exclusion, des applications de confiance, des adresses Web de confiance et des règles du Contrôle des applications.

Correspondance des modules de KSWS et de KES

Lors de la migration de KSWS vers KES, l'ensemble de modules est migré uniquement lorsque l'application est installée localement.

Correspondance des modules Kaspersky Security for Windows Server et Kaspersky Endpoint Security for Windows

Module Kaspersky Security for Windows Server	Module Kaspersky Endpoint Security for Windows
Fonctionnalité de base	Noyau de l'application
Inspection des journaux	Inspection des journaux
Contrôle des appareils	Contrôle des appareils
Gestion du pare-feu	*(non pris en charge)* Les fonctionnalités du Pare-feu de KSWS sont assurées par le Pare-feu au niveau du système. Dans KES, un module distinct est responsable de la fonctionnalité Pare-feu. Après la migration, vous pouvez configurer le Pare-feu de Kaspersky Endpoint Security.
Contrôle de l'intégrité des fichiers	Contrôle de l'intégrité du système
Protection contre les Exploits	Protection contre les Exploits
Icône de la barre d'état système	*(non pris en charge)* Vous pouvez configurer l'interaction avec l'utilisateur dans les paramètres de l'interface de l'application.
Intégration à Kaspersky Security Center	Connecteur de l'Agent d'administration
Endpoint Agent	*(non pris en charge)* Dans Kaspersky Endpoint Security 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution de Kaspersky Endpoint Security. Vous devez télécharger séparément le paquet de distribution de Kaspersky Endpoint Agent.
Protection contre les menaces réseau	Protection contre les menaces réseau
Protection contre le chiffrement	Détection comportementale

Module Kaspersky Security for Windows Server	Module Kaspersky Endpoint Security for Windows
Protection contre le chiffrement pour NetApp	*(non pris en charge)*
Protection du trafic	Protection contre les menaces Internet Protection contre les menaces par emails Contrôle Internet
Analyse à la demande	Noyau de l'application
Protection ICAP des stockages réseau connectés	*(non pris en charge)* Kaspersky Endpoint Security ne prend pas en charge les modules de Protection des stockages réseau. Si vous avez besoin de ces modules, vous pouvez continuer à utiliser Kaspersky Security for Windows Server.
Protection RPC des stockages réseau connectés	*(non pris en charge)* Kaspersky Endpoint Security ne prend pas en charge les modules de Protection des stockages réseau. Si vous avez besoin de ces modules, vous pouvez continuer à utiliser Kaspersky Security for Windows Server.
Protection des fichiers en temps réel	Protection contre les fichiers malicieux
Surveillance des scripts	*(non pris en charge)* La Surveillance des scripts est assurée par d'autres modules, par exemple, la Protection AMSI.
Utilisation du KSN	Kaspersky Security Network
Contrôle du lancement des applications	Contrôle des applications
Compteurs de performance	*(non pris en charge)*

Correspondance des paramètres de KSWS et de KES

Lors de la migration des stratégies et des tâches, KES est configuré conformément aux paramètres de KSWS. Les paramètres des modules d'application dont KSWS ne dispose pas sont définis par défaut.

Paramètres de l'application

Évolutivité, interface et paramètres d'analyse

Les paramètres de l'application ne sont pas pris en charge par Kaspersky Endpoint Security for Windows.

Paramètres de l'application

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Paramètres d'optimisation	*(ne migre pas)* Kaspersky Endpoint Security gère tous les processus de travail.
Afficher l'icône de la barre d'état système	*(ne migre pas)* La fenêtre principale de Kaspersky Endpoint Security et l'icône de la zone de notification Windows sont disponibles par défaut 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. Vous pouvez configurer l'interaction avec l'utilisateur dans les paramètres de l'interface de l'application.
Restaurer les attributs du fichier après l'analyse	*(ne migre pas)* Kaspersky Endpoint Security restaure automatiquement les attributs des fichiers après avoir analysé un fichier.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Limiter l'utilisation du processeur pour les threads d'analyse	*(ne migre pas)* Kaspersky Endpoint Security ne limite pas l'utilisation du processeur lors de l'analyse. Vous pouvez configurer la tâche de manière à ce qu'elle s'exécute lorsque l'ordinateur fonctionne sous une charge minimale.
Dossier pour les fichiers temporaires créés pendant l'analyse	*(ne migre pas)* Kaspersky Endpoint Security place les fichiers temporaires dans le dossier `C:\Windows\Temp`.
Paramètres du système HSM	*(ne migre pas)* Kaspersky Endpoint Security ne prend pas en charge les systèmes HSM.

Sécurité et fiabilité

Les paramètres de sécurité de KSWS sont migrés vers la section **Paramètres généraux**, dans les sous-sections **Paramètres de l'application** et **Interface**.

Paramètres de sécurité des applications

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Protection des processus de l'application contre les menaces externes	**Activer l'Autodéfense** (sous-section **Paramètres de l'application**)
Utiliser la protection par mot de passe	*(ne migre pas)* Kaspersky Endpoint Security dispose d'une fonctionnalité intégrée de protection par mot de passe (voir la sous-section **Interface**).
Réaliser la restauration des tâches	*(ne migre pas)* Kaspersky Endpoint Security ne restaure automatiquement que les tâches *Analyse des logiciels malveillants*. Kaspersky Endpoint Security exécute d'autres tâches selon une planification.
Ne pas lancer les tâches d'analyse programmée	**Reporter les tâches planifiées en cas d'alimentation par batterie** (sous-section **Paramètres de l'application**)
Arrêter les tâches d'analyse en cours	*(ne migre pas)* Lorsque l'ordinateur est alimenté par un onduleur, Kaspersky Endpoint Security n'arrête pas les tâches d'analyse en cours d'exécution.

Paramètres de connexion

Les paramètres d'interaction du Serveur d'administration sont migrés vers la section **Paramètres généraux**, dans les sous-sections **Paramètres du réseau** et **Paramètres de l'application**.

Paramètres d'interaction du Serveur d'administration

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Paramètres du serveur proxy	**Paramètres du serveur proxy** (sous-section **Paramètres du réseau**)
Ne pas utiliser le serveur proxy pour les adresses locales	**Ne pas utiliser de serveur proxy pour les adresses locales** (sous-section **Paramètres du réseau**)
Paramètres d'authentification du serveur proxy	**Utiliser l'authentification sur le serveur proxy** (sous-section **Paramètres du réseau**) Le mot de passe d'authentification sur le serveur proxy ne fait pas l'objet d'une migration. Une fois qu'une stratégie a été migrée, le mot de passe doit être saisi manuellement.
Utiliser Kaspersky Security Center comme serveur proxy pour l'activation de l'application	**Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation** (sous-section **Paramètres de l'application**)

Lancer les tâches locales du système

Kaspersky Endpoint Security ignore les paramètres d'exécution des tâches locales du système de Kaspersky Security for Windows Server. Vous pouvez configurer l'utilisation des tâches locales de KES sous **Tâches locales**, **Administration des tâches**. Vous pouvez également configurer une planification pour l'exécution des tâches *Analyse des logiciels malveillants* et *Mise à jour des bases et des modules d'application* dans les propriétés de ces tâches.

Complémentaire

Exclusions de l'analyse pour l'application

Les paramètres de la Zone de confiance de KSWS sont migrés vers la section **Paramètres généraux**, dans la sous-section **Exclusions**.

Paramètres des zones de confiance

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Objet à analyser (Exclusions)	**Exclusions de l'analyse** (Exclusions de l'analyse) Les méthodes utilisées par KSWS et KES pour sélectionner les objets diffèrent. Lors de la migration, KES prend en charge les exclusions définies comme des fichiers individuels ou des chemins d'accès au fichier / dossier. Si KSWS a des exclusions configurées comme une zone prédéfinie ou une URL de script, ces exclusions ne font pas l'objet d'une migration. Après la migration, vous devez ajouter ces exclusions manuellement. Les exclusions en tant que zones prédéfinies doivent être configurées dans les paramètres de la tâche *Analyse des logiciels malveillants*. Les exclusions en tant qu'adresses Internet de script doivent être ajoutées aux adresses Internet de confiance pour la Protection contre les menaces Internet.
Appliquer également aux sous-dossiers (Exclusions)	**Inclure les sous-dossiers** (Exclusions de l'analyse)
Objets à détecter (Exclusions)	**Type d'un objet détecté** (Exclusions de l'analyse)
Zone d'application des exclusions (Exclusions)	**Modules de la protection** (Exclusions de l'analyse) Si au moins un module est sélectionné dans KSWS, KES applique les exclusions à tous les modules de l'application.
Commentaires (Exclusions)	**Commentaires** (Exclusions de l'analyse)
Processus de confiance (Processus de confiance)	**Applications de confiance** Les méthodes de sélection des processus/applications de confiance diffèrent dans KSWS et KES. Lors de la migration, KES prend en charge les applications de confiance configurées comme un chemin d'accès au fichier exécutable ou au masque. Si KSWS a des processus de confiance configurés comme un fichier de hachage, ces processus de confiance ne font pas l'objet d'une migration. Après la migration, vous devez ajouter manuellement ces processus de confiance.
Ne pas vérifier les opérations de sauvegarde de fichiers (Processus de confiance)	**Ne pas surveiller l'activité de l'application** (Applications de confiance)

Analyse des disques amovibles

Les paramètres de l'Analyse des disques amovibles sont migrés vers la section **Tâches locales**, dans la sous-section **Analyse des disques amovibles**.

Paramètres d'analyse des disques amovibles

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Analyser les disques amovibles à la connexion via USB	**Action lorsqu'un disque amovible est connecté**
Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)	**Taille maximale du disque amovible**
Analyser avec le niveau de sécurité : • **Protection maximale** • **Recommandé** • **Performance maximale**	**Action lorsqu'un disque amovible est connecté** : • **Protection maximale**. • **Recommandé**. Les niveaux de sécurité KSWS correspondent aux modes d'analyse KES comme suit : • Protection maximale – Protection maximale • Recommandé – Recommandé • Performance maximale – Recommandé

Autorisations de l'utilisateur pour l'administration de l'application

Kaspersky Endpoint Security ne prend pas en charge l'attribution d'autorisations d'accès aux utilisateurs pour l'administration de l'application et des services de l'application. Vous pouvez configurer les paramètres d'accès des utilisateurs et des groupes d'utilisateurs pour l'administration de l'application dans Kaspersky Security Center.

Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security

Kaspersky Endpoint Security ne prend pas en charge l'attribution d'autorisations d'accès aux utilisateurs pour l'administration de l'application et des services de l'application. Vous pouvez configurer les paramètres d'accès des utilisateurs et des groupes d'utilisateurs pour l'administration de l'application dans Kaspersky Security Center.

Stockages

Les paramètres de stockage de KSWS sont migrés vers la section **Paramètres généraux**, dans la sous-section Rapports et stockage, et vers la section **Protection principale**, dans la sous-section Protection contre les menaces réseau.

Paramètres du stockage

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Dossier de sauvegarde	*(ne migre pas)* Kaspersky Endpoint Security enregistre des copies de sauvegarde des fichiers dans le dossier `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Taille maximale de sauvegarde (Mo)	**Limiter la taille de la sauvegarde à X Mo** (section **Paramètres généraux** → **Rapports et stockage**)
Seuil d'espace disponible (Mo)	*(ne migre pas)* Kaspersky Endpoint Security enregistre l'événement *L'espace de la Quarantaine est presque insuffisant* lorsque le seuil de 50 % est atteint.
Dossier cible pour la restauration des objets	*(ne migre pas)* Kaspersky Endpoint Security restaure les fichiers dans leur dossier d'origine.
Dossier de quarantaine	*(ne migre pas)* Kaspersky Endpoint Security enregistre des copies de sauvegarde des fichiers dans le dossier `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Taille maximale de la quarantaine (Mo)	*(ne migre pas)* Kaspersky Endpoint Security utilise la Sauvegarde pour stocker les objets probablement infectés. Lors de la migration, Kaspersky Endpoint Security ignore les paramètres de la Quarantaine.
Seuil d'espace disponible (Mo)	*(ne migre pas)* Kaspersky Endpoint Security utilise la Sauvegarde pour stocker les objets probablement infectés. Lors de la migration, Kaspersky Endpoint Security ignore les paramètres de la Quarantaine.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Dossier cible pour la restauration des objets	*(ne migre pas)* Kaspersky Endpoint Security restaure les fichiers dans leur dossier d'origine.
Débloquer automatiquement au bout de X	**Bloquer les appareils attaquants pendant X min** (section **Protection principale** → **Protection contre les menaces réseau**)

Protection en temps réel du serveur

Protection des fichiers en temps réel

Les paramètres de la Protection des fichiers en temps réel de KSWS sont migrés vers la section **Protection principale**, dans la sous-section **Protection contre les fichiers malicieux**.

Paramètres de la protection des fichiers en temps réel

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Mode de protection d'objets : • **Mode intelligent** • **À l'exécution** • **À l'accès** • **À l'accès et à la modification**	**Mode d'analyse** : • **Mode intelligent**. • **À l'exécution**. • **À l'accès**. • **À l'ouverture et en cas de modification**.
Analyse plus profonde du lancement de processus	*(ne migre pas)* Kaspersky Endpoint Security ne prend en charge qu'un seul mode d'analyse, le mode Optimal.
Analyse heuristique : • **Superficielle** • **Moyenne** • **Minutieuse**	**Analyse heuristique** : • **Superficielle**. • **Moyenne**. • **Minutieuse**.
Appliquer la zone de confiance	*(ne migre pas)* Kaspersky Endpoint Security applique la zone de confiance à tous les modules. Vous pouvez configurer les exclusions dans les paramètres de la zone de confiance.
Utiliser KSN pour la protection	*(ne migre pas)* Kaspersky Endpoint Security utilise KSN pour tous les modules d'application.
Bloquer l'accès aux ressources réseau partagées pour les hôtes qui affichent une activité malveillante	*(ne migre pas)* Par défaut, Kaspersky Endpoint Security interdit l'accès aux ressources partagées du réseau pour les hôtes qui présentent une activité malveillante.
Lancer une analyse rapide quand une infection active est détectée	*(ne migre pas)* Kaspersky Endpoint Security ne lance pas la tâche d'analyse des zones critiques lorsqu'une infection active est détectée.
Utiliser Kaspersky Sandbox pour la protection	*(ne migre pas)* Par défaut, Kaspersky Endpoint Security envoie les objets à analyser à Kaspersky Sandbox.
Zone de protection	**Zone de protection**
Paramètres de planification	*(ne migre pas)* Kaspersky Endpoint Security utilise sa propre planification pour suspendre la Protection contre les fichiers malicieux.

Utilisation du KSN

Les paramètres de KSWS pour Kaspersky Security Network sont migrés vers la section **Protection avancée**, dans la sous-section **Kaspersky Security Network**.

Paramètres de Kaspersky Security Network

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
J'accepte les conditions de participation à Kaspersky Security Network	**Déclaration de Kaspersky Security Network** Kaspersky Endpoint Security demande le consentement à la Déclaration de Kaspersky Security Network lorsque l'application est installée, qu'une nouvelle stratégie est créée ou que l'utilisation de Kaspersky Security Network est activée.
Envoyer des données sur les fichiers analysés	*(ne migre pas)* Kaspersky Endpoint Security envoie automatiquement des données sur les fichiers analysés si KSN est activé.
Envoyer des données relatives aux adresses Internet sollicitées	*(ne migre pas)* Kaspersky Endpoint Security envoie automatiquement des données sur les URL demandées si KSN est activé.
Envoyer les statistiques de Kaspersky Security Network	**Activer le mode étendu de KSN**
Accepter les conditions de la Déclaration de Kaspersky Managed Protection	*(ne migre pas)* Kaspersky Endpoint Security ne comprend pas le service KMP.
Actions à exécuter sur les objets douteux selon KSN	*(ne migre pas)* Vous pouvez configurer l'action en cas de détection d'une menace dans les paramètres des modules de protection et les paramètres des tâches d'analyse.
Ne pas calculer la somme de contrôle avant l'envoi à KSN si la taille du fichier dépasse X Mo	*(ne migre pas)* Vous pouvez configurer les restrictions d'analyse des fichiers volumineux dans les paramètres des modules de protection et les paramètres des tâches d'analyse.
Utiliser Kaspersky Security Center en tant que serveur proxy du KSN	**Utiliser le Serveur d'administration comme serveur proxy KSN**
Paramètres de planification	*(ne migre pas)* Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Protection du trafic

Les paramètres de protection du trafic KSWS sont migrés vers la section **Protection principale**, dans les sous-sections **Protection contre les menaces Internet** et **Protection contre les menaces par emails**, vers la section **Contrôles de sécurité**, dans la sous-section **Contrôle Internet**, et vers la section **Paramètres généraux**, dans la sous-section **Paramètres du réseau**.

Paramètres de protection du trafic

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Appliquer les règles basées sur l'URL	**Contrôle Internet** (sous-section **Contrôle Internet**) Les règles selon l'URL sont migrées vers des règles séparées dans Kaspersky Endpoint Security.
Appliquer les règles selon le certificat	*(ne migre pas)* Kaspersky Endpoint Security n'est pas compatible avec les règles selon le certificat.
Appliquer les règles pour le contrôle des catégories de trafic Internet	**Contrôle Internet** (sous-section **Contrôle Internet**) Les règles de blocage pour le contrôle des catégories de trafic Internet sont migrées vers une règle de blocage unique dans Kaspersky Endpoint Security. Kaspersky Endpoint Security ignore les règles d'autorisation pour le contrôle des catégories. La correspondance des catégories KSWS et KES est indiquée ci-dessous.
Autoriser l'accès si la page Internet ne peut pas être classée dans une catégorie	*(ne migre pas)* Kaspersky Endpoint Security autorise l'accès si la page Internet ne peut pas être catégorisée.
Autoriser l'accès aux ressources Internet légitimes qui peuvent servir à endommager votre appareil	*(ne migre pas)* Kaspersky Endpoint Security autorise l'accès à des ressources Internet légitimes qui peuvent être utilisées pour endommager l'appareil protégé.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Autoriser l'accès aux publicités légitimes	*(ne migre pas)* Vous pouvez gérer l'accès aux annonces légitimes en utilisant la catégorie de ressources Internet *Bannières* dans les paramètres du Contrôle Internet.
Mode de fonctionnement : • **Intercepteur de pilote** • **Redirection** • **Proxy externe**	*(ne migre pas)* Kaspersky Endpoint Security prend uniquement en charge le mode Intercepteur de pilote.
Paramètres de connexion au service ICAP	*(ne migre pas)* Kaspersky Endpoint Security ne prend pas en charge la Protection ICAP des stockages réseau connectés.
Vérifier les connexions sécurisées via le protocole HTTPS	Mode **Analyser les connexions chiffrées** / **Toujours analyser les connexions chiffrées** (sous-section **Paramètres du réseau**)
Utiliser le protocole TLS version	*(ne migre pas)* Kaspersky Endpoint Security analyse le trafic réseau chiffré transmis via les protocoles suivants : • SSL 3.0 ; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Vous pouvez en outre bloquer les connexions SSL 2.0 dans les paramètres d'analyse des connexions chiffrées.
Ne pas faire confiance aux serveurs Internet dotés d'un certificat non valide	**Adresse** (sous-section **Paramètres du réseau**)
Intercepter les ports (Zone d'interception)	**Ports contrôlés** (sous-section **Paramètres du réseau**) Lors de la migration, KES décoche les cases **Contrôler tous les ports pour les applications de la liste recommandée par Kaspersky** et **Contrôler tous les ports pour les applications indiquées**.
Exclure les ports (Zone d'interception)	*(ne migre pas)*
Exclure les adresses IP (Zone d'interception)	**Configurer les adresses de confiance** (sous-section **Paramètres du réseau**)
Exclure les processus (Zone d'interception)	**Configurer les applications de confiance** (sous-section **Paramètres du réseau**) Lors de la migration, KES configure les paramètres suivants pour l'application de confiance : • La case **Ne pas analyser le trafic réseau** est sélectionnée. KES n'analyse pas le trafic réseau à la recherche d'adresses IP distantes et de ports. • Les autres cases à cocher dans les paramètres de l'application de confiance sont désactivées.
Port de sécurité	*(ne migre pas)*
Analyser les liens Internet à l'aide de la base de données des adresses Internet malveillantes	**Vérifier l'adresse Internet par rapport à la base de données des adresses Internet malveillantes** (sous-section **Protection contre les menaces Internet**)
Analyser les pages Internet à l'aide de la base de données anti-phishing	**Vérifier l'adresse Internet par rapport à la base de données des adresses Internet de phishing** (sous-section **Protection contre les menaces Internet**)
Utiliser KSN pour la protection	*(ne migre pas)* Kaspersky Endpoint Security utilise KSN pour tous les modules d'application.
Utiliser la zone de confiance	*(ne migre pas)* Kaspersky Endpoint Security applique la zone de confiance à tous les modules. Vous pouvez configurer les exclusions dans les paramètres de la zone de confiance.
Utiliser l'analyse heuristique	**Utiliser l'analyse heuristique** (sous-sections **Protection contre les menaces Internet** and **Protection contre les menaces par emails**)
Niveau de sécurité	*(ne migre pas)* Kaspersky Endpoint Security possède ses propres niveaux de sécurité pour les modules Protection contre les menaces Internet et Protection contre les menaces par emails. Par défaut, Kaspersky Endpoint Security définit le niveau de sécurité recommandé.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Activer la protection contre les menaces email	**Protection contre les menaces par emails** (sous-section **Protection contre les menaces par emails**) **Connecter l'extension Microsoft Outlook** **Analyser uniquement les messages entrants** (Zone de protection) **Analyser à la réception** (Protection du courrier)
Paramètres de planification	*(ne migre pas)* Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Protection contre les Exploits

Les paramètres de la Protection contre les Exploits de KSWS sont migrés vers la section **Protection avancée**, dans la sous-section **Protection contre les Exploits**.

Paramètres de protection contre les exploits

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Empêcher l'exploit des processus vulnérables : • **Terminer en cas d'exploit** • **Informer uniquement**	**En cas de détection d'un exploit** : • **Bloquer**. • **Informer**.
Signaler les processus exploités via le service de terminal	*(ne migre pas)* Kaspersky Endpoint Security ne prend pas en charge les services de terminal.
Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé	*(ne migre pas)* Kaspersky Endpoint Security empêche en permanence les exploits des processus vulnérables.
Processus protégés	**Activer la protection de la mémoire des processus système** Kaspersky Endpoint Security ne prend pas en charge la sélection des processus protégés. Vous pouvez uniquement activer la protection de la mémoire des processus système.
Techniques de protection contre les exploits : • **Appliquer toutes les techniques de protection contre les exploits disponibles** • **Appliquer les techniques de protection contre les exploits indiquées**	*(ne migre pas)* Kaspersky Endpoint Security applique toutes les techniques de protection contre les exploits disponibles.

Protection contre les menaces réseau

Les paramètres de la Protection contre les menaces réseau de KSWS sont migrés vers la section **Protection principale**, dans la sous-section **Protection contre les menaces réseau**.

Paramètres de la Protection contre les menaces réseau

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Mode de fonctionnement : • **Pass-through** • **Informer uniquement sur les attaques réseau** • **Bloquer les connexions quand une attaque est détectée**	**Protection contre les menaces réseau** Si le mode **Pass-through** est sélectionné, la Protection contre les menaces réseau est désactivée. Si le mode **Informer uniquement sur les attaques réseau** ou **Bloquer les connexions quand une attaque est détectée** est sélectionné, la Protection contre les menaces réseau est activée. Kaspersky Endpoint Security fonctionne toujours en mode **Bloquer les connexions quand une attaque est détectée**.
Ne pas arrêter l'analyse du trafic lorsque la tâche n'est pas exécutée	*(ne migre pas)* Kaspersky Endpoint Security analyse le trafic en continu si le module est activé.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Ne pas contrôler les adresses IP exclues	**Exclusions**
Paramètres de planification	*(ne migre pas)* Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Surveillance des scripts

Kaspersky Endpoint Security ne prend pas en charge le module Surveillance des scripts. La Surveillance des scripts est assurée par d'autres modules, par exemple, la protection AMSI.

Catégories de sites

Kaspersky Endpoint Security ne prend pas en charge toutes les catégories de Kaspersky Security for Windows Server. Les catégories qui n'existent pas dans Kaspersky Endpoint Security ne font pas l'objet d'une migration. Par conséquent, les règles de classification d'une ressource Internet dont les catégories ne sont pas prises en charge ne font pas l'objet d'une migration.

Catégories de sites

Catégories de Kaspersky Security for Windows Server	Catégories de Kaspersky Endpoint Security for Windows
Jeux de guerre	Jeux vidéo
Avortement	*(ne migre pas)*
Loteries (étendu)	Jeux de hasard, loterie, tirages au sort
Alcool	Alcool, tabac, stupéfiants
Serveurs proxy anonymes	Sites Internet de navigation anonyme
Anorexie	*(ne migre pas)*
Locations immobilières	*(ne migre pas)*
Audio, vidéo et logiciels	Logiciel, audio, vidéo
Banques	Banques
Blogs	Blogs
Militaire	Armes, explosifs, contenu militaire
Enfants	*(ne migre pas)*
Discrimination	Violence, intolérance
Maison et famille	*(ne migre pas)*
Services d'hébergement et de domaine	Communication via Internet
Animaux	*(ne migre pas)*
Droit et politique	Interdit par les lois régionales
Limité par Roskomnadzor (Féd. de Russie)	Interdit conformément aux lois de la Fédération de Russie
Limité par la Loi fédérale 436 (Féd. de Russie)	Interdit conformément aux lois de la Fédération de Russie
Limité par la législation (Féd. de Russie)	Interdit conformément aux lois de la Fédération de Russie
Limité par la législation mondiale	Interdit par les lois régionales
Rencontre pour plus de 18 ans	Contenu pour adultes
Services Internet	*(ne migre pas)*
Sex shops	Contenu pour adultes
Technologies de l'information	*(ne migre pas)*
Casinos, jeux de cartes	Jeux de hasard, loterie, tirages au sort

Catégories de Kaspersky Security for Windows Server	Catégories de Kaspersky Endpoint Security for Windows
Livres et littérature	*(ne migre pas)*
Jeux	Jeux vidéo
Santé et beauté	*(ne migre pas)*
Culture et société	*(ne migre pas)*
LGBT	Contenu pour adultes
Loteries	Jeux de hasard, loterie, tirages au sort
Médecine	*(ne migre pas)*
Mode	*(ne migre pas)*
Musique	*(ne migre pas)*
Narcotiques	Alcool, tabac, stupéfiants
Violence	Violence, intolérance
Mécontentement	*(ne migre pas)*
Drogue illicites	Alcool, tabac, stupéfiants
Haine et discrimination	Violence, intolérance
Vocabulaire obscène	Vulgarité, obscénités
Lingerie	Contenu pour adultes
Actualités	Médias d'actualités
Nudisme	Contenu pour adultes
Enseignement	*(ne migre pas)*
Boutiques en ligne	Boutiques en ligne
Tous les supports de communication	Communication via Internet
Paiement par carte de crédit	Systèmes de paiement
Boutiques en ligne (propre système de paiement)	Boutiques en ligne
Encyclopédies en ligne	*(ne migre pas)*
Banques en ligne	Banques
Armes	Armes, explosifs, contenu militaire
Pêche et chasse	*(ne migre pas)*
Systèmes de paiement	Systèmes de paiement
Recherche d'emploi	Recherche d'emploi
Moteurs de recherche	*(ne migre pas)*
Décision de police (JP)	Interdit par la police japonaise
De confiance pour KPSN	*(ne migre pas)*
Douteux pour KPSN	*(ne migre pas)*
Porno	Contenu pour adultes
Hébergement et diffusion sur les médias	Médias d'actualités
Courrier Internet	Emails en ligne
Voyages	*(ne migre pas)*
TV et radio	Médias d'actualités
Services de bandes-annonces et d'annonces	Bannières
Religion	Religions, associations religieuses
Restaurants, cafés et alimentation	*(ne migre pas)*

Catégories de Kaspersky Security for Windows Server	Catégories de Kaspersky Endpoint Security for Windows
Sites de rencontres	Sites de rencontres
Éducation sexuelle	Contenu pour adultes
Réseaux sociaux	Réseaux sociaux
Sport	*(ne migre pas)*
Paris	Jeux de hasard, loterie, tirages au sort
Suicide	Violence, intolérance
Tabac	Alcool, tabac, stupéfiants
Torrents	Torrents
Mentionné dans la Liste fédérale des extrémistes (Féd. de Russie)	Interdit conformément aux lois de la Fédération de Russie
Stockage de fichiers	Stockage de fichiers
Pharmacie	*(ne migre pas)*
Loisirs	*(ne migre pas)*
Chats et forums	Chats, forums, messages
Pages d'écoles et d'universités	*(ne migre pas)*
Astrologie et ésotérisme	*(ne migre pas)*
Extrémisme et racisme	Violence, intolérance
E-commerce	Boutiques en ligne
Érotique	Contenu pour adultes
Humour	*(ne migre pas)*

Contrôle de l'activité locale

Contrôle du lancement des applications

Les paramètres du Contrôle des applications de KSWS sont migrés vers la section **Contrôles de sécurité**, dans la sous-section **Contrôle des applications**.

Paramètres du Contrôle du lancement des applications

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Mode de fonctionnement : • **Statistiques seulement** • **Actif**	**Action** (Contrôle des applications) : • **Tester les règles**. • **Appliquer les règles**.
Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs	*(ne migre pas)* Kaspersky Endpoint Security analyse l'application chaque fois qu'elle tente de s'exécuter.
Interdire le lancement de l'interpréteur de commande sans commande à exécuter	*(ne migre pas)* Kaspersky Endpoint Security autorise l'exécution d'interpréteurs de commandes s'ils ne sont pas interdits par le Contrôle des applications.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Règles	**Règles du Contrôle des applications** *(pris en charge avec des limitations)* Kaspersky Endpoint Security 11.11.0 introduit la prise en charge de la migration des règles de contrôle du lancement des applications. La fonctionnalité de migration des règles de contrôle du lancement des applications présente certaines limitations. Par défaut, le contrôle du lancement des applications KSWS inclut deux règles : • **Autoriser les scripts et les paquets MSI en fonction du certificat reconnu par le système d'exploitation** • **Autoriser les fichiers exécutables en fonction du certificat reconnu par le système d'exploitation** Si au moins une règle KSWS source a le type **Autoriser**, pendant la migration, KES crée une nouvelle règle d'autorisation **Applications avec certificats racine de confiance**. C'est-à-dire que le Contrôle des applications KES utilise une seule règle pour autoriser l'exécution de scripts approuvés, de paquets MSI et de fichiers exécutables. Si les deux règles KSWS source ont le type **Interdire**, KES n'ajoute pas de règles pour administrer les applications avec des certificats racine de confiance.
Utiliser les règles pour les fichiers exécutables	*(ne migre pas)* La zone d'application de la règle ne peut pas être configurée dans les paramètres du contrôle des applications KES. Le contrôle des applications KES applique des règles à tous les types de fichiers : fichiers exécutables, scripts et paquets MSI. Si tous les types de fichiers sont inclus dans la zone d'application de règles dans KSWS, pendant la migration, KES reprend les règles KSWS. Si un type de fichier est exclu de la zone d'application de règle dans KSWS, pendant la migration, KES reprend également les règles KSWS, mais les **Tester les règles** sont sélectionnées comme action du contrôle des applications.
Contrôle du chargement des modules DLL	**Surveiller le téléchargement des modules DLL (augmente considérablement la charge sur le système)**
Utiliser les règles pour les scripts et les paquets MSI	*(ne migre pas)* La zone d'application de la règle ne peut pas être configurée dans les paramètres du contrôle des applications KES. Le contrôle des applications KES applique des règles à tous les types de fichiers : fichiers exécutables, scripts et paquets MSI. Si tous les types de fichiers sont inclus dans la zone d'application de règles dans KSWS, pendant la migration, KES reprend les règles KSWS. Si un type de fichier est exclu de la zone d'application de règles dans KSWS, pendant la migration, KES reporte les règles KSWS, mais les **Tester les règles** sont sélectionnées comme action du contrôle des applications.
Interdire les applications douteuses selon le KSN	*(ne migre pas)* Kaspersky Endpoint Security ne tient pas compte de la réputation des applications et autorise ou interdit l'exécution des applications conformément aux règles.
Autoriser les applications de confiance selon le KSN	Lors de la migration, KES ajoute une nouvelle règle d'autorisation. La catégorie KL **Autres programmes\Applications de confiance selon la réputation dans KSN** est spécifiée comme condition de déclenchement de la règle.
Utilisateurs et/ou groupes d'utilisateurs autorisés à lancer les applications de confiance d'après KSN	**Utilisateurs et leurs droits** dans une règle d'autorisation du Contrôle des applications qui inclut la catégorie KL **Autres programmes\Applications de confiance selon la réputation dans KSN**.
Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Au cours de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications pour lesquelles la distribution automatique de logiciels est autorisée. Le hachage du fichier est spécifié comme condition de déclenchement de la règle.
Toujours autoriser la diffusion de logiciel via Windows Installer	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Lors de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications dont la distribution automatique de logiciels est autorisée (**Applications et paquets de distribution de logiciels autorisés**). Le hachage du fichier est spécifié comme condition de déclenchement de la règle. Dans les propriétés du compte, la case **Programmes de mise à jour de confiance** est cochée.
Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)	*(ne migre pas)*
Liste des applications et des paquets de distribution autorisés	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Au cours de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications pour lesquelles la distribution automatique de logiciels est autorisée. Le hachage du fichier est spécifié comme condition de déclenchement de la règle. Dans les propriétés du compte, la case **Programmes de mise à jour de confiance** est cochée.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Paramètres de planification	*(ne migre pas)* Si une planification est configurée pour le module dans les paramètres KSWS, le module Contrôle des applications est activé lors de la migration. Si une planification n'est pas configurée pour le module dans les paramètres KSWS, le Contrôle des applications est désactivé lors de la migration. Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Contrôle des appareils

Les paramètres du Contrôle des appareils de KSWS sont migrés vers la section **Contrôles de sécurité**, dans la sous-section **Contrôle des appareils**.

Paramètres du contrôle des appareils

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Mode de fonctionnement : • **Actif** • **Statistiques seulement**	*(ne migre pas)* Le Contrôle des applications fonctionne en mode *actif*. Les statistiques de connexion des appareils sont fournies en permanence par Audit.
Autoriser l'utilisation de tous les appareils externes quand la tâche Contrôle des appareils n'est pas exécutée	*(ne migre pas)* Le Contrôle des appareils est toujours actif lorsque Kaspersky Endpoint Security fonctionne.
Règles du Contrôle des appareils	**Appareils de confiance** Lors de la migration, Kaspersky Endpoint Security ignore les règles désactivées de KSWS.
Paramètres de planification	*(ne migre pas)* Kaspersky Endpoint Security utilise sa propre planification pour accéder à certains types d'appareils.

Protection des stockages réseau

Protection RPC des stockages réseau connectés

Kaspersky Endpoint Security ne prend pas en charge les modules de Protection des stockages réseau. Si vous avez besoin de ces modules, vous pouvez continuer à utiliser Kaspersky Security for Windows Server.

Protection ICAP des stockages réseau connectés

Kaspersky Endpoint Security ne prend pas en charge les modules de Protection des stockages réseau. Si vous avez besoin de ces modules, vous pouvez continuer à utiliser Kaspersky Security for Windows Server.

Protection contre le chiffrement pour NetApp

Kaspersky Endpoint Security ne prend pas en charge la Protection contre le chiffrement pour NetApp. La fonctionnalité Protection contre le chiffrement est assurée par d'autres modules d'application, comme la Détection comportementale.

Contrôle de l'activité réseau

Gestion du pare-feu

Kaspersky Endpoint Security ne prend pas en charge la gestion du pare-feu de KSWS. Les fonctionnalités du Pare-feu de KSWS sont assurées par le Pare-feu au niveau du système. Après la migration, vous pouvez configurer le Pare-feu de Kaspersky Endpoint Security.

Protection contre le chiffrement

Les paramètres de la Protection contre le chiffrement du réseau sont migrés vers la section **Protection avancée**, dans la sous-section **Détection comportementale**.

Paramètres de la protection contre le chiffrement

Paramètres KSWS	Paramètres KES
Mode de fonctionnement : • **Statistiques seulement** • **Actif**	**Lors de la détection du chiffrement externe de dossiers partagés** : • **Informer**. • **Bloquer**.
Analyse heuristique	*(ne migre pas)* Kaspersky Endpoint Security n'utilise pas l'analyse heuristique pour la Détection comportementale.
Configuration de la zone de protection : • **Tous les dossiers réseau partagés de l'appareil protégé** • **Uniquement les dossiers partagés indiqués**	*(ne migre pas)* Kaspersky Endpoint Security empêche le chiffrement de tous les dossiers réseau partagés de l'ordinateur protégé.
Exclusions	*(ne migre pas)* Kaspersky Endpoint Security prévoit ses propres exclusions pour le module Détection comportementale. Vous pouvez ajouter manuellement des exclusions après la migration.
Paramètres de planification	*(ne migre pas)* Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Diagnostic du système

Contrôle de l'intégrité des fichiers

Les paramètres Contrôle de l'intégrité des fichiers de KSWS sont migrés vers la section **Contrôles de sécurité**, dans la sous-section **Contrôle de l'intégrité du système**.

Paramètres du Contrôle de l'intégrité des fichiers

Paramètres KSWS	Paramètres KES
Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du contrôle	*(ne migre pas)* Kaspersky Endpoint Security n'enregistre pas les événements des opérations sur les fichiers effectuées pendant la période d'interruption du moniteur.
Bloquer les tentatives de compromission du journal USN	*(ne migre pas)* Kaspersky Endpoint Security ne bloque pas les tentatives de compromission du journal USN.
Zone de surveillance	**Zone de surveillance** → **Fichier** *(pris en charge avec des limitations)* Les enregistrements de la zone de surveillance désactivés ne sont pas migrés vers KES. Kaspersky Endpoint Security ajoute uniquement les enregistrements activés à la zone de surveillance.

Paramètres KSWS	Paramètres KES
Utilisateurs de confiance	**Utilisateurs et/ou groupes d'utilisateurs de confiance**
Marqueurs d'opérations sur les fichiers	**Marqueurs d'opérations sur les fichiers**
Calculer la somme de contrôle pour le fichier si possible	**Hachage**
Exclusions	**Exclusions → Fichier**

Inspection des journaux

Les paramètres d'inspection des journaux de KSWS sont migrés vers la section **Contrôles de sécurité**, dans la sous-section **Inspection des journaux**.

Paramètres de l'Inspection des journaux

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Inspecter les journaux selon les règles personnalisées	*(ne migre pas)* Kaspersky Endpoint Security applique toutes les règles personnalisées activées.
Règles personnalisées	**Règles personnalisées** La règle prédéfinie **Service (pour Server 2003) installé dans le système** n'est pas migrée vers KES.
Inspecter les journaux selon les règles prédéfinies	*(ne migre pas)* Kaspersky Endpoint Security applique toutes les règles prédéfinies activées.
Règles prédéfinies	**Règles prédéfinies**
Détection des attaques brute-force contre les mots de passe	**Détection d'une attaque par force brute**
Détection de la connexion au réseau	**Détection des connexions au réseau**
Exclusions (Adresses IP)	**Exclusions** (Adresse IP)
Exclusions (utilisateurs)	**Exclusions** (Utilisateurs)
Paramètres de planification	*(ne migre pas)* Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Journaux et notifications

Journaux d'exécution de la tâche

Les paramètres des Journaux de KSWS sont migrés vers la section **Paramètres généraux**, dans les sous-sections **Interface** et **Rapports et stockage**.

Paramètres des journaux

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Enregistrement des événements dans le journal	**Notifications** (sous-section **Interface**)
Dossier des journaux	*(ne migre pas)* Kaspersky Endpoint Security enregistre les rapports dans le dossier `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Supprimer les journaux d'exécution de la tâche de plus de X jour(s)	*(ne migre pas)* Vous pouvez configurer la période de stockage des rapports KES sous **Paramètres généraux**, **Rapports et stockage**.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Supprimer les événements du journal d'audit système X jour(s)	*(ne migre pas)* Kaspersky Endpoint Security applique des limitations de stockage des rapports à tous les rapports, y compris aux rapports d'audit système.
Intégration de SIEM	*(ne migre pas)* Vous pouvez configurer l'intégration à SIEM dans Kaspersky Security Center.

Notifications sur les événements

Les paramètres des notifications de KSWS sont migrés vers la section **Paramètres généraux**, dans la sous-section Interface.

Configuration des notifications

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Notifications	**Notifications**
Informer les utilisateurs : • **Informer via le service terminal** • **Informer via une commande du service Windows Messenger**	*(ne migre pas)* Kaspersky Endpoint Security ne prend pas en charge la modification du texte des notifications. Kaspersky Endpoint Security affiche les notifications standards.
Informer les administrateurs : • **Informer via une commande du service Windows Messenger** • **Lancer le fichier exécutable** • **Informer par email**	Seuls les paramètres de notification par email sont migrés vers Kaspersky Endpoint Security – **Paramètres des notifications par email** (groupe **Notifications**). Les autres méthodes de notification aux administrateurs ne sont pas prises en charge.
Bases de l'application dépassées	**Envoyer la notification "Bases dépassées" si la mise à jour des bases n'a pas eu lieu**
Bases de l'application fortement dépassées	**Envoyer la notification "Bases fortement dépassées" si la mise à jour des bases n'a pas eu lieu**
Analyse rapide non réalisée depuis longtemps	*(ne migre pas)* Kaspersky Endpoint Security génère un événement d'analyse des zones critiques manqué après trois jours.

Interaction avec le serveur d'administration

Les paramètres du Serveur d'administration de KSWS sont migrés vers la section **Paramètres généraux**, dans la sous-section Rapports et stockage.

Paramètres d'interaction du Serveur d'administration

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Fichiers en quarantaine	**Fichiers de quarantaine**
Fichiers sauvegardés	**Fichiers de la sauvegarde**
Ordinateurs bloqués	*(ne migre pas)* Kaspersky Endpoint Security envoie automatiquement des données sur les hôtes bloqués.

Tâches

Activation de l'application

Kaspersky Endpoint Security ne prend pas en charge la tâche *Activation de l'application* (KSWS). Vous pouvez créer une tâche *Ajout d'une clé* (KES), ajouter une clé de licence au paquet d'installation ou activer la distribution automatique des clés de licence.

Copie des mises à jour

Les paramètres de la tâche *Copie des mises à jour* (KSWS) sont migrés vers la tâche *Mise à jour des bases et des modules d'application* (KES).

Paramètres de la tâche Copie des mises à jour

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Source des mises à jour : • **Serveur d'administration Kaspersky Security Center** • **Serveurs de mise à jour de Kaspersky** • **Serveurs HTTP, FTP ou dossiers réseau personnalisés**	**Source des mises à jour** : • **Kaspersky Security Center**. • **Serveurs de mises à jour de Kaspersky**. • **Défini par l'utilisateur**.
Utiliser les serveurs de mise à jour de Kaspersky si les serveurs indiqués ne sont pas disponibles	*(ne migre pas)* Kaspersky Endpoint Security permet de sélectionner plusieurs sources de mise à jour, y compris les serveurs de mises à jour de Kaspersky. Si la première source de mise à jour n'est pas disponible, Kaspersky Endpoint Security vous permet d'obtenir des mises à jour à partir d'une autre source de la liste.
Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Utiliser les paramètres du serveur proxy pour se connecter aux autres serveurs	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Paramètres de copie des mises à jour : • **Copier les mises à jour des bases de l'application** • **Copier les mises à jour critiques des modules de l'application** • **Copier les mises à jour des bases de l'application et les mises à jour critiques des modules de l'application**	*(ne migre pas)* Kaspersky Endpoint Security copie les mises à jour des bases de données et les mises à jour critiques des modules de l'application dans un seul paquet.
Dossier de conservation locale des mises à jour copiées	**Copier les mises à jour dans le dossier**

Surveillance de l'intégrité des fichiers

Les paramètres de la tâche *Surveillance de l'intégrité des fichiers* (KSWS) sont migrés vers la tâche *Vérification de l'intégrité du système* et vers la section **Contrôles de sécurité**, sous-section **Contrôle de l'intégrité du système**.

Paramètres de la tâche Surveillance de l'intégrité des fichiers

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Algorithme de calcul du hachage : • **MD5** • **SHA256**.	*(ne migre pas)* Kaspersky Endpoint Security utilise l'algorithme SHA256 pour le calcul de la somme de contrôle.
Zone d'analyse	**Zone de surveillance** (sous-section **Contrôle de l'intégrité du système**)

Mise à jour des bases de l'application

Les paramètres de la tâche *Mise à jour des bases de l'application* (KSWS) sont migrés vers la tâche *Mise à jour des bases et des modules d'application* (KES).

Paramètres de la tâche Mise à jour des bases de l'application

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Source des mises à jour : • **Serveur d'administration Kaspersky Security Center** • **Serveurs de mise à jour de Kaspersky** • **Serveurs HTTP, FTP ou dossiers réseau personnalisés**	**Source des mises à jour** : • **Kaspersky Security Center**. • **Serveurs de mises à jour de Kaspersky**. • **Défini par l'utilisateur**.
Utiliser les serveurs de mise à jour de Kaspersky si les serveurs indiqués ne sont pas disponibles	*(ne migre pas)* Kaspersky Endpoint Security permet de sélectionner plusieurs sources de mise à jour, y compris les serveurs de mises à jour de Kaspersky. Si la première source de mise à jour n'est pas disponible, Kaspersky Endpoint Security vous permet d'obtenir des mises à jour à partir d'une autre source de la liste.
Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Utiliser les paramètres du serveur proxy pour se connecter aux autres serveurs	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Réduire la charge sur les I/O du disque	*(ne migre pas)*

Mise à jour des modules de l'application

Les paramètres de la tâche *Mise à jour des modules de l'application* (KSWS) sont migrés vers la tâche *Mise à jour des bases et des modules d'application* (KES).

Paramètres de la tâche Mise à jour des modules de l'application

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Source des mises à jour : • **Serveur d'administration Kaspersky Security Center** • **Serveurs de mise à jour de Kaspersky** • **Serveurs HTTP, FTP ou dossiers réseau personnalisés**	**Source des mises à jour** : • **Kaspersky Security Center**. • **Serveurs de mises à jour de Kaspersky**. • **Défini par l'utilisateur**.
Utiliser les serveurs de mise à jour de Kaspersky si les serveurs indiqués ne sont pas disponibles	*(ne migre pas)* Kaspersky Endpoint Security permet de sélectionner plusieurs sources de mise à jour, y compris les serveurs de mises à jour de Kaspersky. Si la première source de mise à jour n'est pas disponible, Kaspersky Endpoint Security vous permet d'obtenir des mises à jour à partir d'une autre source de la liste.
Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Utiliser les paramètres du serveur proxy pour se connecter aux autres serveurs	*(ne migre pas)* Kaspersky Endpoint Security utilise le serveur proxy pour tous les modules. Vous pouvez configurer la connexion du serveur proxy dans les paramètres du réseau de l'application.
Copier et installer les mises à jour critiques des modules de l'application	**Installer les mises à jour critiques et approuvées**
Rechercher uniquement la présence des mises à jour critiques de l'application	*(ne migre pas)* Kaspersky Endpoint Security vérifie en permanence la disponibilité des mises à jour critiques pour les modules d'application.
Autoriser le redémarrage du système d'exploitation	*(ne migre pas)* Kaspersky Endpoint Security demande à l'utilisateur l'autorisation de redémarrer l'ordinateur.
Recevoir des informations sur les mises à jour des modules de l'application prévues	*(ne migre pas)* Kaspersky Endpoint Security affiche des notifications sur les mises à jour des modules logiciels.

Annulation de la mise à jour des bases de l'application

Les paramètres de la tâche *Annulation de la mise à jour des bases de l'application* (KSWS) sont migrés vers la tâche *Annulation de la mise à jour* (KES). La nouvelle tâche *Annulation de la mise à jour* (KES) a une planification de lancement de tâche – *Manuel*.

Analyse à la demande

Les paramètres de la tâche *Analyse à la demande* (KSWS) sont migrés vers la tâche *Analyse des logiciels malveillants* (KES).

Paramètres de la tâche Recherche de virus

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Zone d'analyse	Zone d'analyse
Niveau de protection : • Protection maximale • Recommandé • Performance maximale	Niveau de sécurité : • **Élevé**. • **Recommandé**. • **Faible**. Les paramètres du niveau de sécurité sont différents dans KSWS et KES.
Objets à analyser : • Tous les objets • Objets analysés en fonction du format • Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus • Objets analysés en fonction de la liste d'extensions indiquée	Types de fichiers : • **Tous les fichiers**. • **Fichiers analysés par format**. • **Fichiers analysés par extension**. Kaspersky Endpoint Security ne permet pas de créer des listes d'extensions personnalisées. Kaspersky Endpoint Security remplace la valeur **Objets analysés en fonction de la liste d'extensions indiquée** par la valeur **Fichiers analysés par extension**.
Sous-dossiers	Inclure les sous-dossiers
Sous-fichiers	*(ne migre pas)*
Analyser les secteurs d'amorçage et la partition MBR	*(ne migre pas)*
Analyser les flux NTFS alternatifs	*(ne migre pas)*
Analyser uniquement les nouveaux fichiers et les fichiers modifiés	Analyser uniquement les nouveaux fichiers et les fichiers modifiés
Analyse des objets composés : • Tout les archives • Toutes les archives SFX • Tout les bases de données de messagerie • Tout les objets compactés • Tout les emails en texte brut • Tout les objets OLE intégrés	Analyse des fichiers composés : • **Analyser les archives**. • **Analyser les archives protégées par mot de passe**. • **Analyser les paquets de distribution**. • **Analyser les fichiers au format de messagerie**. • **Analyser les fichiers aux formats Microsoft Office**.
Actions à exécuter sur les objets infectés et autres : • Désinfecter • Désinfecter. Supprimer si la désinfection est impossible • Supprimer • Exécuter l'action recommandée • Informer uniquement	Action en cas de détection d'une menace : • **Désinfecter ; supprimer si la désinfection est impossible**. • **Désinfecter ; informer si la désinfection est impossible**. • **Informer**.
Actions à exécuter sur les objets probablement infectés : • Quarantaine • Supprimer • Exécuter l'action recommandée • Informer uniquement	*(ne migre pas)* Kaspersky Endpoint Security applique l'action si une menace est détectée.
Exécuter les actions en fonction du type d'objet détecté	*(ne migre pas)*
Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré	*(ne migre pas)*

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Exclure les fichiers	*(ne migre pas)* Kaspersky Endpoint Security applique la zone de confiance à tous les modules. Vous pouvez configurer les exclusions dans les paramètres de la zone de confiance.
Ne pas détecter	*(ne migre pas)*
Arrêter si l'analyse dure plus de X secondes	**Ignorer les fichiers si l'analyse dure plus de X s**
Ne pas analyser les objets composés de plus de X Mo	**Ne pas décompresser les fichiers composés volumineux**
Utiliser la technologie iSwift	**Technologie iSwift**
Utiliser la technologie iChecker	**Technologie iChecker**
Actions sur les fichiers autonomes : • **Ne pas analyser** • **Analyser seulement la partie résidente du fichier** • **Analyser le fichier en entier** • **Uniquement si le fichier a été sollicité durant la période indiquée (jours)** • **Ne pas copier le fichier sur le disque dur local si possible**	*(ne migre pas)* Kaspersky Endpoint Security analyse les fichiers hors ligne dans leur intégralité.

Vérification de l'intégrité de l'application

Les paramètres de la tâche *Vérification de l'intégrité de l'application* (KSWS) sont migrés vers la tâche (KES) *Vérification de l'intégrité de l'application*.

Génération des règles du Contrôle du lancement des applications

Kaspersky Endpoint Security ne prend pas en charge la tâche *Générateur Contrôle du lancement des applications*. Vous pouvez générer des règles dans les paramètres du Contrôle des applications.

Générateur de règles pour le Contrôle des appareils

Kaspersky Endpoint Security ne prend pas en charge la tâche *Générateur de règles pour le Contrôle des appareils*. Vous pouvez générer des règles d'accès dans les paramètres du Contrôle des appareils.

Migration des modules de KSWS

Kaspersky Endpoint Security recherche la présence éventuelle d'autres applications de Kaspersky avant l'installation locale. Si Kaspersky Security for Windows Server est installé sur l'ordinateur, KES détecte l'ensemble des modules KSWS qui sont installés et sélectionne les mêmes modules pour procéder à l'installation.

Les modules KES dont KSWS ne dispose pas sont installés comme suit :

- Les modules Protection AMSI, Prévention des intrusions et Réparation des actions malicieuses sont installés avec les paramètres par défaut.
- Les modules Protection BadUSB, Contrôle évolutif des anomalies, Chiffrement des données et Detection and Response sont ignorés.

Lorsqu'elle est installée à distance, l'application KES ignore l'ensemble des modules de KSWS installés. Le programme d'installation installe les modules que vous sélectionnez dans les propriétés du paquet d'installation. Après l'installation de Kaspersky Endpoint Security et la migration des stratégies et des tâches, les paramètres KES sont configurés conformément aux paramètres KSWS.

Migration des tâches et des stratégies de KSWS

Vous pouvez procéder à la migration des paramètres de stratégie et de tâches de KSWS des façons suivantes :

- En utilisant l'Assistant de conversion de masse des stratégies et des tâches (ci-après également appelé Assistant de migration).

  > L'Assistant de migration pour KSWS est disponible uniquement dans la Console d'administration (MMC). Les paramètres de stratégie et de tâche ne peuvent pas être migrés dans Web Console et Cloud Console.

  L'Assistant de conversion par lots fonctionne différemment selon les versions de Kaspersky Security Center. Nous vous recommandons de mettre à jour la solution vers la version 14.2 ou une version ultérieure. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet de migrer les stratégies vers un profil plutôt que vers une stratégie. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet également de migrer un plus large éventail de paramètres de stratégie.

- Utilisation de l'Assistant de création de la stratégie pour Kaspersky Endpoint Security for Windows.

  L'Assistant de création de la stratégie vous permet de créer une stratégie KES basée sur une stratégie KSWS.

Les procédures de migration des stratégies KSWS sont différentes lors de l'utilisation de l'Assistant de migration et de l'Assistant de création de la stratégie.

Assistant de conversion de masse des stratégies et des tâches

L'Assistant de migration transfère les paramètres de stratégies KSWS dans le profil de stratégie au lieu des paramètres de stratégies KES. Le *profil de stratégie* est un ensemble de paramètres de stratégies qui est activé sur un ordinateur si celui-ci satisfait aux règles d'activation configurées. Le tag de l'appareil `UpgradedFromKSWS` est sélectionné comme critère de déclenchement du profil de stratégie. Kaspersky Security Center ajoute automatiquement le tag `UpgradedFromKSWS` à tous les ordinateurs sur lesquels vous installez KES par-dessus KSWS à l'aide de la tâche d'installation à distance. Si vous avez choisi une méthode d'installation différente, vous pouvez attribuer manuellement le tag aux appareils.

Pour ajouter un tag à un appareil :

1. Créez un tag pour les serveurs — `UpgradedFromKSWS`.

   Pour obtenir plus de détails sur la création de tags pour les appareils, consultez l'aide de Kaspersky Security Center.

2. Créez un groupe d'administration dans la console Kaspersky Security Center et ajoutez les serveurs auxquels vous souhaitez attribuer le tag à ce groupe.

   Vous pouvez regrouper les serveurs à l'aide de l'outil de sélection. Pour obtenir plus de détails sur l'utilisation des sélections, consultez l'aide de Kaspersky Security Center.

3. Sélectionnez tous les serveurs du groupe d'administration dans la console Kaspersky Security Center, ouvrez les propriétés des serveurs sélectionnés et attribuez le tag.

Si vous migrez plusieurs stratégies KSWS, chaque stratégie est convertie en un profil au sein d'une stratégie globale. Si la stratégie KSWS contient déjà des profils, ces profils sont également migrés en tant que profils. En conséquence, vous obtiendrez une stratégie unique qui comprend des profils correspondant à toutes les stratégies KSWS.

Comment utiliser l'Assistant de conversion de masse des stratégies et des tâches pour migrer les paramètres des stratégies KSWS

1. Dans la Console d'administration, sélectionnez le Serveur d'administration et faites un clic droit pour ouvrir le menu contextuel.

2. Choisissez **Toutes les tâches** → **Assistant de conversion de masse des stratégies et des tâches**.

   Ensuite, l'Assistant de conversion de masse des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Étape 1. Sélectionnez l'application dont il faut convertir les stratégies et les tâches

À cette étape, vous devez sélectionner Kaspersky Endpoint Security for Windows. Passez à l'étape suivante.

Étape 2. Conversion des stratégies

L'Assistant de migration crée des profils de stratégie KSWS dans une stratégie KES. Sélectionnez les stratégies de Kaspersky Security for Windows Server que vous souhaitez convertir en profils de stratégie. Passez à l'étape suivante.

L'Assistant de migration commencera alors à convertir les stratégies. Les noms des nouveaux profils de stratégie correspondront aux stratégies KSWS d'origine.

Étape 3. Rapport de migration de stratégie

L'Assistant de migration crée un rapport de migration de stratégie. Le rapport de migration de stratégie contient la date et l'heure auxquelles les stratégies ont été converties, le nom de la stratégie KSWS d'origine, le nom de la stratégie KES cible ainsi que le nom du nouveau profil de stratégie.

Étape 4. Conversion des tâches

L'Assistant de migration crée de nouvelles tâches pour Kaspersky Endpoint Security for Windows. Dans la liste de tâches, sélectionnez les tâches de KSWS que vous souhaitez créer pour Kaspersky Endpoint Security. Les nouvelles tâches seront nommées *<nom de la tâche de KSWS> (convertie)*. Passez à l'étape suivante.

Étape 5. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- De nouveaux profils de stratégie sont ajoutés à la stratégie de Kaspersky Endpoint Security.

  La stratégie comprend des profils avec les paramètres de Kaspersky Security for Windows Server. La nouvelle stratégie porte l'état *Active*. L'Assistant laisse les stratégies de KSWS inchangées.

- Crée de nouvelles tâches de Kaspersky Endpoint Security.

  Les nouvelles tâches sont des copies des tâches de KSWS. L'Assistant laisse les tâches de KSWS inchangées.

Le nouveau profil de stratégie avec les paramètres KSWS sera nommé *UpgradedFromKSWS <Nom de la stratégie de Kaspersky Security for Windows Server>*. Dans les propriétés du profil, l'Assistant de migration sélectionne automatiquement le tag de l'appareil `UpgradedFromKSWS` comme critère de déclenchement. Ainsi, les paramètres du profil de stratégie sont automatiquement appliqués aux serveurs.

Assistant de création d'une stratégie basée sur une stratégie KSWS

Lorsqu'une stratégie KES est créée sur la base d'une stratégie KSWS, l'Assistant transfère en conséquence les paramètres vers la nouvelle stratégie. Autrement dit, une stratégie KES correspondra à une stratégie KSWS. L'Assistant ne convertit pas la stratégie en profil.

Comment utiliser l'Assistant de création de la stratégie pour migrer les paramètres de la stratégie de KSWS ?

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 l'espace de travail, sélectionnez l'onglet **Stratégies**.
4. Cliquez sur **Nouvelle stratégie**.

   L'Assistant de création de la stratégie démarre.
5. Suivez les instructions de l'Assistant de création de stratégie.

Étape 1.

Sélectionnez l'application **Kaspersky Endpoint Security for Windows (14.2)**.

Étape 2.

Saisissez le nom de la stratégie de groupe, par exemple *Stratégie pour le bureau*.

Cochez la case **&Utiliser les paramètres de stratégie d'une version antérieure de l'application**. Cliquez sur **Parcourir** et sélectionnez la stratégie de KSWS.

Étape 3. Participation au Kaspersky Security Network

Lisez la Déclaration de Kaspersky Security Network (KSN) et acceptez-la.

Étape 4.

Choisissez le **Mode standard pour protéger les hôtes**. Kaspersky Endpoint Security fournit une stratégie commune pour tous les modes d'application et types de systèmes d'exploitation.

> Nous recommandons d'utiliser des stratégies différentes selon les modes et les types de systèmes d'exploitation.

Étape 5. Paramètres d'importation

> Cette étape est disponible si vous avez sélectionné la configuration manuelle de la stratégie à l'étape 4.

Vous pouvez créer une stratégie à partir des paramètres de Kaspersky Endpoint Security contenus dans un fichier de configuration CFG. L'Assistant de création d'une stratégie ne prend pas en charge les fichiers de configuration chiffrés. Lors de l'exportation du fichier de configuration, ignorez l'étape de chiffrement du fichier.

Lors de l'importation d'un fichier de configuration CFG de l'application, tous les paramètres de stratégie ne sont pas accessibles à l'Assistant. Par exemple, les profils de stratégie ne figurent pas dans les paramètres de l'application. Si vous souhaitez transférer tous les paramètres et profils vers la stratégie, vous pouvez importer une autre stratégie à partir d'un fichier KLP.

> Lors de l'importation d'un fichier de configuration, Kaspersky Endpoint Security ne transfère pas les mots de passe des conteneurs crypto. Si vous utilisez l'authentification bidirectionnelle lors de la connexion aux serveurs, vous devez spécifier les mots de passe des conteneurs crypto depuis le début.

Étape 6–10. Configuration des paramètres de stratégie

> Cette étape est disponible si vous avez sélectionné la configuration manuelle de la stratégie à l'étape 4.

Suivez les étapes pour gérer les paramètres de stratégie.

Étape 11. Configuration de la zone de confiance

Configurez la zone de confiance. Vous pouvez ajouter des exclusions d'analyse et des applications de confiance prédéfinies. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent également vous aider à configurer rapidement Kaspersky Endpoint Security en mode Light Agent dans les environnements virtuels Citrix et VMware.

Étape 12. Selection de l'état de la stratégie

- **Actif**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.

  Les paramètres de la stratégie active sont conservés sur les ordinateurs clients lors de la synchronisation. Il est impossible d'application simultanément plusieurs stratégies à un ordinateur et pour cette raison, il ne peut y avoir qu'une stratégie active par groupe.

- **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.

  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.

- **Pour les utilisateurs itinérants**. La stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.

Quittez l'Assistant.

Configuration supplémentaire des stratégies et des tâches après la migration

KSWS et KES ont des ensembles de modules et de paramètres de stratégie différents. Par conséquent, après la migration, vous devez vérifier que les paramètres de stratégie répondent aux exigences de sécurité de votre entreprise.

Vérifiez les paramètres de stratégie de base suivants :

- Protection par mot de passe. Les paramètres de protection par mot de passe de KSWS ne font pas l'objet d'une migration. Kaspersky Endpoint Security intègre une fonctionnalité de protection par mot de passe. Si nécessaire, activez la protection par mot de passe et définissez un mot de passe.

- Zone de confiance. Les méthodes utilisées par KSWS et KES pour sélectionner les objets diffèrent. Lors de la migration, KES prend en charge les exclusions définies comme des fichiers individuels ou des chemins d'accès au fichier / dossier. Si KSWS a des exclusions configurées comme une zone prédéfinie ou une URL de script, ces exclusions ne font pas l'objet d'une migration. Après la migration, vous devez ajouter ces exclusions manuellement.

Pour assurer le bon fonctionnement de Kaspersky Endpoint Security sur les serveurs, il est recommandé d'ajouter à la zone de confiance les fichiers importants pour le fonctionnement du serveur. Pour les serveurs SQL, vous devez ajouter des fichiers de base de données MDF et LDF. Pour les serveurs Microsoft Exchange, vous devez ajouter des fichiers CHK, EDB, JRS, LOG et JSL. Vous pouvez utiliser des masques, par exemple, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

- Pare-feu. Les fonctionnalités du Pare-feu de KSWS sont assurées par le Pare-feu au niveau du système. Dans KES, un module distinct est responsable de la fonctionnalité Pare-feu. Après la migration, vous pouvez configurer le Pare-feu de Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security ne prend pas en charge la configuration de KSN pour chaque module. Kaspersky Endpoint Security utilise KSN pour tous les modules d'application. Pour utiliser KSN, vous devez accepter les nouvelles conditions de la Déclaration de Kaspersky Security Network.

- Contrôle Internet. Les règles de blocage pour le contrôle des catégories de trafic Internet sont migrées vers une règle de blocage unique dans Kaspersky Endpoint Security. Kaspersky Endpoint Security ignore les règles d'autorisation pour le contrôle des catégories. Kaspersky Endpoint Security ne prend pas en charge toutes les catégories de Kaspersky Security for Windows Server. Les catégories qui n'existent pas dans Kaspersky Endpoint Security ne font pas l'objet d'une migration. Par conséquent, les règles de classification d'une ressource Internet dont les catégories ne sont pas prises en charge ne font pas l'objet d'une migration. Si nécessaire, ajoutez des règles pour le Contrôle Internet.

- Serveur proxy. Le mot de passe de connexion au serveur proxy ne fait pas l'objet d'une migration. Saisissez le mot de passe à utiliser pour vous connecter manuellement au serveur proxy.

- Horaires des modules individuels. Kaspersky Endpoint Security ne prend pas en charge la configuration d'horaires pour chaque module. Les modules sont toujours actifs lorsque Kaspersky Endpoint Security fonctionne.

- Ensemble de modules. L'ensemble des fonctions disponibles dans Kaspersky Endpoint Security dépend du type du système d'exploitation : poste de travail ou serveur. Par exemple, parmi les outils de chiffrement, seul le chiffrement de disque BitLocker est disponible sur les serveurs.

- Attribut 🔒. L'état de l'attribut 🔒 ne fait pas l'objet d'une migration. L'attribut 🔒 prendra la valeur par défaut. Par défaut, presque tous les paramètres de la nouvelle stratégie ont une interdiction appliquée à la modification des paramètres dans les stratégies enfants et dans l'interface de l'application locale. L'attribut présente la valeur 🔓 des paramètres de stratégie dans la section **Managed Detection and Response (Industrial CyberSecurity)** et dans le groupe de paramètres **Assistance aux utilisateurs** (section **Interface**). Si nécessaire, configurez l'héritage des paramètres de la stratégie parent.

- Manipulation des menaces actives. La désinfection active fonctionne différemment pour les postes de travail et les serveurs. Vous pouvez configurer la désinfection active dans les paramètres de la tâche *Analyse des logiciels malveillants* et dans les paramètres de l'application.

- Mise à jour de l'application. Pour installer les mises à jour et les correctifs majeurs sans redémarrer l'ordinateur, vous devez modifier le mode de mise à jour de l'application. Par défaut, la fonctionnalité Installer les mises à jour de l'application sans redémarrer l'ordinateur est désactivée.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security dispose d'un agent intégré pour travailler avec les solutions Detection and Response. Si nécessaire, transférez les paramètres de la stratégie de Kaspersky Endpoint Agent vers la stratégie de Kaspersky Endpoint Security.

- Tâches *Mise à jour des bases et des modules d'application*. Assurez-vous que les réglages de la tâche *Mise à jour des bases et des modules d'application* ont été migrés correctement. Au lieu des trois tâches de KSWS, KES utilise une seule tâche KES. Vous pouvez optimiser les tâches *Mise à jour des bases et des modules d'application* et supprimer les tâches superflues.

- Autres tâches. Les modules Contrôle des applications, Contrôle des appareils et Surveillance de l'intégrité des fichiers fonctionnent différemment dans KSWS et KES. KES n'utilise pas les tâches *Surveillance de l'intégrité des fichiers*, *Générateur Contrôle du lancement des applications*, *Générateur de règles pour le Contrôle des appareils*. Par conséquent, ces tâches ne font pas l'objet d'une migration. Après la migration, vous pouvez configurer les modules Surveillance de l'intégrité des fichiers, Contrôle des applications et Contrôle des appareils.

Migration de la zone de confiance de KSWS

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas. Vous pouvez migrer des objets de zone de confiance de KSWS vers KES à l'aide de l'*Assistant de conversion de masse des stratégies et des tâches* ou de l'Assistant *pour la création d'une nouvelle stratégie KES basée sur la stratégie KSWS*. KSWS et KES ont des ensembles de fonctionnalités et de modules différents. Par conséquent, après la migration, vous devez vérifier que les exclusions répondent aux exigences de sécurité de votre entreprise. Les méthodes d'ajout d'exclusions à la zone de confiance sont également différentes pour KES et KSWS. L'Assistant de migration ne propose pas d'outils permettant de migrer toutes les exclusions de KSWS. Par conséquent, après la migration, vous devez ajouter manuellement certaines des exclusions de KSWS.

Pour assurer le bon fonctionnement de Kaspersky Endpoint Security sur les serveurs, il est recommandé d'ajouter à la zone de confiance les fichiers importants pour le fonctionnement du serveur. Pour les serveurs SQL, vous devez ajouter des fichiers de base de données MDF et LDF. Pour les serveurs Microsoft Exchange, vous devez ajouter des fichiers CHK, EDB, JRS, LOG et JSL. Vous pouvez utiliser des masques, par exemple, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

Méthodes de création de zones de confiance KES et KSWS.

KSWS		KES
Objet à analyser		
• Zone prédéfinie	*(ne migre pas)*	
• Disque, dossier ou objet réseau	→	**Fichier ou dossier**
• Fichier	→	**Fichier ou dossier**
• Fichier ou adresse Internet du script	*(ne migre pas)*	
Objet détecté	→	**Type d'un objet détecté**
Processus de confiance	→	**Applications de confiance**

Migration des objets analysés

Les exclusions KSWS pour lesquelles la méthode **Objet à analyser** est sélectionnée dans leurs propriétés sont migrées vers les exclusions KES pour lesquelles la méthode **Fichier ou dossier** est sélectionnée dans leurs propriétés, avec certaines limitations. La migration d'une exclusion dépend de la méthode de sélection des objets :

- Zone prédéfinie – *ne fait pas l'objet d'une migration*.

  Après la migration, vous devez ajouter ces exclusions manuellement. Les exclusions en tant que zones prédéfinies doivent être configurées dans les paramètres de la tâche *Analyse des logiciels malveillants*.

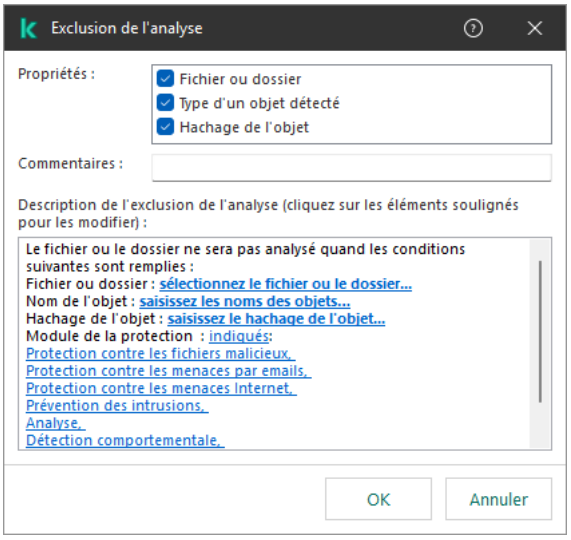
- Disque, dossier ou objet réseau – font l'objet d'une migration vers les exclusions KES pour lesquelles la méthode « Fichier ou dossier » a été sélectionnée dans les propriétés.

- Fichier – fait l'objet d'une migration vers les exclusions KES pour lesquelles la méthode « Fichier ou dossier » a été sélectionnée dans les propriétés.

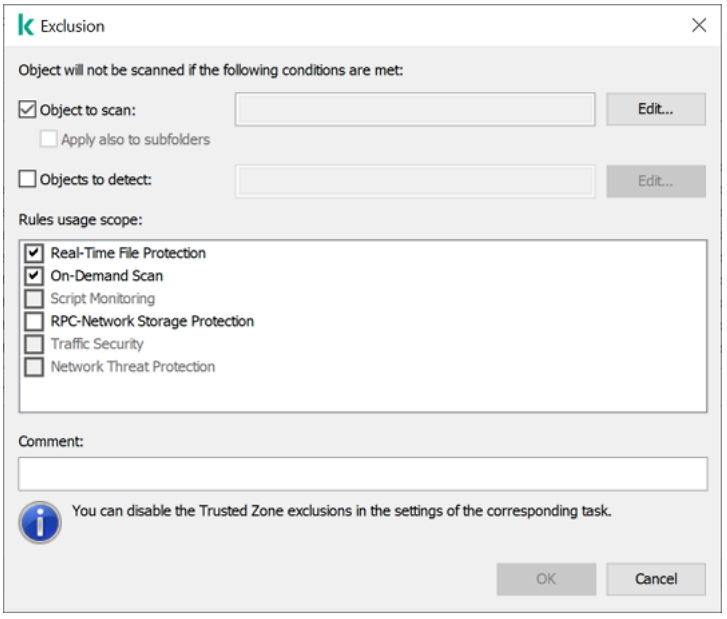
- Fichier ou adresse Internet du script – *ne fait pas l'objet d'une migration*.

  Après la migration, vous devez ajouter ces exclusions manuellement. Les exclusions en tant qu'adresses Internet de script doivent être ajoutées aux adresses Internet de confiance pour la Protection contre les menaces Internet.

Si la case **Appliquer également aux sous-dossiers** est cochée pour l'objet analysé, ce paramètre est migré vers les exclusions KES (la case **Inclure les sous-dossiers**).



Paramètres d'exclusion KES



Paramètres d'exclusion KSWS

Migration des objets détectés

Les exclusions KSWS pour lesquelles la méthode **Objet détecté** est sélectionnée dans leurs propriétés sont migrées vers les exclusions KES pour lesquelles la méthode **Type d'un objet détecté** est sélectionnée dans leurs propriétés. Le nom de l'objet détecté correspond à la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Kaspersky Endpoint Security prend en charge les masques avec le point d'interrogation `?` (correspond à n'importe quel caractère unique) et l'astérisque `*` (correspond à n'importe quelle séquence de caractères).

Migration du champ d'application de l'exclusion

Le champ d'application d'une exclusion est un ensemble de modules auxquels l'exclusion s'applique. KES et KSWS ayant des ensembles de modules différents, l'Assistant de migration ne peut pas migrer le champ d'application de l'exclusion. Par conséquent, si au moins un module est sélectionné dans le champ d'application de KSWS, KES applique l'exclusion à tous les modules de l'application.

Vous pouvez configurer la zone d'application de KSWS dans les paramètres de la zone de confiance ainsi que dans les paramètres des modules de protection de KSWS. Pour ce faire, vous pouvez cocher ou décocher la case **Appliquer la zone de confiance** dans la section correspondante de la stratégie. Les paramètres des modules de protection de KES ne comportent pas de case à cocher de ce type. Cela signifie que l'état de la zone de confiance dans les paramètres des modules individuels est perdu lors de la migration. Une fois que la migration est terminée, sélectionnez les modules auxquels l'exclusion s'applique dans les paramètres de la zone de confiance de la stratégie KES.

Migration des commentaires

Les commentaires de la zone de confiance KSWS sont migrés vers les commentaires d'exclusion KES sans modification.

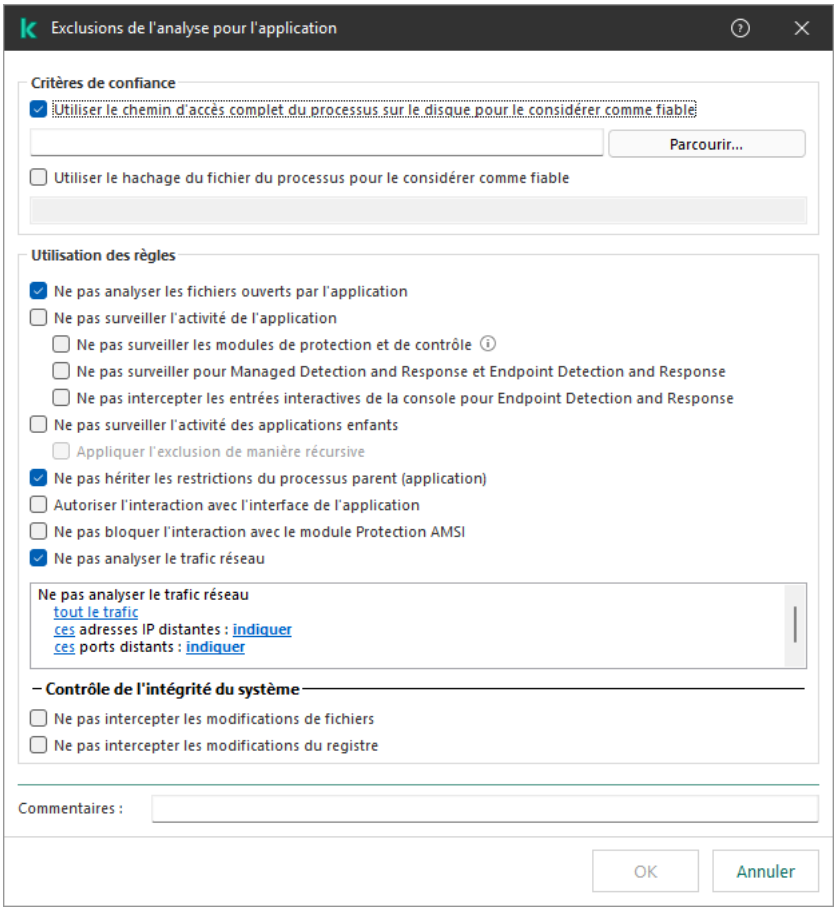
Migration des processus de confiance

Les processus de confiance KSWS sont migrés vers les processus de confiance KES avec certaines limitations. La migration des processus de confiance dépend de la méthode de sélection des objets :

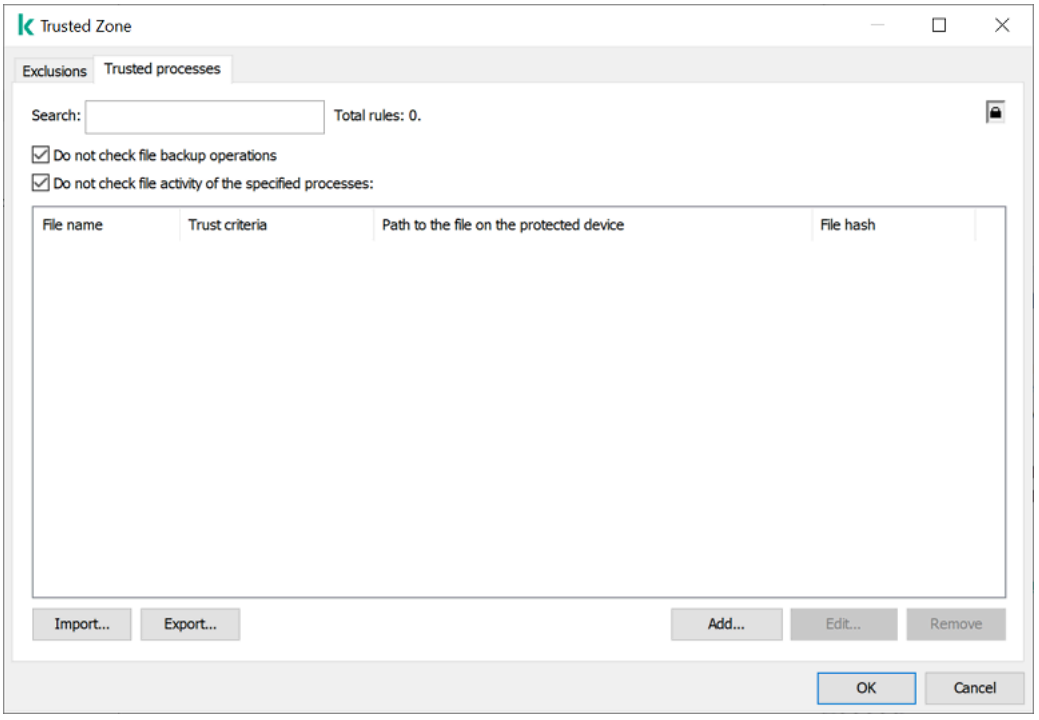
- Chemin d'accès au fichier sur l'appareil protégé – fait l'objet d'une migration vers des applications de confiance KES.
- Hachage du fichier – *ne fait pas l'objet d'une migration*.

Si KSWS a des processus de confiance configurés comme un fichier de hachage, ces processus de confiance ne font pas l'objet d'une migration. Après la migration, vous devez ajouter manuellement ces processus de confiance.

Si la case **Ne pas vérifier les opérations de sauvegarde de fichiers** est cochée dans les paramètres des processus de confiance, ce paramètre est migré vers les applications de confiance KES (la case **Ne pas surveiller l'activité de l'application**).



Paramètres de l'application de confiance KES



Paramètres du processus de confiance KSWS

Migration des règles du Contrôle du lancement des applications de KSWS

Le Contrôle du lancement des applications de KSWS est bloqué par défaut. Autrement dit, le Contrôle du lancement des applications bloque automatiquement toutes les applications qui ne sont pas définies dans les règles comme des applications autorisées. Par conséquent, l'Assistant de migration pour le Contrôle des applications de KES définit automatiquement le mode de contrôle **Liste d'autorisation**, qui correspond au principe de blocage par défaut.

Vous pouvez migrer des règles de KSWS vers KES à l'aide de l'*Assistant de conversion de masse des stratégies et des tâches* ou de l'*Assistant pour la création d'une nouvelle stratégie KES basée sur la stratégie KSWS*.

Migration du mode de Contrôle du lancement des applications

Le mode de Contrôle du lancement des applications de KSWS migre vers le Contrôle des applications de KES comme suit :

- **Statistiques uniquement** → **Tester les règles** ;
- **Actif** → **Appliquer les règles**.

Migration des règles prédéfinies du Contrôle du lancement des applications de KSWS

Par défaut, le contrôle du lancement des applications KSWS inclut deux règles :

- **Autoriser les scripts et les paquets MSI en fonction du certificat reconnu par le système d'exploitation**
- **Autoriser les fichiers exécutables en fonction du certificat reconnu par le système d'exploitation**

Les règles prédéfinies autorisent l'exécution de *scripts*, de *paquets MSI* et de *fichiers exécutables* signés par un certificat racine de confiance. Si au moins une règle KSWS prédéfinie a le type **Autoriser**, l'Assistant de migration crée une nouvelle règle d'autorisation **Applications avec certificats racine de confiance**. C'est-à-dire que le Contrôle des applications KES utilise une seule règle pour autoriser l'exécution de scripts approuvés, de paquets MSI et de fichiers exécutables.

Si les deux règles prédéfinies de KSWS possèdent le type **Refuser**, KES ignore les règles prédéfinies.

Migration des règles personnalisées du Contrôle du lancement des applications de KSWS

Les règles du Contrôle du lancement des applications de KSWS régulent l'exécution des fichiers selon les critères suivants :

- signature à l'aide d'un certificat numérique ;
- hachage SHA256 ;
- chemin du fichier.

Les règles étant créées différemment dans KSWS et KES, l'Assistant de migration crée des *catégories d'applications*, qui incluent les conditions et les exclusions des règles KSWS, et ajoute ces catégories d'applications aux règles KES. L'Assistant utilise les conditions **Certificat**, **Chemin d'accès au dossier** et **Hachage du fichier** dans les catégories d'applications. De nouvelles catégories d'applications sont disponibles dans la Console d'administration de Kaspersky Security Center dans la section **Gestion des applications** → **Catégories d'applications**.

L'Assistant de migration regroupe les règles KSWS par type et par utilisateur. Ensuite, l'Assistant crée des catégories d'applications qui incluent des conditions et des exclusions dans les règles KSWS, et ajoute les catégories d'applications aux nouvelles règles KES. L'Assistant indique les noms des règles KSWS dans le champ **Description** des règles KES.

Migration des paramètres avancés du Contrôle du lancement des applications de KSWS

Le principe de fonctionnement du Contrôle du lancement des applications de KSWS et du Contrôle des applications de KES étant différent, l'Assistant de migration peut migrer un sous-ensemble de paramètres.

Paramètres du Contrôle du lancement des applications

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs	*(ne migre pas)* Kaspersky Endpoint Security analyse l'application chaque fois qu'elle tente de s'exécuter.
Interdire le lancement de l'interpréteur de commande sans commande à exécuter	*(ne migre pas)* Kaspersky Endpoint Security autorise l'exécution d'interpréteurs de commandes s'ils ne sont pas interdits par le Contrôle des applications.
Utiliser les règles pour les fichiers exécutables	*(ne migre pas)* La zone d'application de la règle ne peut pas être configurée dans les paramètres du contrôle des applications KES. Le contrôle des applications KES applique des règles à tous les types de fichiers : fichiers exécutables, scripts et paquets MSI. Si tous les types de fichiers sont inclus dans la zone d'application de règles dans KSWS, pendant la migration, KES reprend les règles KSWS. Si un type de fichier est exclu de la zone d'application de règle dans KSWS, pendant la migration, KES reprend également les règles KSWS, mais les **Tester les règles** sont sélectionnées comme action du contrôle des applications.
Contrôle du chargement des modules DLL	**Surveiller le téléchargement des modules DLL (augmente considérablement la charge sur le système)**
Utiliser les règles pour les scripts et les paquets MSI	*(ne migre pas)* La zone d'application de la règle ne peut pas être configurée dans les paramètres du contrôle des applications KES. Le contrôle des applications KES applique des règles à tous les types de fichiers : fichiers exécutables, scripts et paquets MSI. Si tous les types de fichiers sont inclus dans la zone d'application de règles dans KSWS, pendant la migration, KES reprend les règles KSWS. Si un type de fichier est exclu de la zone d'application de règles dans KSWS, pendant la migration, KES reporte les règles KSWS, mais les **Tester les règles** sont sélectionnées comme action du contrôle des applications.

Paramètres de Kaspersky Security for Windows Server	Paramètres de Kaspersky Endpoint Security for Windows
Interdire les applications douteuses selon le KSN	*(ne migre pas)* Kaspersky Endpoint Security ne tient pas compte de la réputation des applications et autorise ou interdit l'exécution des applications conformément aux règles.
Autoriser les applications de confiance selon le KSN	Lors de la migration, KES ajoute une nouvelle règle d'autorisation. La catégorie KL **Autres programmes\Applications de confiance selon la réputation dans KSN** est spécifiée comme condition de déclenchement de la règle.
Utilisateurs et/ou groupes d'utilisateurs autorisés à lancer les applications de confiance d'après KSN	**Utilisateurs et leurs droits** dans une règle d'autorisation du Contrôle des applications qui inclut la catégorie KL **Autres programmes\Applications de confiance selon la réputation dans KSN**.
Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Au cours de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications pour lesquelles la distribution automatique de logiciels est autorisée. Le hachage du fichier est spécifié comme condition de déclenchement de la règle.
Toujours autoriser la diffusion de logiciel via Windows Installer	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Lors de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications dont la distribution automatique de logiciels est autorisée (**Applications et paquets de distribution de logiciels autorisés**). Le hachage du fichier est spécifié comme condition de déclenchement de la règle. Dans les propriétés du compte, la case **Programmes de mise à jour de confiance** est cochée.
Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)	*(ne migre pas)*
Liste des applications et des paquets de distribution autorisés	Le contrôle de la distribution des logiciels dans KSWS et KES fonctionne différemment. Au cours de la migration, KES ajoute de nouvelles règles d'autorisation pour les applications pour lesquelles la distribution automatique de logiciels est autorisée. Le hachage du fichier est spécifié comme condition de déclenchement de la règle. Dans les propriétés du compte, la case **Programmes de mise à jour de confiance** est cochée.
Paramètres de planification	*(ne migre pas)* Si une planification est configurée pour le module dans les paramètres KSWS, le module Contrôle des applications est activé lors de la migration. Si une planification n'est pas configurée pour le module dans les paramètres KSWS, le Contrôle des applications est désactivé lors de la migration. Il n'est pas possible de configurer une planification distincte pour le module. Le module est toujours actif lorsque Kaspersky Endpoint Security fonctionne.

Installation de KES à la place de KSWS

Vous pouvez installer Kaspersky Endpoint Security des manières suivantes :

- Installation de KES après la suppression de KSWS (recommandé).
- Installation de KES par-dessus KSWS.

Suppression de Kaspersky Security for Windows Server

Vous pouvez supprimer l'application à distance à l'aide de la tâche *Désinstallation à distance d'une application* ou localement sur le serveur. Vous devrez peut-être redémarrer le serveur après avoir supprimé KSWS. Si vous souhaitez installer Kaspersky Endpoint Security sans redémarrage, assurez-vous que Kaspersky Security for Windows Server est complètement supprimé. Si l'application n'est pas complètement supprimée, l'installation de Kaspersky Endpoint Security peut entraîner un dysfonctionnement du serveur. Si vous avez utilisé l'utilitaire kavremover, il est également recommandé de s'assurer que l'application est complètement supprimée. L'utilitaire kavremover ne prend pas en charge la gestion de KSWS.

> Si la Protection par mot de passe est activée pour restreindre l'accès à KSWS, saisissez le mot de passe de désinstallation dans les paramètres du paquet d'installation de KES.

Après avoir supprimé KSWS, installez Kaspersky Endpoint Security for Windows en utilisant n'importe quelle méthode disponible.

Installation de Kaspersky Endpoint Security

Lorsque vous installez KES à distance, les modules que vous avez sélectionnés dans les propriétés du paquet d'installation sont installés sur le serveur. Nous vous recommandons de sélectionner les modules par défaut dans les propriétés du paquet d'installation. Un redémarrage n'est pas nécessaire lors de l'installation de KES par-dessus KSWS.

Kaspersky Endpoint Security recherche la présence éventuelle d'autres applications de Kaspersky avant l'installation locale. Si Kaspersky Security for Windows Server est installé sur l'ordinateur, KES détecte l'ensemble des modules KSWS qui sont installés et sélectionne les mêmes modules pour procéder à l'installation. Un redémarrage n'est pas nécessaire lors de l'installation de KES par-dessus KSWS.

> Si l'installation de KES par-dessus KSWS a échoué, vous pouvez annuler l'installation. Une fois que vous avez annulé l'installation, il est recommandé de redémarrer le serveur et de réessayer.

Les paramètres et les tâches de KSWS ne sont pas migrés lors de l'installation de Kaspersky Endpoint Security for Windows. Pour procéder à la migration des paramètres et des tâches, exécutez l'Assistant de conversion de masse des stratégies et des tâches.

Vous pouvez vérifier la liste des modules installés dans la section **Sécurité** de l'interface de l'application, à l'aide de la commande `status` ou dans la console de Kaspersky Security Center dans les propriétés de l'ordinateur. Vous pouvez modifier l'ensemble des modules après l'installation en utilisant les *Modification de la sélection des modules de l'application*.

Migration de la configuration [KSWS+KEA] vers la configuration [KES+agent intégré]

Pour prendre en charge l'utilisation de Kaspersky Endpoint Security for Windows dans le cadre de EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA et MDR, un agent intégré a été ajouté à l'application. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser ces solutions.

Lors de la migration de KSWS vers KES, les solutions EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA et MDR continuent de fonctionner avec les agents intégrés de Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur.

La migration de la configuration de [KSWS+KEA] vers [KES+agent intégré] comprend les étapes suivantes :

1. **Migration de KSWS vers KES**

   La migration de KSWS vers KES implique l'installation de Kaspersky Endpoint Security au lieu de Kaspersky Security for Windows Server.

   Les administrateurs activent généralement la protection par mot de passe pour restreindre l'accès à KSWS et à KEA. À partir de Kaspersky Security Center Linux 15.1, vous pouvez saisir le mot de passe de désinstallation de l'application dans les paramètres de la tâche *Installation à distance d'une application*. La tâche permet de saisir un seul mot de passe de désinstallation. Autrement dit, si le même mot de passe est défini pour KSWS et KEA, les applications KSWS et KEA sont correctement supprimées. Si les mots de passe diffèrent, une erreur d'accès est signalée lors de la suppression de l'une des applications. Pour terminer la migration, vous devez désactiver la protection par mot de passe pour l'application dont vous n'avez pas pu saisir le mot de passe dans les paramètres de la tâche *Installation à distance d'une application*.

   Pour effectuer la migration, vous devez sélectionner les modules nécessaires pour prendre en charge les solutions Detection and Response dans le cadre de Kaspersky Endpoint Security. Après que l'application a été installée, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

2. **Migration de la stratégie et des tâches**

   La migration des stratégies et des tâches [KSWS+KEA] vers [KES+agent intégré] implique les étapes suivantes :

   1. Migration des stratégies et des tâches de KSWS vers KES à l'aide de l'Assistant de conversion en masse des stratégies et des tâches (uniquement disponible dans la Console d'administration (MMC)).

      Par conséquent, un profil de stratégie portant le nom *UpgradedFromKSWS <nom de la stratégie Kaspersky Security for Windows Server>* est ajouté à la stratégie KES. De nouvelles tâches KES sont également créées avec des noms *<nom de la tâche KSWS> (converti)*.

   2. Migration des stratégies et des tâches de KEA vers KES à l'aide de l'Assistant de migration à partir de Kaspersky Endpoint Agent (uniquement disponible dans Web Console et Cloud Console).

      En conséquence, une nouvelle stratégie est créée portant le nom *<nom de la stratégie Kaspersky Endpoint Security> et <nom de la stratégie Kaspersky Endpoint Agent>*. De nouvelles tâches et tâches KES sont également créées.

3. **Fonctionnalités des licences**

Si vous utilisez une licence commune Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Security for Windows et Kaspersky Endpoint Agent, la fonctionnalité EDR Optimum sera activée automatiquement après la mise à jour de l'application vers la version 11.7.0. Aucune autre action n'est nécessaire.

Si vous utilisez une licence autonome de l'extension Kaspersky Endpoint Detection and Response Optimum pour activer la fonctionnalité EDR Optimum, vous devez vous assurer que la clé de module complémentaire EDR Optimum est ajoutée au stockage de Kaspersky Security Center et que la fonctionnalité de distribution automatique des clés de licence est activée. Une fois que la mise à jour de l'application vers la version 11.7.0 est effectuée, la fonctionnalité EDR Optimum est activée automatiquement.

Si vous utilisez une licence Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security pour activer Kaspersky Endpoint Agent et une autre licence pour activer Kaspersky Endpoint Security for Windows, vous devez remplacer la clé de Kaspersky Endpoint Security for Windows par la clé commune de Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Optimum Security. Vous pouvez remplacer la clé à l'aide de la tâche *Ajout d'une clé*.

Vous n'avez pas besoin d'activer la fonctionnalité de Kaspersky Sandbox. La fonctionnalité de Kaspersky Sandbox sera disponible immédiatement après la mise à jour et l'activation de Kaspersky Endpoint Security for Windows.

Seule la licence Kaspersky Anti Targeted Attack Platform peut être utilisée pour activer Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Anti Targeted Attack Platform. Une fois que la mise à jour de l'application vers la version 12.1 est effectuée, la fonctionnalité EDR (KATA) est activée automatiquement. Aucune autre action n'est nécessaire.

4 **Vérification de l'état de santé de Kaspersky Endpoint Detection and Response Optimum et de Kaspersky Sandbox**

Si après la mise à jour, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

- Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
- Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*.
- Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

Assurez-vous que la fonctionnalité EDR Optimum est activée à l'aide de l'icône *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous que la fonctionnalité de distribution automatique des clés de licence de EDR Optimum est activée.

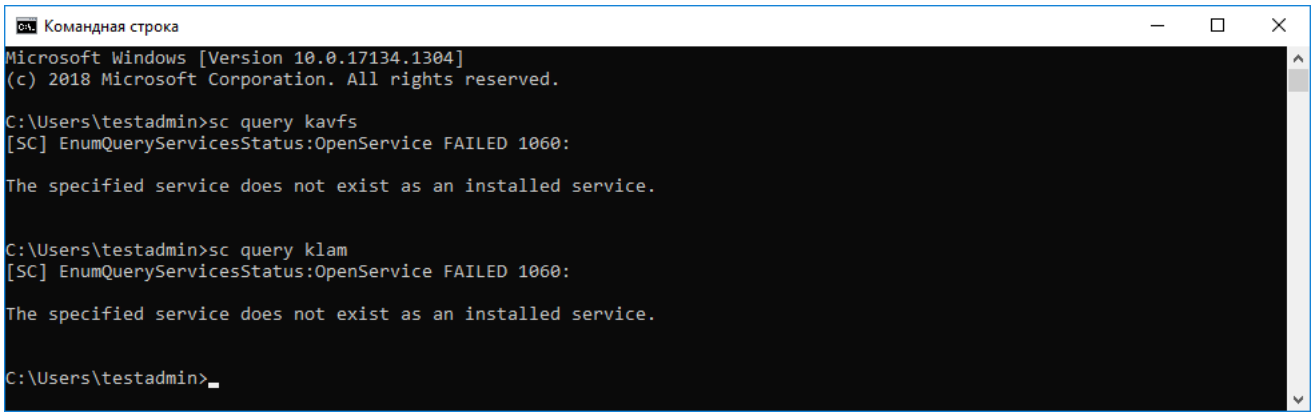
Vérification que Kaspersky Security for Windows Server a bien été supprimé

Assurez-vous que Kaspersky Security for Windows Server est complètement supprimé :

- Le dossier `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` n'existe pas.
- Les services suivants ne sont pas présents :
  - Kaspersky Security Service (KAVFS)
  - Service Kaspersky Security Management (KAVFSGT)
  - Service Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Service Kaspersky Security Script Checker (KAVFSSCS)

  Vous pouvez vérifier les services en cours d'exécution dans le Gestionnaire des tâches ou en lançant la commande `sc query` (cf. ill. ci-dessous).
- Les pilotes suivants ne sont pas présents :
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

Vous pouvez vérifier les pilotes installés dans le dossier `C:\Windows\System32\drivers` ou en lançant la commande `sc query`. Si un service ou un pilote est manquant, vous obtiendrez la réponse suivante :



Vérification que les services Kaspersky Security for Windows Server ont bien été supprimés

Si des fichiers d'application ou de pilote restent sur le serveur, supprimez manuellement les fichiers en question. Si les services de Kaspersky Security for Windows Server sont toujours en cours d'exécution sur le serveur, arrêtez (`sc stop`) et supprimez (`sc delete`) les services manuellement. Pour arrêter le pilote klam.sys, utilisez la commande `fltmc unload klam`.

Activation de KES avec une clé KSWS

Après avoir installé l'application, vous pouvez activer Kaspersky Endpoint Security for Windows (KES) à l'aide d'une clé de licence de Kaspersky Security for Windows Server (KSWS). Le processus d'activation après la migration dépend de la méthode d'activation de KSWS (cf. tableau ci-après).

Kaspersky Endpoint Security ne prend pas en charge la *licence de Kaspersky Security for Storage*. Pour travailler avec cette licence, vous devez utiliser Kaspersky Security for Windows Server.

Pour activer KES avec la clé KSWS, vous ne pouvez utiliser que le code d'activation. Si vous utilisez un fichier clé pour activer l'application, vous devez contacter le support technique et demander un fichier clé de Kaspersky Endpoint Security.

Activation de Kaspersky Endpoint Security for Windows avec une clé de Kaspersky Security for Windows Server

Méthode d'activation de Kaspersky Security for Windows Server	Migration de la clé vers Kaspersky Endpoint Security for Windows.
Distribution automatique de la clé de licence de KSWS aux ordinateurs.	Si la distribution automatique des clés est activée dans les propriétés de la clé de licence de KSWS, KES est automatiquement activé avec la clé de KSWS.
La clé de KSWS est ajoutée par une tâche.	Si KSWS est activé à l'aide de la tâche, la clé de licence KSWS est supprimée lors de la migration depuis KSWS. Vous devez réactiver l'application. Par exemple, vous pouvez ajouter une clé de licence au paquet d'installation de Kaspersky Endpoint Security for Windows.
La clé de KSWS est ajoutée localement dans l'interface de l'application.	Si KSWS est activé localement à l'aide de l'Assistant d'activation de l'application, la clé de licence KSWS est supprimée lors de la migration depuis KSWS. Vous devez réactiver l'application. Par exemple, vous pouvez ajouter une clé de licence au paquet d'installation de Kaspersky Endpoint Security for Windows.
La clé de KSWS est ajoutée au paquet d'installation.	Si KSWS est activée à l'aide de la clé du paquet d'installation, la clé de licence de KSWS est supprimée lors de la migration depuis KSWS. Vous devez réactiver l'application. Par exemple, vous pouvez ajouter une clé de licence au paquet d'installation de Kaspersky Endpoint Security for Windows.

Méthode d'activation de Kaspersky Security for Windows Server	Migration de la clé vers Kaspersky Endpoint Security for Windows.
Image de machine virtuelle payante (Amazon Machine Image – AMI) dans Amazon Web Services (AWS).	Si vous avez acheté Kaspersky Security Center en tant qu'image de machine virtuelle payante (Amazon Machine Image – AMI) dans Amazon Web Services (AWS), l'activation de KES n'est pas nécessaire. Dans ce cas, Kaspersky Security Center utilise l'abonnement AWS qui est déjà ajouté à l'application.
Image Kaspersky Security Center prête à l'emploi et gratuite avec votre propre licence (modèle Apportez votre propre licence).	Si vous utilisez une image Kaspersky Security Center gratuite prête à l'emploi avec votre propre licence dans un environnement cloud (modèle Apportez votre propre licence), vous devez activer l'application en utilisant n'importe quelle méthode disponible. Vous aurez besoin d'une licence Kaspersky Hybrid Cloud Security.

Particularités relatives à la migration de serveurs à forte charge

Sur les serveurs à forte charge, il est important de surveiller les performances et d'éviter les pannes. Après la migration vers Kaspersky Endpoint Security for Windows, nous vous recommandons de désactiver temporairement les modules de l'application qui utilisent des ressources serveur importantes par rapport aux autres modules. Après vous être assuré que le serveur fonctionne normalement, vous pouvez réactiver les modules de l'application.

Nous vous recommandons de migrer les serveurs à forte charge comme suit :

1. Créer une stratégie de Kaspersky Endpoint Security avec les paramètres par défaut.

   Les paramètres par défaut sont considérés comme optimaux. Ces paramètres sont recommandés par les experts de Kaspersky. Les paramètres par défaut fournissent le niveau de protection recommandé et une utilisation optimale des ressources.

2. Dans les paramètres de stratégie, désactivez les modules suivants : Protection contre les menaces réseau, Détection comportementale, Protection contre les Exploits, Réparation des actions malicieuses et Contrôle des applications.

   Si votre organisation a déployé la solution Kaspersky Managed Detection and Response (MDR), chargez le fichier de configuration BLOB dans la stratégie de Kaspersky Endpoint Security.

3. Supprimez Kaspersky Security for Windows Server du serveur.

4. Installez Kaspersky Endpoint Security for Windows avec l'ensemble de modules par défaut.

   Si votre organisation a déployé des solutions de détection et de réponse, sélectionnez les modules appropriés dans les propriétés du paquet d'installation.

5. Vérifiez les paramètres de l'application :

   - L'application est activée avec la clé de licence KSWS.
   - La nouvelle stratégie est appliquée. Les modules précédemment sélectionnés sont désactivés.

6. Assurez-vous que le serveur fonctionne. Assurez-vous que Kaspersky Endpoint Security for Windows n'utilise pas plus de 1 % des ressources du serveur.

7. Si nécessaire, créez des exclusions d'analyse, ajoutez des applications de confiance, créez une liste d'adresses Internet de confiance.

8. Activez les modules Détection comportementale, Protection contre les Exploits et Réparation des actions malicieuses. Assurez-vous que Kaspersky Endpoint Security for Windows n'utilise pas plus de 1 % des ressources du serveur.

9. Activez le module Protection contre les menaces réseau. Assurez-vous que Kaspersky Endpoint Security for Windows n'utilise pas plus de 2 % des ressources du serveur.

10. Activez le module Contrôle des applications dans le mode de test des règles.

11. Assurez-vous que le Contrôle des applications fonctionne. Si nécessaire, ajoutez de nouvelles règles pour le Contrôle des applications et désactivez le mode de test des règles après avoir confirmé que le Contrôle des applications fonctionne.

Une fois que vous avez procédé à la migration de KSWS vers KES, assurez-vous que l'application fonctionne correctement. Vérifiez l'état du serveur dans la console (l'état devrait être *OK*). Assurez-vous qu'aucune erreur n'est signalée pour l'application, vérifiez également l'heure de la dernière connexion au Serveur d'administration, l'heure de la dernière mise à jour de la base de données et l'état de la protection du serveur.

Administration de l'application sur un serveur en mode Server Core

Un serveur en mode Server Core ne présente pas d'interface graphique. Par conséquent, vous ne pouvez gérer l'application qu'à distance à l'aide de la console Kaspersky Security Center ou localement au moyen de la ligne de commande.

Gestion de l'application à l'aide de la console Kaspersky Security Center

L'installation de l'application à l'aide de la console Kaspersky Security Center ne diffère pas de l'installation normale. Lors de la création d'un paquet d'installation, vous pouvez ajouter une clé de licence pour activer l'application. Vous pouvez utiliser une clé Kaspersky Endpoint Security for Windows ou une clé Kaspersky Security for Windows Server.

> Sur un serveur en mode Server Core, les modules de l'application suivants ne sont pas disponibles : Protection contre les menaces Internet, Protection contre les menaces par emails, Contrôle Internet, Prévention des attaques BadUSB, Chiffrement des fichiers (FLE), Kaspersky Disk Encryption (FDE).

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. L'application ne peut pas afficher une fenêtre pour inviter l'utilisateur à redémarrer le serveur. Les rapports de la console de Kaspersky Security Center vous informent de la nécessité de redémarrer le serveur.

La gestion de l'application sur le serveur en mode Server Core n'est pas différente de la gestion d'un ordinateur. Vous pouvez utiliser des stratégies et des tâches pour configurer l'application.

La gestion de l'application sur les serveurs en mode Server Core implique les considérations particulières suivantes :

- Le serveur en mode Server Core ne possède pas d'interface graphique, c'est pourquoi Kaspersky Endpoint Security n'affiche aucun avertissement indiquant à l'utilisateur que la Désinfection active est nécessaire. Pour désinfecter une menace, vous devez appliquer la technologie de désinfection avancée dans les paramètres de l'application et activer la désinfection immédiate de l'infection active dans les paramètres de la tâche *Analyse des logiciels malveillants*. Ensuite, vous devez démarrer la tâche *Analyse des logiciels malveillants*.

- Le chiffrement de disque BitLocker n'est disponible qu'avec Trusted Platform Module (TPM). Un PIN / mot de passe ne peut pas être utilisé pour le chiffrement, car l'application est incapable d'afficher la fenêtre d'invite du mot de passe pour l'authentification avant le démarrage. Si le système d'exploitation prend en charge la norme FIPS (Federal Information Processing Standard), connectez un disque amovible pour enregistrer la clé de chiffrement avant de commencer à chiffrer le disque.

Administration de l'application via la ligne de commande

Lorsque vous ne pouvez pas utiliser une interface graphique, vous pouvez gérer Kaspersky Endpoint Security à partir de la ligne de commande.

Pour installer l'application sur un serveur en mode Server Core, exécutez la commande suivante :

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Pour activer l'application, exécutez la commande suivante :

```
avp.com license /add <activation code or key file>
```

Pour vérifier les états des profils d'application, exécutez la commande suivante :

```
avp.com status
```

Pour afficher la liste des commandes d'administration des applications, exécutez la commande suivante :

```
avp.com help
```

Migration de [KSWS+KEA] vers [KES+agent intégré]

Lors de la migration de Kaspersky Security for Windows Server (KSWS) vers Kaspersky Endpoint Security (KES), vous pouvez utiliser les recommandations suivantes pour configurer la protection du serveur et optimiser les performances. Ici, nous examinerons un exemple de migration pour une seule organisation.

Infrastructure de l'organisation

L'entreprise a installé les équipements suivants :

- Kaspersky Security Center 14.2

  L'administrateur gère les solutions Kaspersky à l'aide de la Console d'administration (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) est également déployé

  Dans Kaspersky Security Center, trois groupes d'administration sont créés, contenant les serveurs de l'organisation : deux groupes d'administration pour les serveurs SQL et un groupe d'administration pour les serveurs Microsoft Exchange. Chaque groupe d'administration est géré par sa propre stratégie. Les tâches *Mise à jour des bases de l'application* et *Analyse à la demande* sont créées pour tous les serveurs de l'organisation.

  La clé d'activation KSWS est ajoutée à Kaspersky Security Center. La distribution automatique des clés est activée.

- Serveurs SQL avec Kaspersky Security for Windows Server 11.0.1 et Kaspersky Endpoint Agent 3.11 installés. Les serveurs SQL sont combinés en deux clusters.

  KSWS est géré par les stratégies *SQL_Policy(1)* et *SQL_Policy(2)*. Les tâches *Mise à jour des bases de l'application* et *Analyse à la demande* sont également créées.

- Un serveur Microsoft Exchange avec Kaspersky Security for Windows Server 11.0.1 et Kaspersky Endpoint Agent 3.11 installés.

  KSWS est géré par la stratégie *Exchange_Policy*. Les tâches *Mise à jour des bases de l'application* et *Analyse à la demande* sont également créées.

Planification de la migration

La migration implique les étapes suivantes :

1. Migration des tâches et des stratégies KSWS à l'aide de l'Assistant de conversion de masse des stratégies et des tâches.

2. Migration de la stratégie de Kaspersky Endpoint Agent à l'aide de l'Assistant de conversion de masse des stratégies et des tâches.

3. Utilisation de tags pour activer les profils de stratégie dans les propriétés de la nouvelle stratégie.

4. Installation de KES à la place de KSWS.

5. Activation d'EDR Optimum.

6. Vérification du fonctionnement de KES.

Le scénario de migration est initialement effectué sur l'un des clusters des serveurs SQL. Ensuite, le scénario de migration est exécuté sur l'autre cluster des serveurs SQL. Ensuite, le scénario de migration est exécuté sur Microsoft Exchange.

Migration des tâches et des stratégies KSWS à l'aide de l'Assistant de conversion de masse des stratégies et des tâches

Pour migrer des tâches KSWS, vous pouvez utiliser l'Assistant de conversion de masse des stratégies et des tâches (l'Assistant de migration). En conséquence, au lieu des stratégies *SQL_Policy(1)*, *SQL_Policy(2)* et *Exchange_Policy*, vous obtiendrez une seule stratégie avec trois profils pour les serveurs SQL et Microsoft Exchange respectivement. Le nouveau profil de stratégie avec les paramètres KSWS sera nommé *UpgradedFromKSWS <Nom de la stratégie de Kaspersky Security for Windows Server>*. Dans les propriétés du profil, l'Assistant de migration sélectionne automatiquement le tag de l'appareil `UpgradedFromKSWS` comme critère de déclenchement. Ainsi, les paramètres du profil de stratégie sont automatiquement appliqués aux serveurs.

Migration de la stratégie de Kaspersky Endpoint Agent à l'aide de l'Assistant de conversion de masse des stratégies et des tâches

Pour migrer les stratégies de Kaspersky Endpoint Agent, vous pouvez utiliser l'Assistant de conversion de masse des stratégies et des tâches. L'Assistant de migration des stratégies et des tâches pour Kaspersky Endpoint Agent est uniquement disponible dans Web Console.

Utilisation de tags pour activer les profils de stratégie dans les propriétés de la nouvelle stratégie

Sélectionnez le tag de l'appareil que vous avez attribué précédemment comme condition d'activation du profil. Ouvrez les propriétés de la stratégie et sélectionnez *Règles générales d'activation du profil de stratégie* comme condition d'activation du profil.

Installation de KES à la place de KSWS

Avant d'installer KES, vous devez désactiver la protection par mot de passe dans les propriétés de la stratégie KSWS.

L'installation de KES implique les étapes suivantes :

1. Préparez le paquet d'installation. Dans les propriétés du paquet d'installation, sélectionnez le kit de distribution de Kaspersky Endpoint Security for Windows 12.0 et sélectionnez l'ensemble de modules par défaut.

2. Créez une tâche *Installation à distance d'une application* pour l'un des groupes d'administration du serveur SQL.

3. Dans les propriétés de la tâche, sélectionnez le paquet d'installation et le fichier clé de licence.

4. Attendez que la tâche se termine avec succès.

5. Répétez l'installation de KES pour les groupes d'administration restants.

Kaspersky Security Center ajoute automatiquement le tag `UpgradedFromKSWS` aux noms d'ordinateurs sur la console une fois l'installation de KES terminée.

Pour vérifier l'installation de KES, vous pouvez utiliser le *rapport sur le déploiement de la protection*. Vous pouvez également vérifier l'état de l'appareil. Pour confirmer l'activation de l'application, vous pouvez utiliser le *rapport sur les clés de licence utilisées*.

Activation d'EDR Optimum

Vous pouvez activer la fonctionnalité EDR Optimum à l'aide d'une licence autonome de l'extension Kaspersky Endpoint Detection and Response Optimum. Vous devez confirmer que la clé EDR Optimum est ajoutée au stockage de Kaspersky Security Center et que la fonctionnalité de distribution automatique des clés de licence est activée.

Pour vérifier l'activation d'EDR Optimum, vous pouvez utiliser le *Rapport sur l'état des modules de l'application*.

Vérification du fonctionnement de KES

Pour confirmer que KES fonctionne, vous pouvez vérifier qu'aucune erreur n'est signalée. L'état de l'appareil doit être *OK*. Tâches de mise à jour et de recherche d'applications malveillantes terminées avec succès.

Mode Light Agent pour protéger les machines virtuelles

À partir de la version 12.8, vous pouvez utiliser Kaspersky Endpoint Security for Windows dans le cadre de Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* est une solution intégrée qui offre une protection complète pour les machines virtuelles contre divers types de menaces informatiques, de réseaux et d'attaques de phishing. Pour utiliser cette solution, il convient d'installer l'application en mode Light Agent.

L'installation de Kaspersky Endpoint Security en mode Light Agent sur des machines virtuelles basées sur l'architecture ARM n'est pas prise en charge.

Vous pouvez utiliser Kaspersky Endpoint Security en mode Light Agent dans le cadre de Kaspersky Security for Virtualization Light Agent à partir de la version 6.2.

Lorsque vous démarrez le Light Agent, il établit et maintient une connexion avec la machine virtuelle SVM (Secure Virtual Machine). Un Serveur de protection est déployé sur la SVM. Le *Serveur de protection* est le module de la solution Kaspersky Security for Virtualization Light Agent qui analyse les fichiers à la recherche de virus et autres programmes malveillants, met à jour les bases antivirus et gère les clés de licence. Le Light Agent envoie à la SVM les fichiers ou les fragments de fichiers qui doivent être analysés. Les résultats de l'analyse sont disponibles pour toutes les machines virtuelles sur lesquelles le Light Agent est installé (la technologie SharedCache). Cette technologie augmente l'efficacité de la solution et accélère la réaction aux menaces.

L'infrastructure de l'organisation peut contenir de nombreuses machines virtuelles sur lesquelles le Light Agent est installé, ainsi que de nombreuses SVM. Le Serveur d'intégration gère l'interaction entre les machines virtuelles et les SVM. Le *Serveur d'intégration* est un module de la solution Kaspersky Security for Virtualization Light Agent qui génère la liste des SVM disponibles et transfère ces données aux Light Agents, participe à la découverte des SVM par les Light Agents, protège la connexion entre les Light Agents et les SVM et assure d'autres fonctions.

Considérations particulières pour le mode Light Agent

Vous pouvez gérer Kaspersky Endpoint Security en mode Standard et en mode Light Agent à l'aide des stratégies et des tâches de Kaspersky Endpoint Security. En mode Light Agent, certains modules et certaines fonctionnalités de l'application ne sont pas disponibles.

Mise à jour des bases de données et des modules de l'application

Kaspersky Endpoint Security en mode Light Agent utilise les bases de données spéciales de programmes malveillants dont l'application a besoin lorsqu'elle travaille dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security obtient les mises à jour des bases de données et des modules de l'application à partir du Serveur de protection.

Les bases de données et les modules des machines virtuelles protégées sont mis à jour à l'aide d'une tâche spéciale *Mise à jour des bases et des modules d'application*, dans laquelle un dossier de la SVM est défini comme source de mises à jour. Le Light Agent exécute automatiquement la tâche *Mise à jour des bases et des modules d'application*. Vous ne pouvez pas sélectionner une autre source de mise à jour, configurer la planification de la tâche ou supprimer la tâche.

Une annulation de la dernière mise à jour des bases de données de programmes malveillants est également gérée du côté du Serveur de protection. Après une annulation de la mise à jour des bases de données et des modules d'application sur la SVM, une tâche locale spéciale *Mise à jour des bases et des modules d'application* démarre sur la machine virtuelle protégée. Cette tâche permet au Light Agent d'utiliser de nouveau l'ensemble précédent de bases de données malveillantes.

Kaspersky Endpoint Security en mode Light Agent ne prend pas en charge la tâche *Annulation de la mise à jour*.

Activation du Light Agent

Pour activer l'application, vous devez ajouter une clé de licence à la SVM à laquelle le Light Agent est connecté. Il n'est pas nécessaire d'activer l'application séparément.

Autres particularités du mode Light Agent

- Lors de la création d'une stratégie pour l'application, il est conseillé de sélectionner le mode Light Agent. Dans ce mode, l'Assistant de création d'une stratégie vous invite à configurer la connexion à la SVM. Ces paramètres sont nécessaires au fonctionnement de l'application en mode Light Agent.
- Vous ne pouvez pas installer les modules Chiffrement des données et Contrôle évolutif des anomalies en mode Light Agent. L'ensemble de modules dépend également du type de système d'exploitation invité : poste de travail ou serveur.
- Light Agent ne prend pas en charge l'intégration avec les solutions Kaspersky Endpoint Detection and Response Expert et Kaspersky Endpoint Detection and Response Expert (cloud).
- Vous pouvez gérer le Light Agent dans la Console d'Administration (MMC) et dans Kaspersky Security Center Web Console. Il n'est pas possible d'administrer le Light Agent dans Kaspersky Security Center Cloud Console.
- La modification de l'ensemble des modules d'application sur les machines virtuelles VDI n'est pas prise en charge.
- Kaspersky Endpoint Security communique avec les serveurs KSN via un serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge.
- Le mode Cloud de Kaspersky Security Network n'est pas pris en charge.
- L'utilisation du serveur proxy d'applications lors de la connexion au Serveur d'intégration (VIS), au Serveur de protection (SVM) et aux serveurs KSN n'est pas prise en charge.

Préconfiguration de la machine virtuelle

Vous pouvez installer Kaspersky Endpoint Security sur une machine virtuelle qui utilise la technologie de la plateforme virtuelle. Kaspersky Endpoint Security prend en charge les plateformes virtuelles VMware, Microsoft Hyper-V et Citrix. Avant l'installation, vous devez effectuer la configuration préliminaire des machines virtuelles.

Compatibilité avec la technologie Citrix App Layering

Si vous avez l'intention d'utiliser le Full User Layer pour enregistrer l'état des machines virtuelles temporaires, il faut réaliser les actions suivantes avant d'installer sur le modèle de machine virtuelle :

1. Créez le fichier C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt et ajoutez-y les exclusions suivantes :

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. Dans le registre du système d'exploitation, dans la clé HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, créez une valeur DWORD nommée MiniFilterBypass et définissez-la sur 1.

3. Dans le registre du système d'exploitation, dans la clé HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, créez une valeur MULTI_SZ nommée ExcludeKey et définissez-la sur \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Redémarrez la machine virtuelle.

Pour l'installation sur des machines virtuelles dans une infrastructure qui utilise Citrix App Layering, vous devez procéder comme suit :

1. Installez l'Agent d'administration de Kaspersky Security Center et Kaspersky Endpoint Security for Windows sur le modèle de machine virtuelle dans la couche d'application.

2. Créez une image de machine virtuelle composée de plusieurs couches.

3. Déployez l'image créée sur les hyperviseurs qui prennent en charge la solution Citrix App Layering.

4. Configurer la création de machines virtuelles temporaires à partir de l'image créée.

Pour en savoir plus sur l'installation d'un antivirus en plus de Citrix App Layering, veuillez consulter la documentation relative à Citrix App Layering.

Compatibilité avec la technologie Citrix Provisioning (Citrix Provisioning Services)

Pour vérifier la compatibilité de l'application avec la technologie Citrix Provisioning (Citrix Provisioning Services) :

- Si le logiciel Citrix Provisioning Target Device est installé sur la machine virtuelle, vous devez le désinstaller avant d'installer l'application Kaspersky Endpoint Security (pour en savoir plus, consultez le site Internet de l'assistance technique de Citrix). Après avoir installé l'application, vous devez réinstaller Citrix Provisioning Target Device. Vous devez également réinstaller l'appareil cible Citrix Provisioning lors de la restauration de l'application, notamment lors de la mise à jour du système d'exploitation.

  La mise à jour du système d'exploitation comprend les étapes suivantes :

  1. Supprimez l'appareil cible Citrix Provisioning.
  2. Mettez à jour le système d'exploitation.
  3. Après le démarrage de la machine virtuelle, assurez-vous que l'application Kaspersky Endpoint Security est en cours d'exécution et fonctionne correctement.
  4. Réinstallez l'appareil cible Citrix Provisioning.

- Lors de l'installation de l'application à l'aide de l'Assistant d'installation ou à distance à l'aide de Kaspersky Security Center, vous devez cocher la case **Garantir la compatibilité avec Citrix PVS**.

Compatibilité avec la technologie Omnissa App Volumes

Avant d'installer le modèle de machine virtuelle, vous devez créer le fichier %SVAgent%\Config\Custom\snapvol.cfg et y ajouter les exclusions suivantes :

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`

- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Pour en savoir plus, veuillez consulter la documentation d'Omnissa.

Installation de Light Agent

L'installation de Kaspersky Endpoint Security en mode Light Agent sur des machines virtuelles basées sur l'architecture ARM n'est pas prise en charge.

L'installation de l'application en mode Light Agent est identique à celle en mode Standard. Avant l'installation du Light Agent sur la machine virtuelle, vous devez vous assurer que l'Agent d'administration de Kaspersky Security Center est installé. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et la machine virtuelle.

Le Light Agent peut être installé sur la machine virtuelle par une des méthodes suivantes :

- À distance via Kaspersky Security Center.
- Localement à l'aide de l'Assistant d'installation de l'application.
- Localement à l'aide de la ligne de commande.

Pour installer le Light Agent, vous devez sélectionner la configuration appropriée dans les paramètres du paquet d'installation ou dans l'Assistant d'installation.

Lors de l'installation de Light Agent sur un serveur, les modules de protection avancés (Détection comportementale, Protection contre les exploits, Réparation des actions malicieuses) sont exclus de la configuration par défaut de l'application. Les paramètres par défaut de l'application offrent le niveau de protection recommandé et une utilisation optimale des ressources du serveur. Lors de l'installation de Light Agent sur un poste de travail, les modules de protection avancée sont inclus dans la configuration par défaut de l'application.

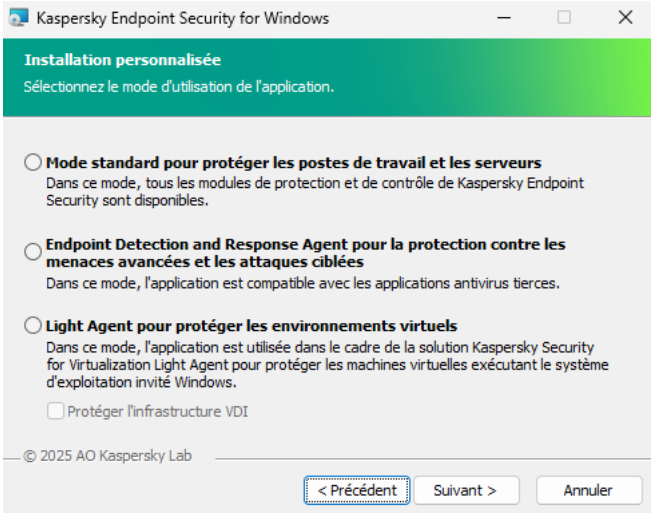
Lors de l'installation du Light Agent, il est recommandé de sélectionner des exclusions prédéfinies et des applications de confiance pour l'environnement virtuel en question. Les exclusions d'analyse et les applications de confiance prédéfinies vous permettent de configurer rapidement l'application et d'éviter les problèmes de compatibilité des environnements virtuels. Vous pouvez également configurer, dans la stratégie, les exclusions d'analyse et les applications de confiance prédéfinies après l'installation.

Comment installer le Light Agent à l'aide de l'Assistant d'installation

1. Copiez le dossier du kit de distribution sur la machine virtuelle.
2. Exécutez le fichier setup_kes.exe.

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

Configuration de Kaspersky Endpoint Security



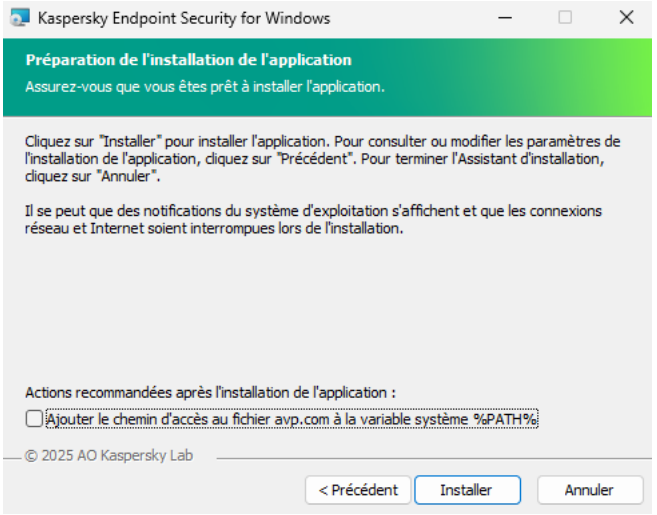
Choix de la configuration de l'application

Sélectionnez la configuration **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Modules de Kaspersky Endpoint Security

Sélectionnez les modules que vous souhaitez installer (voir la figure ci-dessous). 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



Paramètres d'installation avancés de l'application

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 d'accès au fichier avp.com à la variable système %PATH%. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% pour le confort de l'utilisation de l'interface de la ligne de commande.

Comment installer le Light Agent à l'aide 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:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   ou

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   L'option `VDI` active le mode de protection VDI (Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées. Le mode de protection VDI est désactivé par défaut.

Le Light Agent est alors installé sur la machine virtuelle avec l'ensemble de modules par défaut. Vous pouvez éditer l'ensemble de modules et définir les paramètres avancés à l'aide du fichier setup.ini. Vous pouvez également spécifier les paramètres d'installation sur la ligne de commande.

Comment installer le Light Agent à l'aide de la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.

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

3. Ouvrez les propriétés du paquet d'installation de Kaspersky Endpoint Security for Windows.

   Si nécessaire, créez un autre paquet d'installation.

4. Passez à la section **Paramètres**.

5. Sélectionnez la configuration **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

6. Sélectionnez les modules que vous souhaitez installer.

   Vous pouvez modifier la liste des modules après avoir installé l'application.

7. Configurez la zone de confiance. Sélectionnez les exclusions de l'analyse et les applications de confiance prédéfinies pour l'environnement virtuel dans lequel vous installez l'application.

   Les exclusions d'analyse et les applications de confiance prédéfinies vous permettent de configurer rapidement l'application et d'éviter les problèmes de compatibilité des environnements virtuels.

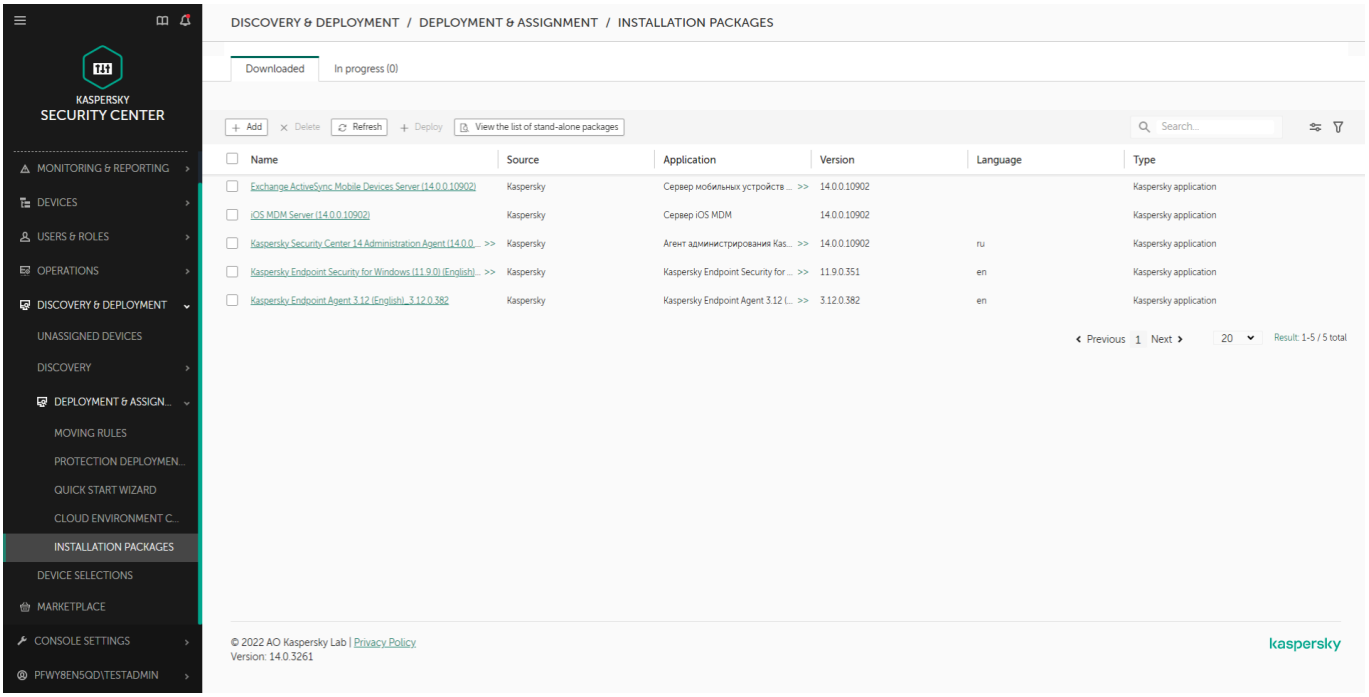
8. Enregistrez vos modifications.

9. Créez une tâche d'installation à distance. Dans les propriétés de la tâche, sélectionnez le paquet d'installation que vous avez créé.

Comment installer le Light Agent à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

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



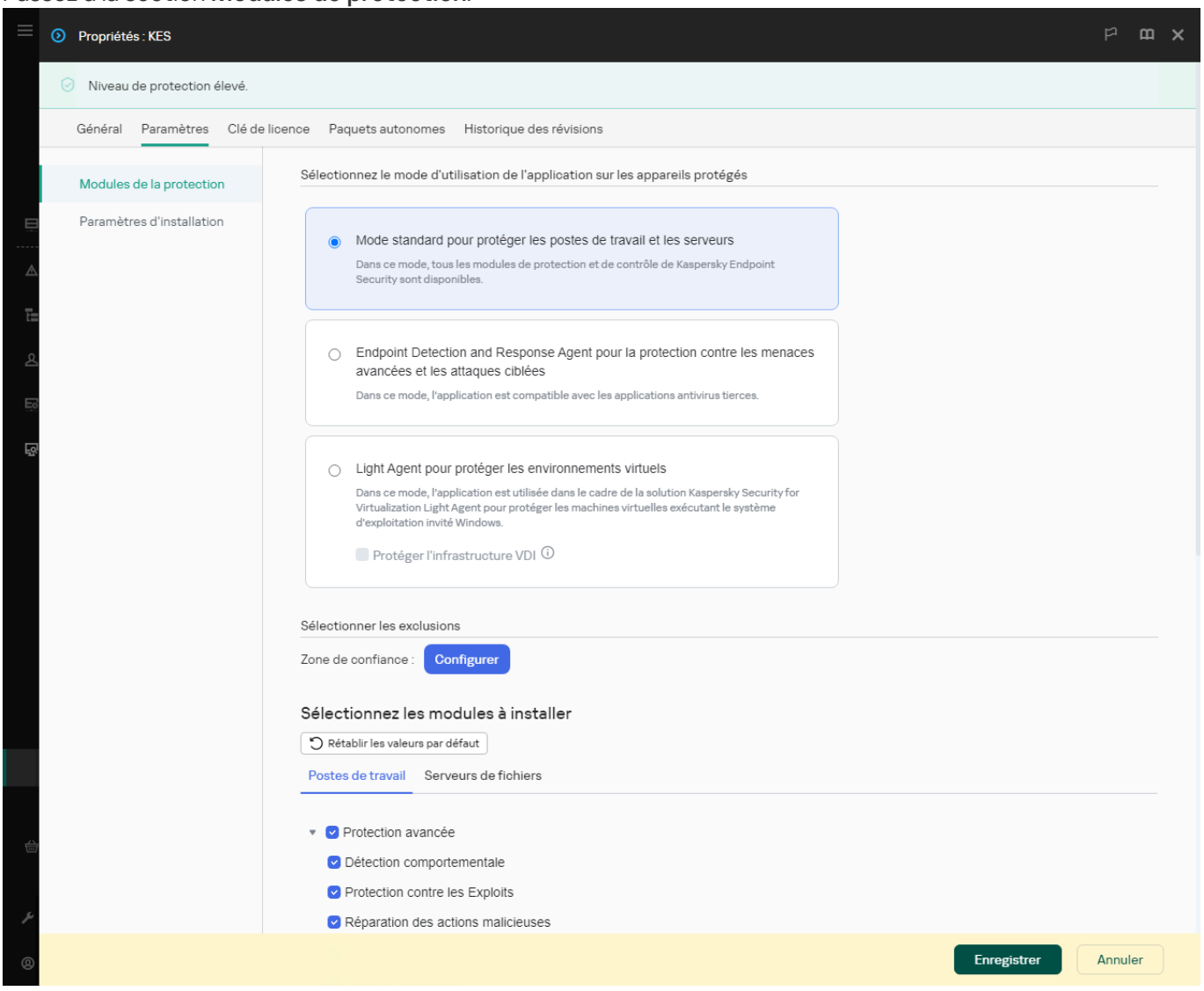
Liste des paquets d'installation

2. Ouvrez les propriétés du paquet d'installation de Kaspersky Endpoint Security for Windows.

   Si nécessaire, créez un autre paquet d'installation.

3. Sélectionnez l'onglet **Paramètres**.

4. Passez à la section **Modules de protection**.



Modules inclus dans le paquet d'installation

5. Sélectionnez la configuration **Light Agent pour protéger les environnements virtuels**. Cette configuration est destinée à l'application utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent. Le Light Agent doit être installé sur chaque machine virtuelle qui doit être protégée à l'aide de la solution. Dans cette configuration, vous ne pouvez pas utiliser les modules Chiffrement des données ni Contrôle évolutif des anomalies. Si vous installez le Light Agent sur un modèle de machine virtuelle qui sera utilisé pour créer des *machines virtuelles non persistantes*, cochez la case **Protéger l'infrastructure VDI** (VDI signifiant Virtual Desktop Infrastructure). Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Dans ce mode, le Light Agent refuse les mises à jour d'applications qui nécessitent le redémarrage de la machine virtuelle. Lors de la réception de mises à jour d'applications nécessitant un redémarrage, le Light Agent génère un événement sur la nécessité de mettre à jour le modèle des machines virtuelles protégées.

6. Sélectionnez les modules que vous souhaitez installer.

   Vous pouvez modifier la liste des modules après avoir installé l'application.

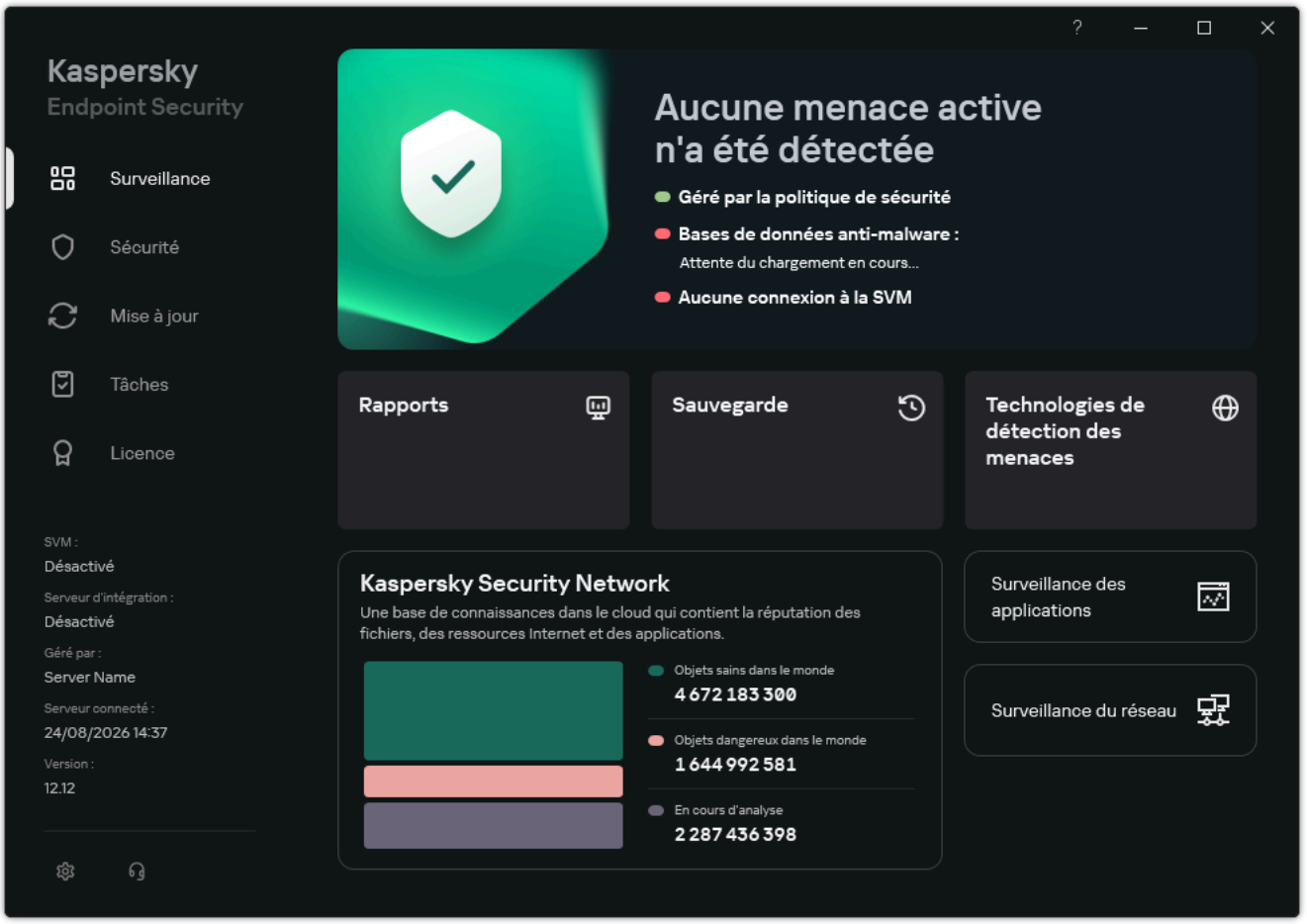
7. Configurez la zone de confiance. Sélectionnez les exclusions de l'analyse et les applications de confiance prédéfinies pour l'environnement virtuel dans lequel vous installez l'application.

   Les exclusions d'analyse et les applications de confiance prédéfinies vous permettent de configurer rapidement l'application et d'éviter les problèmes de compatibilité des environnements virtuels.

8. Enregistrez vos modifications.

9. Créez une tâche d'installation à distance. Dans les propriétés de la tâche, sélectionnez le paquet d'installation que vous avez créé.

Le Light Agent est alors installé sur la machine virtuelle. Vous pouvez utiliser l'interface de l'application, et une icône de l'application s'affiche dans la zone de notification . Il ne vous reste plus qu'à configurer la connexion du Light Agent à la SVM.



Fenêtre principale du Light Agent

À propos de la connexion Light Agent à la SVM

La solution Kaspersky Security for Virtualization Light Agent requiert une communication permanente entre le Light Agent et la SVM. Celle-ci est nécessaire pour analyser les fichiers envoyés par le Light Agent à la recherche de virus et d'autres programmes malveillants. Sans connexion SVM, le Light Agent ne peut pas envoyer de fichiers pour analyse. Si la connexion ne peut pas être établie plus de cinq minutes, l'analyse se termine sur une erreur.

La connexion d'un Light Agent à une SVM comprend les étapes suivantes :

1. Le Light Agent obtient la liste des SVM disponibles.

2. Le Light Agent détermine un Serveur de protection (SVM) disponible optimal pour la connexion en fonction de l'algorithme de sélection de la SVM.

3. Le Light Agent vérifie les paramètres de connexion complémentaires à la SVM, c'est-à-dire les tags, l'état de protection de la connexion et les fonctionnalités de l'application couvertes par la licence.

4. À propos de la connexion de Light Agent à la SVM.

Vous pouvez obtenir des informations sur l'état de connexion du Light Agent à la SVM dans Kaspersky Endpoint Security ou à l'aide de la commande de l'application. L'application génère un événement chaque fois que la connexion à la SVM du Light Agent est perdue ou établie, et envoie ces événements à Kaspersky Security Center. Si vous utilisez un Serveur d'intégration pour la recherche de SVM, vous pouvez obtenir des informations sur l'état de la SVM et le nombre de Light Agents connectés dans la Console du Serveur d'intégration. Pour en savoir plus sur la surveillance de l'état des SVM, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Recherche de SVM

Pour le Light Agent, vous pouvez choisir une des méthodes de détection des SVM :

- À l'aide du Serveur d'intégration (VIIS).

  Le *Serveur d'intégration* est le module de la solution qui permet à Kaspersky Security for Virtualization Light Agent d'interagir avec l'infrastructure virtuelle et génère une liste des SVM disponibles pour la connexion. Le Light Agent établit une connexion avec le Serveur d'intégration et obtient la liste des adresses des SVM.

  Le Serveur d'intégration est particulièrement utile dans les grandes infrastructures virtuelles, car il équilibre automatiquement la charge entre les SVM, obtient des informations sur les SVM disponibles, analyse ces informations et fournit aux Light Agents une liste des Serveurs de protection (SVM) optimaux pour la connexion.

  Pour que le Light Agent puisse obtenir une liste des SVM, il suffit d'entrer l'adresse du Serveur d'intégration.

- Utilisation d'un cluster haute disponibilité de Serveurs d'intégration.

  Le déploiement d'un cluster haute disponibilité de Serveurs d'intégration est disponible dans Kaspersky Security for Virtualization Light Agent à partir de la version 6.4. Un cluster haute disponibilité de Serveurs d'intégration assure une protection ininterrompue de l'environnement virtuel grâce au basculement des SVM et des Light Agents vers un Serveur d'intégration de sauvegarde en cas de défaillance du Serveur d'intégration principal. Un module spécial du cluster, l'*équilibreur de charge*, est responsable du basculement du serveur. Pour en savoir plus sur un cluster haute disponibilité de Serveurs d'intégration, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

  Pour que le Light Agent obtienne la liste des SVM, vous devez saisir l'adresse de l'appareil sur lequel l'équilibreur de charge est installé.

- À l'aide de la liste d'adresses de SVM.

  Si vous devez spécifier des SVM particulières auxquelles vous souhaitez que le Light Agent se connecte, vous pouvez préparer une liste manuellement.

  Il convient de lister les adresses des SVM disponibles auxquelles le Light Agent peut se connecter.

Comment configurer la détection des SVM par le Light Agent dans la Console d'administration (MMC)

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Stratégies**.

3. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

4. Dans la fenêtre de la stratégie, sélectionnez **Mode Light Agent** → **Paramètres de détection des SVM**.

5. Sélectionnez une méthode de détection des SVM.

- **Utiliser le Serveur d'intégration**. Saisissez les paramètres de connexion au Serveur d'intégration en fonction de votre infrastructure :

  - **Serveur d'intégration unique**. Saisissez les paramètres de connexion au Serveur d'intégration : adresse IPv4 ou nom de domaine pleinement qualifié (FQDN) de l'appareil.

  - **Cluster haute disponibilité de Serveurs d'intégration**. Saisissez l'adresse IP et le port de l'équilibreur de charge qui fait partie du cluster.

- **Utiliser la liste d'adresses des SVM définie manuellement**. Créez une liste des SVM auxquelles le Light Agent peut se connecter. Indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Chaque élément de la liste doit être placé sur une nouvelle ligne ou séparé de l'élément précédent par un point-virgule (`;`).

  > La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans le texte.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer la détection des SVM par le Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Mode Light Agent** → **Paramètres de détection des SVM**.

5. Sélectionnez une méthode de détection des SVM.

- **Utiliser le Serveur d'intégration**. Saisissez les paramètres de connexion au Serveur d'intégration en fonction de votre infrastructure :

  - **Serveur d'intégration unique**. Saisissez les paramètres de connexion au Serveur d'intégration : adresse IPv4 ou nom de domaine pleinement qualifié (FQDN) de l'appareil.

  - **Cluster haute disponibilité de Serveurs d'intégration**. Saisissez l'adresse IP et le port de l'équilibreur de charge qui fait partie du cluster.

- **Utiliser la liste d'adresses des SVM définie manuellement**. Créez une liste des SVM auxquelles le Light Agent peut se connecter. Indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Chaque élément de la liste doit être placé sur une nouvelle ligne ou séparé de l'élément précédent par un point-virgule (`;`).

  La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans le texte.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer la détection des SVM par le Light Agent 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, sous **Mode Light Agent**, cliquez sur le lien **Paramètres de détection des SVM**.

3. Sélectionnez une méthode de détection des SVM.

   - **Utiliser le Serveur d'intégration**. Saisissez les paramètres de connexion au Serveur d'intégration en fonction de votre infrastructure :

     - **Serveur d'intégration unique**. Saisissez les paramètres de connexion au Serveur d'intégration : adresse IPv4 ou nom de domaine pleinement qualifié (FQDN) de l'appareil.

     - **Cluster haute disponibilité de Serveurs d'intégration**. Saisissez l'adresse IP et le port de l'équilibreur de charge qui fait partie du cluster.

   - **Utiliser la liste d'adresses des SVM définie manuellement**. Créez une liste des SVM auxquelles le Light Agent peut se connecter. Indiquez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Chaque élément de la liste doit être placé sur une nouvelle ligne ou séparé de l'élément précédent par un point-virgule (`;`).

     La liste des adresses des SVM ne doit contenir que des noms de domaine complets (FQDN) auxquels est associée une adresse IP unique. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans le texte.

4. Enregistrez vos modifications.

Configuration de l'algorithme de sélection de la SVM pour le Light Agent

L'infrastructure de l'organisation peut avoir plusieurs SVM déployées auxquelles les Light Agents peuvent se connecter. Pour équilibrer la charge sur le réseau et les ressources de l'infrastructure virtuelle, vous devez répartir les Light Agents entre les SVM.

Algorithmes de sélection des SVM

Les Light Agents peuvent appliquer les algorithmes de sélection des SVM suivants pour la connexion : l'algorithme standard (par défaut) et l'algorithme étendu.

Algorithmes de sélection des SVM

Algorithme standard	Algorithme étendu
Si cet algorithme est utilisé, après l'installation et le démarrage, le Light Agent sur la machine virtuelle choisit de se connecter à la SVM qui est *locale* par rapport au Light Agent. Si aucune SVM locale adaptée à la connexion n'est trouvée, le Light Agent sélectionne une SVM à laquelle est connecté le plus petit nombre de Light Agents, quelle que soit la position de la SVM dans l'infrastructure virtuelle. Le caractère local de la SVM par rapport au Light Agent n'est pas déterminé si le mode de protection des grandes infrastructures est activé pour le Serveur de protection sur cette SVM. Dans ce cas, il est recommandé d'utiliser l'algorithme étendu de sélection des SVM et de sélectionner le Serveur d'intégration comme méthode de détection des SVM. La question de savoir si une SVM est considérée comme locale pour un Light Agent dépend du type d'infrastructure virtuelle.	Si cet algorithme est appliqué, vous pouvez spécifier les paramètres suivants de sélection des SVM : • prendre en compte ou ignorer l'emplacement de la SVM dans l'infrastructure lors de la sélection d'une SVM pour la connexion ; • si l'emplacement de la SVM est pris en compte, la méthode pour déterminer la localité de la SVM par rapport à l'Agent Light Si les Light Agents ignorent l'emplacement de la SVM dans l'infrastructure, alors les Light Agents pourront se connecter à n'importe quelle SVM disponible pour la connexion. Si les Light Agents doivent prendre en compte l'emplacement de la SVM dans l'infrastructure, vous devez sélectionner le type d'emplacement de la SVM qui sera pris en compte pour déterminer la localité de la SVM par rapport au Light Agent. La question de savoir si une SVM est considérée comme locale pour un Light Agent dépend du type d'infrastructure virtuelle. Si les Light Agents prennent en compte l'emplacement de la SVM dans l'infrastructure lors de la sélection d'une SVM pour la connexion, alors les Light Agents ne peuvent se connecter qu'à la SVM locale. Par exemple, si vous désignez un cluster hyperviseur en tant que type d'emplacement des SVM, alors toutes les SVM déployées sur ce cluster hyperviseur seront considérés comme locales pour le Light Agent et le Light Agent pourra se connecter à une seule de ces SVM. En l'absence de SVM disponibles pour une connexion dans le cluster dans lequel fonctionne le Light Agent, le Light Agent ne se connecte pas à la SVM. Lors de la sélection des SVM, les Light Agents tiennent aussi compte du nombre de Light Agents connectés pour garantir une répartition équitable des Light Agents entre les SVM disponibles pour la connexion. Si un algorithme étendu de sélection des SVM est utilisé pour un Light Agent et que la liste d'adresses des SVM est sélectionnée comme méthode de détection des SVM et que le mode de protection des grandes infrastructures est activé sur la SVM, la connexion du Light Agent à cette SVM n'est possible que si le Light Agent ignore l'emplacement de la SVM.
Basis Dynamix Enterprise	
Dans une infrastructure virtuelle basée sur Basis Dynamix Enterprise, toute SVM déployée sur le même nœud que la machine virtuelle sur laquelle Light Agent est installé est considérée comme une SVM locale pour Light Agent.	Dans une infrastructure virtuelle basée sur Basis Dynamix Enterprise, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM est déployée sur le même nœud que celui où se trouve la machine virtuelle dotée de Light Agent. • Une SVM est déployée dans la même zone que celui où se trouve la machine virtuelle dotée de Light Agent. • Une SVM est déployée dans le même centre de données que la machine virtuelle dotée de Light Agent.

Algorithme standard	Algorithme étendu
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer et Basis Dynamix Standard	
Dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, toute SVM déployée sur le même hyperviseur que la machine virtuelle sur laquelle Light Agent est installé est considérée comme une SVM locale pour Light Agent.	Dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM est déployée sur le même hyperviseur que la machine virtuelle dotée de Light Agent. • Une SVM est déployée sur le même cluster hyperviseur que la machine virtuelle dotée de Light Agent.Agent. • Une SVM est déployée dans le même centre de données que la machine virtuelle dotée de Light Agent.
SVM OpenStack et VK Private Cloud	
Dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud, vous pouvez spécifier comment la localité de la SVM par rapport au Light Agent est déterminée à l'aide du paramètre `StandardAlgorithmSvmLocality` dans la section `HypervisorSpecificSettings:Openstack` dans le fichier de configuration appsettings.json du Serveur d'intégration. Selon la version du Serveur d'intégration, le fichier se trouve dans le chemin suivant : • /var/opt/kaspersky/viis/common/ : fichier du Serveur d'intégration sous Linux. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ : fichier du Serveur d'intégration sous Windows. Le paramètre `StandardAlgorithmSvmLocality` peut prendre les valeurs suivantes : • `ServerGroup` : si cette valeur est définie, on considère comme SVM locale pour Light Agent toute SVM qui se trouve dans le même groupe de serveurs que la machine virtuelle dotée de Light Agent. Cette valeur est utilisée par défaut. • `Project` : si cette valeur est définie, on considère comme SVM locale pour Light Agent la SVM déployée dans le cadre du même projet OpenStack que celui de la machine virtuelle avec Light Agent. • `AvailabilityZone` : si cette valeur est définie, on considère comme SVM locale pour Light Agent la SVM qui se trouve dans la même zone de disponibilité que la machine virtuelle dotée de Light Agent.	Dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud, une SVM peut être considérée comme locale par rapport au Light Agent dans l'un des cas suivants : • Une SVM se trouve dans le même groupe de serveurs que la machine virtuelle dotée du Light Agent. • Une SVM est déployée dans le même projet OpenStack que la machine virtuelle dotée de Light Agent. • Une SVM se trouve dans la même zone de disponibilité que la machine virtuelle dotée de Light Agent.

En plus des algorithmes de connexion à la SVM, vous pouvez réguler la connexion des Light Agents aux SVM à l'aide des tags.

Configuration de l'algorithme de sélection des SVM

Comment configurer l'algorithme de sélection des SVM pour le Light Agent dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Mode Light Agent** → **Algorithme de sélection des SVM**.

4. Sélectionnez l'algorithme :

- **Utiliser l'algorithme standard de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le même hyperviseur.

- **Utiliser l'algorithme étendu de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le type de chemin d'accès à la SVM sélectionné (par défaut, **Hyperviseur**).

5. Si nécessaire, sélectionnez les chemin d'accès à la SVM pour l'algorithme étendu de sélection de la SVM :

- **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - La SVM se trouve dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve sur le même nœud que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  S'il n'y a aucune SVM disponible pour la connexion sur le même hyperviseur ou dans le même groupe de serveurs où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Cluster**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM sont déployées dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans la même zone que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Bais Dynamix Enterprise).

  S'il n'y a aucune SVM disponible à laquelle se connecter dans le même cluster d'hyperviseur ou dans le même projet OpenStack où se trouve la machine virtuelle Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Centre de données**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM se trouvent dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  En l'absence de SVM disponible pour la connexion dans le même centre de données ou la même zone de disponibilité que la machine virtuelle avec le Light Agent, ce dernier ne se connecte pas à la SVM.

- **Ignorer**. Le Light Agent ignore le chemin d'accès à la SVM pour se connecter au Serveur de protection. Le Light Agent prend en compte d'autres critères, comme les tags, le nombre de Light Agents connectés à une SVM, etc.

6. Enregistrez vos modifications.

Comment configurer l'algorithme de sélection des SVM pour le Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Mode Light Agent** → **Algorithme de sélection des SVM**.

5. Sélectionnez l'algorithme :

   - **Utiliser l'algorithme standard de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le même hyperviseur.

   - **Utiliser l'algorithme étendu de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le type de chemin d'accès à la SVM sélectionné (par défaut, **Hyperviseur**).

6. Si nécessaire, sélectionnez les chemin d'accès à la SVM pour l'algorithme étendu de sélection de la SVM :

- **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - La SVM se trouve dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve sur le même nœud que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  S'il n'y a aucune SVM disponible pour la connexion sur le même hyperviseur ou dans le même groupe de serveurs où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Cluster**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM sont déployées dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans la même zone que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Bais Dynamix Enterprise).

  S'il n'y a aucune SVM disponible à laquelle se connecter dans le même cluster d'hyperviseur ou dans le même projet OpenStack où se trouve la machine virtuelle Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Centre de données**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM se trouvent dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

En l'absence de SVM disponible pour la connexion dans le même centre de données ou la même zone de disponibilité que la machine virtuelle avec le Light Agent, ce dernier ne se connecte pas à la SVM.

- **Ignorer**. Le Light Agent ignore le chemin d'accès à la SVM pour se connecter au Serveur de protection. Le Light Agent prend en compte d'autres critères, comme les tags, le nombre de Light Agents connectés à une SVM, etc.

7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer l'algorithme de sélection des SVM pour le Light Agent dans l'interface d'application

1. Dans la fenêtre principale de l'application, cliquez sur le bouton .

2. Dans la fenêtre des paramètres de l'application, sous **Mode Light Agent**, cliquez sur le lien **Paramètres de détection des SVM**.

3. Sélectionnez l'algorithme :

   - **Utiliser l'algorithme standard de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le même hyperviseur.

   - **Utiliser l'algorithme étendu de sélection des SVM**. Le Light Agent sélectionne les SVM déployées dans le type de chemin d'accès à la SVM sélectionné (par défaut, **Hyperviseur**).

4. Si nécessaire, sélectionnez les chemin d'accès à la SVM pour l'algorithme étendu de sélection de la SVM :

   - **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

     - Les SVM sont déployées sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

     - La SVM se trouve dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

     - La SVM se trouve sur le même nœud que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

     S'il n'y a aucune SVM disponible pour la connexion sur le même hyperviseur ou dans le même groupe de serveurs où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.

   - **Cluster**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

     - Les SVM sont déployées dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

     - Les SVM sont déployées dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

     - La SVM se trouve dans la même zone que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Bais Dynamix Enterprise).

S'il n'y a aucune SVM disponible à laquelle se connecter dans le même cluster d'hyperviseur ou dans le même projet OpenStack où se trouve la machine virtuelle Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Centre de données**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :

  - Les SVM sont déployées dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle basée sur Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - Les SVM se trouvent dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack ou VK Private Cloud).

  - La SVM se trouve dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans l'infrastructure virtuelle Basis Dynamix Enterprise).

  En l'absence de SVM disponible pour la connexion dans le même centre de données ou la même zone de disponibilité que la machine virtuelle avec le Light Agent, ce dernier ne se connecte pas à la SVM.

- **Ignorer**. Le Light Agent ignore le chemin d'accès à la SVM pour se connecter au Serveur de protection. Le Light Agent prend en compte d'autres critères, comme les tags, le nombre de Light Agents connectés à une SVM, etc.

5. Enregistrez vos modifications.

Répartition des connexions des Light Agents aux SVM (tags)

Plusieurs Light Agents peuvent se connecter à une SVM. Pour équilibrer les connexions du Light Agent, vous pouvez spécifier une liste distincte de SVM. Si vous utilisez un Serveur d'intégration pour la découverte des SVM, vous pouvez utiliser les *tags* pour équilibrer les connexions du Light Agent aux SVM. Autrement dit, pour un Light Agent, vous pouvez désigner une liste de SVM auxquelles se connecter à l'aide d'un tag. Pour ce faire, il convient d'attribuer un tag au Light Agent et de spécifier ce tag dans les paramètres de la SVM. Pour en savoir plus sur la définition des tags dans les paramètres de la SVM, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Exemple : la solution Kaspersky Endpoint Detection and Response Optimum est déployée dans votre infrastructure pour les hôtes de machines virtuelles désignés. Dans ce cas, vous pouvez attribuer le tag `[EDROptimum]` au Light Agent pour le connecter aux SVM auxquelles la clé de licence EDR Optimum (module complémentaire EDR Optimum) a été ajoutée. Par conséquent, vous pouvez utiliser la fonctionnalité EDR Optimum sur la machine virtuelle avec le Light Agent. Lors de la connexion du Light Agent à une SVM sans clé de licence EDR Optimum, la fonctionnalité de Kaspersky Endpoint Detection and Response Optimum n'est pas disponible.

Comment attribuer un tag de connexion SVM à un Light Agent dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Mode Light Agent** → **Tag de connexion à la SVM**.

4. Cochez la case **Utiliser le tag de connexion** et saisissez un tag de connexion à la SVM.

   En guise de tag, vous pouvez saisir un texte de 255 caractères maximum. Vous pouvez utiliser n'importe quel caractère à l'exception du caractère `;`.

5. Enregistrez vos modifications.

Comment attribuer un tag de connexion SVM à un Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Passez à la section **Mode Light Agent** → **Tag de connexion à la SVM**.

5. Cochez la case **Utiliser le tag de connexion** et saisissez un tag de connexion à la SVM.

   En guise de tag, vous pouvez saisir un texte de 255 caractères maximum. Vous pouvez utiliser n'importe quel caractère à l'exception du caractère `;`.

6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment attribuer un tag de connexion SVM à un Light Agent 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, sous **Mode Light Agent**, cliquez sur le lien **Tag de connexion à la SVM**.

3. Cochez la case **Utiliser le tag de connexion** et saisissez un tag de connexion à la SVM.

   En guise de tag, vous pouvez saisir un texte de 255 caractères maximum. Vous pouvez utiliser n'importe quel caractère à l'exception du caractère `;`.

4. Enregistrez vos modifications.

Protection de la connexion entre Light Agent et une SVM

Vous pouvez configurer le chiffrement de la connexion entre les Light Agents et le Serveur de protection. Pour ce faire, vous devez activer le chiffrement du canal de données entre le Light Agent et le Serveur de protection dans les paramètres du Serveur de protection sur la SVM ainsi que dans les paramètres du Light Agent.

Un Light Agent pour lequel la protection des connexions est activée peut se connecter uniquement aux SVM pour lesquelles le chiffrement du canal de données entre le Light Agent et le Serveur de protection est activé. Un Light Agent pour lequel la protection des connexions est désactivée peut se connecter uniquement aux SVM pour lesquelles le chiffrement du canal est désactivé ou pour lesquelles une connexion non sécurisée entre le Serveur de protection et le Light Agent est autorisée.

Pour en savoir plus sur la configuration de la protection des connexions sur le Serveur de protection, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

La protection de la connexion à l'aide du chiffrement peut réduire les performances de Kaspersky Security for Virtualization Light Agent.

Comment configurer la protection des connexions dans un Light Agent dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Mode Light Agent** → **Protection de la connexion**.
4. Cochez la case **Chiffrer le canal de données entre le Light Agent et le Serveur de protection**.
5. Enregistrez vos modifications.

Comment configurer la protection des connexions dans un Light Agent dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Mode Light Agent** → **Protection de la connexion**.
5. Cochez la case **Chiffrer le canal de données entre le Light Agent et le Serveur de protection**.
6. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment configurer la protection des connexions dans un Light Agent 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, sous **Mode Light Agent**, cliquez sur le lien **Protection de la connexion**.
3. Cochez la case **Chiffrer le canal de données entre le Light Agent et le Serveur de protection**.
4. Enregistrez vos modifications.

Activation du Light Agent

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger des environnements virtuels, il n'est pas nécessaire d'activer l'application séparément. Pour activer l'application, vous devez ajouter une clé de licence à la SVM. Vous pouvez ajouter une clé de licence à la SVM à l'aide de la tâche spéciale dans Kaspersky Security Center Console. Vous ne pouvez pas gérer les clés de licence dans l'interface du Light Agent, mais vous pouvez consulter des informations sur la licence (voir la figure ci-dessous). Vous pouvez également consulter les informations de licence du Light Agent sur la ligne de commande (voir les instructions ci-dessous). Le Light Agent obtient ces informations depuis la SVM. Pour en savoir plus sur l'activation de la solution et la gestion des clés de licence, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Pour consulter les informations de licence du Light Agent, procédez comme suit :

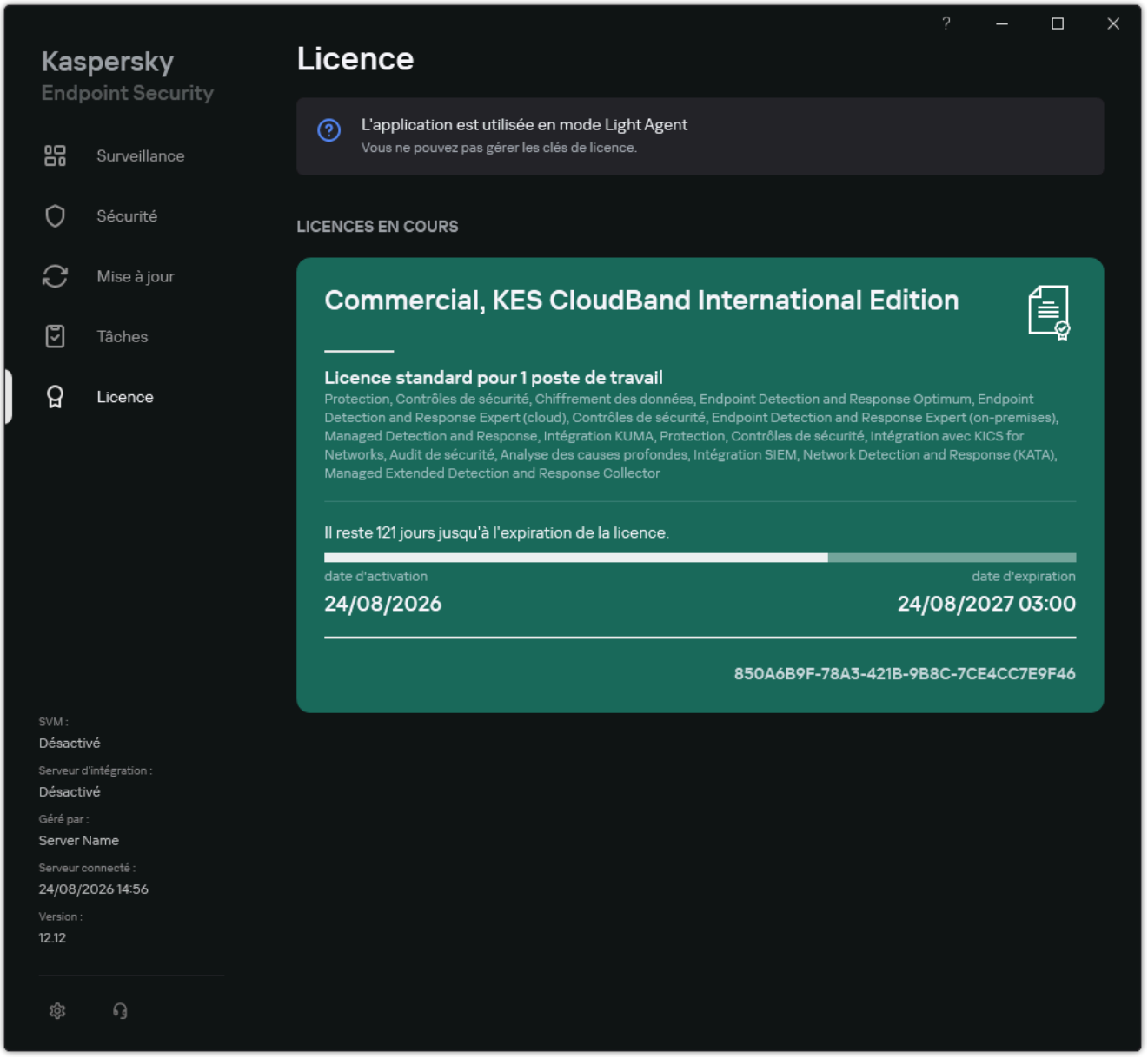
1. Lancez l'interpréteur de ligne de commande (cmd) au nom de l'administrateur.

2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

3. Exécutez la commande:

   ```
   avp.com LICENSE /CHECK
   ```

   Par conséquent, Kaspersky Endpoint Security affiche les informations sur la licence suivantes : adresse de la SVM à laquelle le Light Agent est connecté, nombre de jours avant l'expiration de la licence, et autres informations. Si vous rencontrez des problèmes lors de l'activation du Light Agent, veuillez consulter la base des connaissances du Support Technique.



Fenêtre Licence

Guide de migration de KSVLA Light Agent vers KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent inclut le module Light Agent for Windows 5.2 (ci-après également « KSVLA Light Agent »). Dans Kaspersky Security for Virtualization Light Agent 6.2, Kaspersky Endpoint Security en mode Light Agent est utilisé comme module Light Agent. Pour mettre à jour la solution vers la version 6.2, vous devez migrer de KSVLA Light Agent 5.2 vers Kaspersky Endpoint Security en mode Light Agent (également appelé « KES Light Agent » ci-dessous). Pour en savoir plus sur la mise à jour de la version de la solution Kaspersky Security for Virtualization Light Agent , consultez l'aide de Kaspersky Security for Virtualization Light Agent .

Configuration logicielle

Avant de commencer la migration de KSVLA Light Agent vers KES Light Agent, assurez-vous que votre machine virtuelle répond à la configuration matérielle et logicielle requise par Kaspersky Endpoint Security for Windows. Les listes des versions du système d'exploitation prises en charge sont différentes pour KES et KSWS. Par exemple, KES ne prend pas en charge les serveurs fonctionnant sous Windows Server 2003.

Configuration logicielle minimale requise pour la migration de KSVLA Light Agent vers KES Light Agent :

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (y compris les modules Serveur de protection et Serveur d'intégration).
- Kaspersky Security Center 14.2

  Si une version antérieure de Kaspersky Security Center est installée, mettez-la à jour vers la version 14.2 ou une version ultérieure. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet de migrer les stratégies vers un profil plutôt que vers une stratégie. Dans cette version de Kaspersky Security Center, l'Assistant de conversion de masse des stratégies et des tâches vous permet également de migrer un plus large éventail de paramètres de stratégie.

Étapes de migration

La migration de KSVLA Light Agent vers KES Light Agent est exécutée de manière semi-automatique. Cette démarche est nécessaire en raison des architectures différentes des applications.

Migrez de KSVLA Light Agent vers KES Light Agent dans l'ordre suivant :

1. **Migrez les tâches et les stratégies de KSVLA Light Agent**

   Pour migrer les paramètres de stratégie, vous devez exécuter l'Assistant de conversion de masse des stratégies et des tâches (l'Assistant de migration). Après la migration des paramètres de stratégie, vous devez configurer manuellement les paramètres que l'Assistant de migration ne peut pas migrer automatiquement (par exemple, les paramètres de mise à jour de la base de données). Après la migration, il est également recommandé de vérifier si l'Assistant de migration a correctement migré tous les paramètres.

   Si la protection par mot de passe est activée pour restreindre l'accès à KSVLA Light Agent, vous devez désactiver la protection par mot de passe dans la stratégie de KSVLA Light Agent avant d'installer KES Light Agent. Vous ne pouvez pas saisir le mot de passe de désinstallation dans les paramètres du paquet d'installation de KES Light Agent. Une fois que vous avez terminé l'installation de KES Light Agent par-dessus KSVLA Light Agent, vous devez activer la protection par mot de passe dans la stratégie de KES.

2. **Installation de Kaspersky Endpoint Security en mode Light Agent**

   Vous pouvez installer KES Light Agent des manières suivantes :

   - Installation de KES Light Agent après la désinstallation de KSVLA Light Agent (recommandé)
   - Installation de KES Light Agent par-dessus KSVLA Light Agent

3. **Confirmer que l'application fonctionne correctement après la migration**

   Une fois que vous avez procédé à la migration de KSVLA Light Agent vers KES Light Agent, assurez-vous que l'application fonctionne correctement. Activez la stratégie convertie. Vérifiez l'état de la machine virtuelle dans la console de Kaspersky Security Center (l'état devrait être *OK*). Assurez-vous qu'aucune erreur n'est rapportée pour l'application, et vérifiez également l'heure de la dernière connexion à la SVM et l'état de protection de la machine virtuelle. Vous n'avez pas besoin d'activer le Light Agent, car la clé de licence est ajoutée à la SVM.

Installation de KES Light Agent à la place de KSVLA Light Agent

Vous pouvez installer KES Light Agent des manières suivantes :

- Installation de KES Light Agent après la désinstallation de KSVLA Light Agent (recommandé)
- Installation de KES Light Agent par-dessus KSVLA Light Agent

Suppression de KSVLA Light Agent

Vous pouvez supprimer l'application à distance à l'aide de la tâche *Installation à distance d'une application*, localement sur la machine virtuelle ou dans le modèle de machine virtuelle. Après la suppression de KSVLA Light Agent, vous devrez peut-être redémarrer la machine virtuelle.

Après la suppression de KSVLA Light Agent, installez KES Light Agent par tout moyen approprié.

Installation de Kaspersky Endpoint Security

> Si la protection par mot de passe est activée pour restreindre l'accès à KSVLA Light Agent, vous devez désactiver la protection par mot de passe dans la stratégie de KSVLA Light Agent avant d'installer KES Light Agent. Vous ne pouvez pas saisir le mot de passe de désinstallation dans les paramètres du paquet d'installation de KES Light Agent. Une fois que vous avez terminé l'installation de KES Light Agent par-dessus KSVLA Light Agent, vous devez activer la protection par mot de passe dans la stratégie de KES.

Lors de l'installation de Kaspersky Endpoint Security, vous devez sélectionner le mode **Light Agent pour protéger les environnements virtuels**. Avant d'installer KES Light Agent sur une machine virtuelle, le programme d'installation détecte KSVLA Light Agent comme un logiciel incompatible et le supprime. La migration de la configuration de KSVLA Light Agent n'est pas prise en charge. Autrement dit, lorsque vous installez KES Light Agent, l'ensemble de modules à installer est déterminé par votre sélection dans les propriétés du paquet d'installation ou dans l'Assistant d'installation. Après la suppression de KSVLA Light Agent, vous devez redémarrer la machine virtuelle.

Les paramètres et les tâches de KSVLA Light Agent ne sont pas migrés lorsque vous installez KES Light Agent. Pour procéder à la migration des paramètres et des tâches, exécutez l'Assistant de conversion de masse des stratégies et des tâches.

Vous pouvez vérifier la liste des modules installés dans la section **Sécurité** de l'interface de l'application, à l'aide de la commande `status` ou dans la console de Kaspersky Security Center dans les propriétés de l'ordinateur. Vous pouvez modifier l'ensemble des modules après l'installation en utilisant les *Modification de la sélection des modules de l'application*.

Correspondance des modules KSVLA Light Agent et KES Light Agent

Les ensembles de modules de KSVLA Light Agent et de KES Light Agent sont pratiquement les mêmes. KES Light Agent comporte plus de paramètres que KSVLA Light Agent. Après la migration, les nouveaux paramètres présentent des valeurs par défaut.

Correspondance des modules KSVLA Light Agent et KES Light Agent

Light Agent 5.2	KES Light Agent
Noyau de l'analyse	Noyau de l'application
Antivirus fichiers	Protection contre les fichiers malicieux
Antivirus Courrier	Protection contre les menaces par emails
Antivirus Internet	Protection contre les menaces Internet
Pare-feu	Pare-feu
Prévention des intrusions	Protection contre les menaces réseau
Contrôle des privilèges des applications	Prévention des intrusions
Contrôle du lancement des applications	Contrôle des applications
Contrôle Internet	Contrôle Internet
Contrôle des appareils	Contrôle des appareils
Surveillance du système	Dans Kaspersky Endpoint Security, ce module comprend les éléments suivants : • Protection contre les Exploits • Détection comportementale • Réparation des actions malicieuses
Contrôle de l'intégrité du système	Contrôle de l'intégrité du système
Intégration avec Kaspersky Endpoint Agent	*(non pris en charge)* À partir de Kaspersky Endpoint Security for Windows 11.9.0, le paquet de distribution de Kaspersky Endpoint Agent ne fait plus partie du kit de distribution.
Protection AMSI	Protection AMSI

Migration des tâches et des stratégies de KSVLA Light Agent

Vous pouvez migrer les paramètres des stratégies et des tâches de KSVLA Light Agent à l'aide de l'Assistant de conversion de masse des stratégies et des tâches (ci-après également « l'Assistant de migration »).

L'Assistant de migration pour KSVLA Light Agent est disponible uniquement dans la Console d'administration (MMC). Les paramètres de stratégie et de tâche ne peuvent pas être migrés dans Web Console et Cloud Console.

Il convient de tenir compte des considérations particulières suivantes lors de la migration des stratégies et des tâches

- Une nouvelle stratégie porte le nom *<Policy> (converted)*.
- La nouvelle stratégie porte l'état *Stratégie inactive*.
- L'interdiction de modifier les paramètres (le « cadenas ») n'est pas migrée. L'Assistant de migration définit les valeurs par défaut.
- Les profils de stratégie ne sont pas migrés. Vous devez ajouter manuellement les profils de stratégie.
- Amélioration de la gestion des zones de confiance. Dans KSVLA Light Agent, vous pouviez ajouter des exclusions prédéfinies uniquement lors de la création d'une stratégie. Ensuite, vous pouvez configurer les exclusions prédéfinies ajoutées auparavant dans les propriétés de la stratégie ou ajouter des exclusions manuellement. Vous ne pouvez pas ajouter d'exclusions prédéfinies dans les propriétés de la stratégie. Dans KES Light Agent, les exclusions prédéfinies sont disponibles lors de la création de la stratégie et dans les propriétés de la stratégie créée. Vous pouvez également sélectionner des exclusions prédéfinies dans le paquet d'installation.
- La configuration de l'interface utilisateur de l'application dans Kaspersky Endpoint Security a été déplacée du programme d'installation vers la stratégie. Si vous devez, par exemple, masquer l'interface utilisateur de l'application, gérez les paramètres de la stratégie.
- Les ensembles de fonctionnalités de configuration du Contrôle d'accès basé sur les droits (RBAC) sont différents dans Kaspersky Endpoint Security et dans KSVLA Light Agent. Vous devez entièrement configurer les privilèges d'accès des utilisateurs dans les zones fonctionnelles.

Comment utiliser l'Assistant de conversion de masse des stratégies et des tâches pour migrer les paramètres des stratégies KSVLA Light Agent

1. Dans la Console d'administration, sélectionnez le Serveur d'administration et faites un clic droit pour ouvrir le menu contextuel.
2. Choisissez **Toutes les tâches** → **Assistant de conversion de masse des stratégies et des tâches**.

   Ensuite, l'Assistant de conversion de masse des stratégies et des tâches se lance. Suivez les instructions de l'Assistant.

Étape 1. Sélectionnez l'application dont il faut convertir les stratégies et les tâches

À cette étape, vous devez sélectionner Kaspersky Endpoint Security for Windows. Passez à l'étape suivante.

Étape 2. Conversion des stratégies

Sélectionnez la stratégie Kaspersky Security for Virtualization 5.2 Light Agent for Windows que vous souhaitez convertir. Passez à l'étape suivante.

L'Assistant de migration commencera alors à convertir les stratégies. Lors de la conversion, l'Assistant de migration vous invite à accepter les conditions de la Déclaration KSN. Une nouvelle stratégie porte le nom *<Policy> (converted)*.

Étape 3. Conversion des tâches

L'Assistant de migration crée de nouvelles tâches pour Kaspersky Endpoint Security for Windows. Dans la liste de tâches, sélectionnez les tâches de KSVLA Light Agent que vous souhaitez créer pour Kaspersky Endpoint Security. Les nouvelles tâches seront nommées *<Nom de la tâche> (convertie)*. Passez à l'étape suivante.

Étape 4. Fin de l'Assistant

Quittez l'Assistant.

Après la migration d'une stratégie, il faut ouvrir les propriétés de la stratégie, vérifier ses paramètres et enregistrer la stratégie. Si vous ne suivez pas ces étapes, KES Light Agent risque d'ignorer la stratégie convertie.

Portez une attention particulière à la migration des paramètres de connexion SVM des Light Agents, des listes d'exclusion, des applications de confiance, des adresses Web de confiance et des règles du Contrôle des applications.

Migration de la configuration [KSVLA Light Agent+KEA] vers la configuration [KES Light Agent+agent intégré]

Pour prendre en charge l'utilisation de Kaspersky Endpoint Security for Windows dans le cadre de EDR (KATA), EDR Optimum et Kaspersky Sandbox, un agent intégré a été ajouté à l'application. Vous n'avez plus besoin d'une application Kaspersky Endpoint Agent distincte pour utiliser ces solutions.

Lors de la migration de KSVLA Light Agent vers KES Light Agent, les solutions EDR (KATA), EDR Optimum et Kaspersky Sandbox continuent de fonctionner avec les agents intégrés de Kaspersky Endpoint Security. De plus, Kaspersky Endpoint Agent sera supprimé de l'ordinateur.

Avant la migration de KSVLA Light Agent vers KES Light Agent, vous devez mettre à jour tous les modules de Kaspersky Security for Virtualization vers la version 6.2, y compris le Serveur de protection et le Serveur d'intégration. Pour en savoir plus sur la mise à jour de la version de la solution Kaspersky Security for Virtualization Light Agent , consultez l'aide de Kaspersky Security for Virtualization Light Agent .

La migration de la configuration de [KSVLA Light Agent+KEA] vers [KES Light Agent+agent intégré] comprend les étapes suivantes :

1. **Migration de la stratégie et des tâches**

La migration des stratégies et des tâches [KSVLA Light Agent+KEA] vers [KES Light Agent+agent intégré] implique les étapes suivantes :

1. Migration des stratégies et des tâches de KSVLA Light Agent vers KES Light Agent à l'aide de l'Assistant de conversion en masse des stratégies et des tâches (uniquement disponible dans la Console d'administration (MMC)).

   Une nouvelle stratégie est alors créée sous le nom *<Stratégie> (converti)*. De nouvelles tâches KES sont également créées avec des noms *<Nom de la tâche> (converti)*.

2. Migration des stratégies et des tâches de KEA vers KES à l'aide de l'Assistant de migration à partir de Kaspersky Endpoint Agent (uniquement disponible dans Web Console et Cloud Console).

   En conséquence, une nouvelle stratégie est créée portant le nom *<nom de la stratégie Kaspersky Endpoint Security> et <nom de la stratégie Kaspersky Endpoint Agent>*. De nouvelles tâches et tâches KES sont également créées.

2 Migration de KSVLA Light Agent vers KES Light Agent

La migration de KSVLA Light Agent vers KES Light Agent implique l'installation de KES Light Agent au lieu de KSVLA Light Agent.

Les administrateurs activent généralement la protection par mot de passe pour restreindre l'accès à KSVLA Light Agent et à KEA. Vous pouvez saisir le mot de passe de désinstallation de KEA uniquement dans les propriétés de la tâche *Installation à distance d'une application*. Pour la migration, vous devez désactiver la Protection par mot de passe pour KSVLA Light Agent.

Pour effectuer la migration, vous devez sélectionner les modules nécessaires pour prendre en charge les solutions Detection and Response dans le cadre de Kaspersky Endpoint Security. Après que l'application a été installée, Kaspersky Endpoint Security passe à l'utilisation de l'agent intégré et supprime Kaspersky Endpoint Agent.

3 Fonctionnalités des licences

Si l'application est utilisée en mode Light Agent, il n'est pas nécessaire d'activer l'application. Pour activer l'application, vous devez ajouter une clé de licence à la SVM. Vous devez également ajouter la clé de licence pour activer les fonctionnalités supplémentaires (par exemple, EDR Optimum) dans la SVM. Autrement dit, dans le cadre de la migration, l'octroi de la licence des fonctionnalités est exécuté automatiquement.

4 Vérification de l'état de santé de Kaspersky Endpoint Detection and Response Optimum et de Kaspersky Sandbox

Si après la mise à jour, l'ordinateur présente l'état *Critique* dans la console de Kaspersky Security Center, procédez comme suit :

- Assurez-vous que la version 13.2 de l'Agent d'administration ou une version ultérieure est installée sur l'ordinateur.
- Vérifiez l'état de fonctionnement de l'agent intégré en consultant le *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non installé*, installez-le à l'aide de la tâche *Modification de la sélection des modules de l'application*.
- Assurez-vous d'accepter la Déclaration de Kaspersky Security Network dans la nouvelle stratégie de Kaspersky Endpoint Security for Windows.

- Assurez-vous que la fonctionnalité EDR Optimum est activée à l'aide de l'icône *Rapport sur l'état des modules de l'application*. Si un module présente l'état *Non compris dans la licence*, assurez-vous que la fonctionnalité de distribution automatique des clés de licence de EDR Optimum est activée.

- Vérifiez l'état de la connexion de la machine virtuelle à la SVM. Vous pouvez obtenir des informations sur l'état de connexion du Light Agent à la SVM dans Kaspersky Endpoint Security ou à l'aide de la commande de l'application.

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 `avp.com HELP`. Pour obtenir de l'aide sur la syntaxe d'une commande en particulier, saisissez `avp.com HELP <command>`.

Les caractères spéciaux doivent être escamotés dans la commande. Pour escamoter les caractères `&`, `|`, `(`, `)`, `<`, `>` et `^`, utilisez le caractère `^` (par exemple, pour utiliser le caractère `&`, saisissez `^&`). Pour escamoter le caractère `%`, saisissez `%%`.

Les valeurs `yes`, `on`, `enable`, `enabled` et `true` peuvent être utilisées à la place de la valeur `1`. Les valeurs `no`, `off`, `disable`, `disabled` et `false` peuvent être utilisées à la place de la valeur `0`.

Setup. Installation de l'application

L'installation de l'application depuis la ligne de commande comprend les étapes suivantes :

1. **Choix du paquet de distribution**

   Kaspersky fournit des paquets de distribution pour différentes localisations, compatibles avec différentes architectures de processeur et comprenant divers modules de chiffrement.

   La distribution contient les paquets de distribution suivants :

   - **AES256**

     Ce paquet de distribution est conçu pour être installé sur des ordinateurs avec une architecture x86/x64. Ce paquet de distribution contient des outils cryptographiques qui mettent en œuvre l'algorithme de chiffrement AES (Advanced Encryption Standard) avec une longueur de clé effective de 256 bits.

   - **AES56**

     Ce paquet de distribution est conçu pour être installé sur des ordinateurs avec une architecture x86/x64. Le paquet de distribution contient les outils de chiffrement qui exploitent l'algorithme de chiffrement AES avec une clé de 56 bits.

   - **Arm64**

     Ce paquet de distribution est conçu pour être installé sur des ordinateurs basés sur l'architecture ARM. Ce paquet de distribution n'est pas conçu pour être installé sur des serveurs.

2. **Transfert du paquet de distribution de l'application vers le stockage de l'ordinateur**

   Le paquet de distribution est une archive autoextractible au format EXE. Pour afficher le contenu du paquet de distribution, vous devez extraire l'archive dans un dossier séparé. Pour installer l'application, vous avez besoin de tous les fichiers du paquet de distribution, y compris le fichier bases.cab.

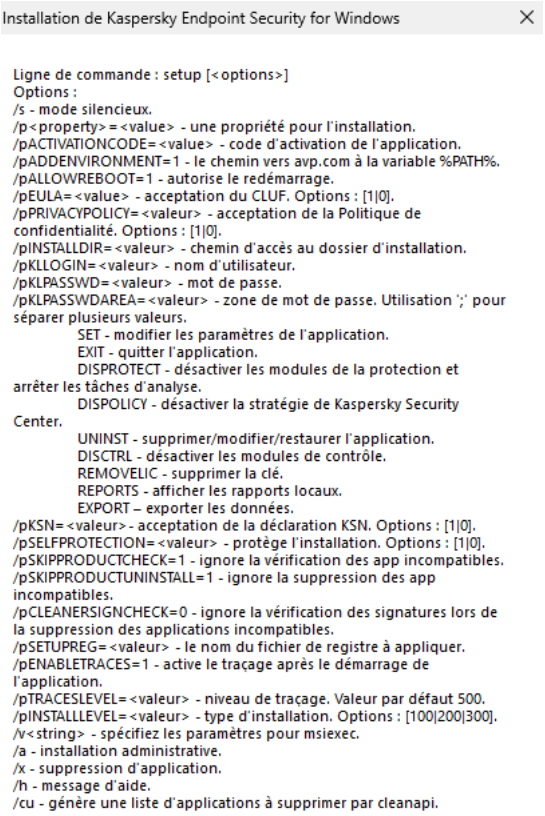
3. **Exécution de la commande d'installation**

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 (installation silencieuse). 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.

Vous pouvez consulter la liste des commandes d'installation de l'application à l'aide de la commande `/h`. Pour obtenir de l'aide sur la syntaxe de la commande d'installation, tapez `setup_kes.exe /h`. En conséquence, le programme d'installation affiche une fenêtre avec une description des options de commande (voir la figure ci-dessous).



Description des options de commande d'installation

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] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

ou

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

L'application est alors installée sur l'ordinateur. Vous pouvez confirmer que l'application est installée et vérifier les paramètres de l'application en lançant la commande `status`.

Paramètres d'installation de l'application

`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. L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.
`KSN`	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 : • `1` : acceptation de la participation à KSN. • `0` : refus de la participation à KSN (valeur par défaut). 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.
`CONFIGPATH=<path to the configuration file>`	Installation de l'application avec les paramètres prédéfinis. Pour ce faire, vous devez charger un 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.
`ALLOWREBOOT=1`	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. 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.
`SKIPPRODUCTCHECK=1`	Désactivez la recherche d'un logiciel installé. La liste des logiciels susceptibles de poser des problèmes de compatibilité figure dans le fichier incompatible.txt du kit de distribution. Si aucune valeur n'est définie pour ce paramètre et qu'aucun logiciel de la liste n'est détecté, l'installation de Kaspersky Endpoint Security sera interrompue.

`SKIPPRODUCTUNINSTALL=1`	Désactivez la suppression automatique des logiciels détectés de la liste incompatible.txt. Si le paramètre n'est pas spécifié, Kaspersky Endpoint Security tente de supprimer le logiciel susceptible de poser des problèmes de compatibilité. La suppression automatique du logiciel ne peut pas être activée lors de l'installation de Kaspersky Endpoint Security en utilisant le programme d'installation msiexec. Pour supprimer automatiquement les logiciels qui peuvent poser des problèmes de compatibilité, utilisez le fichier setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	Vérification des signatures numériques des fichiers de logiciels détectés dans la liste incompatible.txt. Pour supprimer le logiciel, Kaspersky Endpoint Security exécute le fichier d'installation du logiciel. Si le fichier d'installation ne possède pas de signature numérique, Kaspersky Endpoint Security considère que le fichier n'est pas fiable et interrompt la suppression du logiciel pour éviter l'exécution d'un code potentiellement malveillant. Si l'application ne peut pas vérifier la signature numérique du fichier logiciel détecté, l'installation de Kaspersky Endpoint Security est arrêtée avec une erreur. La valeur par défaut est différente selon la méthode d'installation du logiciel : • `0` signifie que la vérification de la signature numérique est désactivée (valeur par défaut en cas de déploiement via Kaspersky Security Center). • `1` signifie que la vérification de la signature numérique est activée (valeur par défaut si l'application est installée localement).
`STANDALONEMODE=1`	Installation de l'application dans la configuration Endpoint Detection and Response Agent (EDR Agent) pour l'intégration avec les solutions Kaspersky Endpoint Detection and Response (KATA) ou Kaspersky Endpoint Detection and Response Expert (on-premises). Cette configuration est nécessaire si une plateforme de protection des terminaux (PPE) tierce est déployée dans votre organisation en même temps que la solution Kaspersky Endpoint Detection and Response. Cela rend Kaspersky Endpoint Security dans la configuration Endpoint Detection and Response Agent compatible avec les applications PPE tierces.
`KLLOGIN`	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.
`KLPASSWD`	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`). 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.
`KLPASSWDAREA`	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 `KLLOGIN` et `KLPASSWD`). Pour indiquer plusieurs valeurs, utilisez le caractère `;`. Valeurs possibles : • `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. • `EXPORT` – exportation des paramètres de l'application Par exemple, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe. Il est donc impossible de configurer la zone d'action du mot de passe pour le compte KLAdmin. Si vous essayez de configurer la portée du mot de passe du compte KLAdmin, l'application interdit l'exécution des actions indiquées pour le groupe « Tous ».
`PROTECTOSSERVICES`	Protection des fonctionnalités des services du système d'exploitation. La protection des services du système d'exploitation empêche les applications tierces d'interférer avec le fonctionnement des services du système d'exploitation. Ces services incluent par exemple le service de lancement automatique de l'application. • `1` signifie que la protection des services du système d'exploitation est activée (valeur par défaut). • `0` signifie que la protection des services du système d'exploitation est désactivée.
`ENABLETRACES`	Activation ou désactivation du traçage de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` après le lancement. Valeurs possibles : • `1` : le traçage est activé. • `0` : le traçage est désactivé (valeur par défaut).

`TRACESLEVEL`	Niveau de détail du traçage Valeurs possibles : • `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.
`ENABLEAZURESUPPORT`	Activation ou désactivation du mode de compatibilité Azure WVD. Valeurs possibles : • `1` – Le mode de compatibilité Azure WVD est activé. • `0` – Le mode de compatibilité Azure WVD est désactivé (valeur par défaut). Cette fonctionnalité garantit l'affichage correct de l'état de la machine virtuelle Azure dans la console de Kaspersky Anti Targeted Attack Platform. Pour surveiller les performances de l'ordinateur, Kaspersky Endpoint Security envoie la télémétrie aux serveurs KATA. La télémétrie comprend un identifiant de l'ordinateur (Sensor ID). Le mode de compatibilité Azure WVD permet d'attribuer un Sensor ID unique permanent à ces machines virtuelles. Si le mode de compatibilité est désactivé, l'Sensor ID peut changer après le redémarrage de l'ordinateur en raison du fonctionnement des machines virtuelles Azure. Cela peut entraîner l'apparition de doublons de machines virtuelles sur la console.
`AMPPL`	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. La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019. Valeurs possibles : • `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.
`UPGRADEMODE`	Mode de mise à jour de l'application : • `Seamless` signifie mettre à jour l'application avec un redémarrage de l'ordinateur (valeur par défaut). • `Force` signifie mettre à jour l'application sans redémarrage. Vous pouvez mettre à jour l'application sans redémarrage à partir de la version 11.10.0. Pour mettre à jour une version antérieure de l'application, vous devez redémarrer l'ordinateur. Vous pouvez aussi installer les correctifs sans redémarrage à partir de la version 11.11.0. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Ainsi, le mode de mise à jour de l'application sera précisé dans les paramètres de l'application. Vous pouvez modifier ce paramètre dans les paramètres de l'application ou dans la stratégie. Lors de la mise à jour d'une application déjà installée, la priorité du paramètre de la ligne de commande est inférieure à celle du paramètre indiqué dans les paramètres de l'application ou dans le fichier setup.ini. Par exemple, si le mode de mise à jour `Force` est spécifié dans la ligne de commande et que le mode `Seamless` est précisé dans les paramètres de l'application, la mise à jour sera installée avec un redémarrage de l'ordinateur (`Seamless`).
`RESTAPI`	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`). Valeurs possibles : • `1` : l'administration via l'API REST est autorisée. • `0` : l'administration via l'API REST est interdite (valeur par défaut). 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 administrer l'application via l'API REST, il est impossible de l'administrer via les systèmes d'administration de Kaspersky.
`RESTAPI_User`	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. L'ajout d'un nom d'utilisateur est une condition indispensable à l'administration de l'application via l'API REST.
`RESTAPI_Port`	Port destiné à l'administration de l'application via l'API REST. Le port 6782 est utilisé par défaut. Assurez-vous que le port est disponible.
`RESTAPI_Certificate`	Certificat pour l'identification des demandes (par exemple, `RESTAPI_Certificate=C:\cert.pem`). L'interaction sécurisée de Kaspersky Endpoint Security avec le client REST nécessite la configuration de l'identification des requêtes. Pour ce faire, vous devez installer un certificat et signer ensuite la charge utile de chaque demande.

`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 : • `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.
`EnableUniqueSensorID`	Création d'un identifiant unique d'ordinateur (Sensor ID) lors de l'installation ou de la mise à jour de l'application. Le Sensor ID est utilisé dans la solution Kaspersky Anti Targeted Attack Platform pour identifier les ordinateurs qui envoient des données télémétriques au serveur. Lors de la création du Sensor ID, l'application utilise un algorithme qui prend en compte la configuration de l'ordinateur, comme le numéro de série de la carte mère. Dans certains cas, par exemple lors de l'utilisation de l'application dans un environnement virtuel, le Sensor ID peut être dupliqué. Par conséquent, Kaspersky Anti Targeted Attack Platform ne peut pas identifier l'ordinateur à partir duquel les données télémétriques sont envoyées. Pour créer un Sensor ID unique, vous devez définir le paramètre `EnableUniqueSensorID=1`. Par conséquent, l'application créera le Sensor ID à l'aide d'un algorithme différent, qui prend en compte les autres données relatives à l'ordinateur. Cela permet d'obtenir un Sensor ID unique. Par défaut, le paramètre n'est pas défini. L'application hérite du Sensor ID dans les cas suivants : • mise à jour de la version de l'application ; • migration de la configuration [KES+KEA] vers la configuration [KES+agent intégré]. Dans le cadre de la réparation de l'application, le programme d'installation tente d'hériter Sensor ID. Si le Sensor ID ne peut pas être restauré, l'application crée un nouveau Sensor ID.
`SKIPKB5007186CHECK=1`	Désactivation de la recherche de la mise à jour installée du système d'exploitation KB5007186. Avant l'installation de l'application, le programme d'installation vérifie les mises à jour installées du système d'exploitation. La mise à jour KB5007186 figure sur la liste des mises à jour du système d'exploitation qui peuvent entraîner des problèmes pour l'application. Pour en savoir plus, consultez la Base des connaissances du Support Technique. Par conséquent, le programme d'installation interrompt l'installation si cette mise à jour est détectée. Pour poursuivre l'installation, définissez `SKIPKB5007186CHECK=1`.

Exemple

```
setup_kes.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.

  Pour appliquer les paramètres du fichier setup.ini, placez le fichier dans le dossier contenant le kit de distribution de Kaspersky Endpoint Security.

- install.cfg : paramètres locaux de l'application Kaspersky Endpoint Security.

  Pour appliquer les paramètres du fichier de configuration install.cfg, vous devez indiquer le chemin d'accès au fichier dans la commande suivante d'installation de l'application : `CONFIGPATH=<path to the configuration file>`.

- 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 du fichier setup.reg, placez le fichier 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=<path to the setup.reg file>`.

Setup /x. Suppression de l'application

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 (suppression silencieuse). 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_kes.exe /s /x
     ```

     ou

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

     où `<GUID>` représente l'identifiant unique de l'application. Vous pouvez trouver le GUID de l'application dans la base de connaissances du support technique ou en utilisant la commande suivante :

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

   - Si la suppression est protégée par un mot de passe:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     ou

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Vous pouvez également utiliser le paramètre `SAVEQB` pour enregistrer les fichiers analysés par l'application et placés dans la Sauvegarde. Les copies de sauvegarde des fichiers sont enregistrées dans le dossier `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. Par défaut, l'enregistrement des fichiers dans la Sauvegarde est désactivé (`SAVEQB=0`).

Exemple

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

msiexec /i. Restauration de l'application

Lors de la restauration, l'application vérifie et restaure l'intégrité de tous les modules d'application et clés de registre système endommagés créés dans le cadre du processus d'installation de l'application.

La restauration 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. Après le démarrage de la restauration en mode silencieux, aucune intervention de votre part n'est requise.

Si le programme d'installation de Kaspersky Endpoint Security s'exécute en mode de restauration et que l'application n'a pas besoin d'être restaurée, le programme d'installation n'apporte aucune modification.

Si le programme d'installation de Kaspersky Endpoint Security s'exécute en mode de restauration et que l'application n'est pas installée, le programme d'installation démarre le processus d'installation.

Pour restaurer 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 restauration n'est pas protégée par un mot de passe:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     où `<GUID>` représente l'identifiant unique de l'application. Vous pouvez trouver le GUID de l'application dans la base de connaissances du support technique ou en utilisant la commande suivante :

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

   - Si la restauration est protégée par un mot de passe:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Exemple

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Commandes AVP

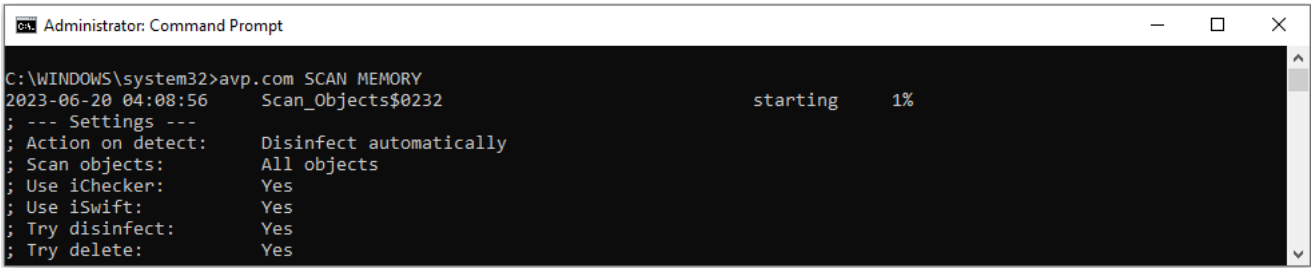
Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

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.

   Vous pouvez ajouter le chemin du fichier exécutable à la variable système %PATH% pendant la mise en place d'applications.
3. Utilisez le modèle suivant pour exécuter la commande :

   ```
   avp.com <command> [options]
   ```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



Administration de l'application via la ligne de commande

SCAN. Analyse des logiciels malveillants

Lancement de la tâche *Analyse des logiciels malveillants*

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report
file>] [<scan technologies>] [/C:<file with scan settings>]
```

Zone d'analyse	
`<files to scan>`	Liste de fichiers et de dossiers séparés par un espace. 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 : • `"C:\Program Files (x86)\Example Folder"` : long chemin d'accès. • `C:\PROGRA~2\EXAMPL~1` : chemin court.
`/ALL`	Lancer la tâche *Analyse des logiciels malveillants*. Kaspersky Endpoint Security 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 Dans Kaspersky Endpoint Security for Windows 12.12, la messagerie est exclue du champ d'application de l'analyse. L'analyse des messages entrants et sortants est effectuée par le module Protection contre les menaces par emails. Si vous utilisez une version antérieure du plug-in d'administration, l'application exclut les emails de la portée de l'analyse, même si la stratégie les inclut.
`/MEMORY`	Analyser la mémoire du noyau
`/STARTUP`	Analyser les objets chargés au lancement du système d'exploitation
`/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.
`/@:<file list.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 : • `"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`	**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.
`/i1`	**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 échoue, 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, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. Cette action est sélectionnée par défaut.
`/i3`	**Supprimer si la désinfection est impossible**. Supprimer également les fichiers composés (par exemple, les archives) s'il est impossible de désinfecter ou de supprimer le fichier infecté.
`/i4`	**Supprimer**. Supprimer également les fichiers composés (par exemple, les archives) s'il est impossible de supprimer le fichier infecté.

Types de fichiers	
`/fe`	**Fichiers analysés par extension**. Si ce paramètre est sélectionné, l'application 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, l'application 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, l'application 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:<file mask>`	Exclusion de l'analyse des fichiers sur la base d'un masque. Par exemple : • 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:<seconds>`	Exclusion de l'analyse des fichiers dont la durée d'analyse dépasse la valeur spécifiée en secondes.
`-es:<megabytes>`	Exclusion de l'analyse des fichiers dont la taille dépasse la valeur spécifiée en mégaoctets.

Mode d'enregistrement des événements dans un fichier de rapport (pour les profils Analyse, Programme de mise à jour et Restauration uniquement)	
`/R:<report file>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<report file>`	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 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 iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.

Paramètres avancés	
`/C:<file with scan settings>`	Fichier avec les paramètres de la tâche *Analyse des logiciels malveillants*. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Exemple

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "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

Lancement de la tâche *Mise à jour des bases et des modules d'application*

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Paramètres de la tâche de la mise à jour	
`local`	Démarrage de la tâche *Mise à jour des bases et des modules d'application* qui a été créée automatiquement après l'installation de l'application. Vous pouvez modifier les paramètres de la tâche *Mise à jour des bases et des modules d'application* 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 *Mise à jour des bases et des modules d'application* avec les paramètres par défaut ou avec les paramètres indiqués dans la commande. Vous pouvez configurer les paramètres de la tâche *Mise à jour des bases et des modules d'application* comme suit : • `UPDATE` lance la tâche *Mise à jour des bases et des modules d'application* 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 *Mise à jour des bases et des modules d'application* qui a été créée automatiquement après l'installation (tâche prédéfinie). • `UPDATE <update settings>` lance la tâche *Mise à jour des bases et des modules d'application* avec des paramètres définis manuellement (voir ci-dessous).

Source des mises à jour	
`"<update source>"`	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 d'enregistrement des événements dans un fichier de rapport (pour les profils Analyse, Programme de mise à jour et Restauration uniquement)	
`/R:<report file>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<report file>`	Enregistrer tous les événements dans le fichier de rapport.

Paramètres avancés	
`/C:<file with update settings>`	Fichier avec les paramètres de la tâche *Mise à jour des bases et des modules d'application*. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : `["<update source>"] [/R[A]:<report file>]`.

Exemple

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Restauration de la dernière mise à jour

Annulation des 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.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Mode d'enregistrement des événements dans un fichier de rapport (pour les profils Analyse, Programme de mise à jour et Restauration uniquement)	
`/R:<report file>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<report file>`	Enregistrer tous les événements dans le fichier de rapport.

Exemple

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. 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.14.2\Traces`. Par défaut, le traçage est désactivé.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Niveau de traçage	
`<tracing level>`	Niveau de détail du traçage Valeurs possibles : • `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 `file` et `mem`.
`file`	Enregistrer un fichier de traçage (sans limite de taille).
`rot`	Enregistrer les résultats du traçage dans un nombre limité d'ensembles 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.

Exemple

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Création d'un profil

Lancement d'un profil (par exemple, démarrage d'une mise à jour de base de données ou activation d'un module de protection).

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Nom du profil. Un *profil* désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP START`.

Mode d'enregistrement des événements dans un fichier de rapport (pour les profils Analyse, Programme de mise à jour et Restauration uniquement)	
`/R:<report file>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<report file>`	Enregistrer tous les événements dans le fichier de rapport.

Exemple

```
avp.com START Scan_Objects
```

STOP. Désactivation du profil

Arrêt de l'exécution du profil (par exemple, arrêt de l'analyse des disques amovibles ou désactivation d'un module de protection).

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit disposer des autorisations **Désactiver les modules de la protection**, **Désactiver les modules de contrôle**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Nom du profil. Un *profil* désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP STOP`.

Autorisation	
`/login=<user name> /password=<password>`	Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

STATUS. État du profil

Affichage des 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 informations sur l'état des profils de service peuvent être utiles lors de l'interaction avec le Support Technique de Kaspersky.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com STATUS [<profile>]
```

Si vous saisissez la commande sans profil, Kaspersky Endpoint Security affiche l'état de tous les profils de l'application.

STATISTICS. Statistiques de l'exécution du profil

Affichage des 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`.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com STATISTICS <profile>
```

RESTORE. Restauration des fichiers depuis la sauvegarde

Restauration d'un fichier depuis la Sauvegarde vers son emplacement d'origine. Si un fichier portant le même nom existe déjà dans le chemin indiqué, l'application demandera la confirmation du remplacement 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 avoir l'autorisation **Restaurer 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.14.2\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.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Paramètres avancés	
`/REPLACE`	Écraser le fichier existant.
`<file name>`	Nom du fichier à restaurer.

Autorisation	
`/login=<user name> /password=<password>`	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=samplePassword
```

EXPORT. Exportation des paramètres de l'application

Exportation des paramètres de Kaspersky Endpoint Security dans un fichier. Si la commande ne contient que le nom du fichier vers lequel vous souhaitez exporter les paramètres, l'application place le fichier comme suit :

- Si le chemin d'accès à avp.com est ajouté à la variable système %PATH%, l'application place le fichier dans le dossier `C:\Windows\SysWOW64`.
- Si vous exécutez la commande à partir du dossier d'installation de l'application, l'exportation échouera, car l'autoprotection de l'application bloque la création d'un nouveau fichier dans le dossier de l'application. Pour exporter les paramètres de l'application dans un fichier, saisissez le chemin d'accès au fichier.

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Exporter les paramètres**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Nom du profil. Un *profil* désigne un module, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP EXPORT`.

Fichier à exporter	
`<file name>`	Nom dans lequel les paramètres de l'application vont être exportés. Vous pouvez également saisir le chemin d'accès au fichier. Vous pouvez exporter les paramètres de Kaspersky Endpoint Security dans un fichier de configuration au format DAT ou CFG, un fichier au format TXT ou un document au format XML.

Autorisation	
`/login=<user name> /password= <password>`	Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

Exemple

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importation des paramètres de l'application

Importation des paramètres de Kaspersky Endpoint Security à partir d'un fichier créé avec la commande `EXPORT`.

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Configurer les paramètres de l'application**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Fichier à importer	
`<file name>`	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	
`/login=<user name> /password= <password>`	Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

Exemple

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Application du fichier clé

Activation de Kaspersky Endpoint Security à l'aide d'un fichier clé. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Fichier clé	
`<file name>`	Nom du fichier de licence

Autorisation	
`/login=<user name> /password=<password>`	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

Gestion des clés de licence de Kaspersky Endpoint Security, EDR Optimum ou EDR Expert (module complémentaire de Kaspersky Endpoint Detection and Response).

Pour pouvoir exécuter la commande de suppression de clé de licence, la Protection par mot de passe doit être activée. L'utilisateur doit avoir l'autorisation **Supprimer la clé**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Opération	
/ADD <file name>	Activation de Kaspersky Endpoint Security à l'aide d'un fichier clé. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve.
/ADD <activation code>	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	Mettez à jour l'état de la licence de Kaspersky Endpoint Security. L'application reçoit alors des informations à jour concernant l'état de la licence de la part des serveurs d'activation de Kaspersky.
/REFRESH <license ID>	Mettez à jour l'état des licences à l'aide de l'ID de licence. Cette commande permet de mettre à jour l'état du module complémentaire EDR, du module complémentaire MDR, du module complémentaire KUMA ou d'autres licences. Vous pouvez obtenir l'ID de licence à partir du certificat de licence. L'application reçoit alors des informations à jour concernant l'état de la licence de la part des serveurs d'activation de Kaspersky.
/CHECK	Obtenez les informations sur la licence Kaspersky Endpoint Security affiche des informations sur toutes les clés de licence ajoutées, y compris les clés de réserve, les clés du module complémentaire EDR, les clés du module complémentaire MDR, les clés du module complémentaire KUMA et les autres clés. Kaspersky Endpoint Security affiche les informations de licence suivantes : • nom de la licence ; • identifiant de la licence ; • adresse du Serveur de protection (SVM) auquel la machine virtuelle est connectée et sur lequel l'application est installée en mode Light Agent ; • type de licence : d'évaluation, commerciale, bêta, abonnement ; • date et heure de l'activation de l'application ; • date et heure d'expiration de la licence ; • nombre de jours restant avant l'expiration de la licence.
/CHECK <license ID>	Obtenez les informations sur la licence par ID. Vous pouvez utiliser cette commande pour obtenir des informations sur la licence. Vous pouvez obtenir l'ID de licence à partir du certificat de licence.
/DEL /login=<user name> /password= <password>	Supprimez la clé de licence de l'application. La clé de licence de réserve est également supprimée.
/DEL <license ID> /login=<user name> /password=<password>	Supprimer la clé à l'aide de l'ID de licence. Cette commande permet de supprimer une clé des modules complémentaires EDR, MDR, KUMA ou d'autres licences. Vous pouvez obtenir l'ID de licence à partir du certificat de licence.

Autorisation	
/login=<user name> /password= <password>	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 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Exemple

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Achat d'une licence

Accès au site de Kaspersky pour acheter une licence ou la renouveler.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

PBATESTRESET. Réinitialisation des résultats de l'analyse avant le chiffrement du disque

Réinitialisation des 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.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

EXIT. Quitter l'application

Quitter 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**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Désactiver la stratégie

Désactivation de 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 avoir l'autorisation **Désactiver la stratégie de Kaspersky Security Center**.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Activation de la stratégie

Activation de la stratégie de Kaspersky Security Center sur l'ordinateur. Les paramètres de l'application sont alors configurés conformément à la stratégie.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

DISABLE. Désactivation de la protection

Désactivation de la Protection contre les fichiers malicieux sur un ordinateur doté d'une licence de 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.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

SPYWARE. Détection de logiciels espion

Gestion de la détection des logiciels espions. La détection de logiciels espion est activée par défaut.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com SPYWARE on|off
```

KSN. Basculement entre KSN / KPSN

Sélection d'une solution Kaspersky pour déterminer la réputation de fichiers ou de sites Web. Kaspersky Endpoint Security prend en charge les solutions d'infrastructure suivantes pour utiliser les bases de données de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky 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.

- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
avp.com KSN /global | /private <file name>
```

Fichier de configuration de Kaspersky Security Network	
`<file name>`	Nom du fichier de configuration contenant les paramètres de Kaspersky Private Security Network. Ce fichier porte l'extension PKCS7 ou PEM.

Exemple

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Exemple

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Désactivation de la protection de la connexion au serveur

Exécution de la tâche *Protection de la connexion au Serveur d'administration*, qui entraîne la suppression du mot de passe de la connexion de l'ordinateur au Serveur d'administration. De cette manière, la tâche désactive la protection de la connexion au Serveur d'administration.

L'exécution de la commande requiert l'activation de la Protection par mot de passe.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Mot de passe	
`/password=<password>`	Le mot de passe du compte utilisateur KL Admin ou le mot de passe de la tâche *Protection de la connexion au Serveur d'administration*. Si le paramètre n'est pas indiqué, Kaspersky Endpoint Security vous invite à saisir un mot de passe à la ligne suivante.

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 standard, comme *Analyse des logiciels malveillants* et *Mise à jour des bases et des modules d'application*.

Vous pouvez consulter la liste des commandes KESCLI à l'aide de la commande `kescli --help` ou en utilisant la commande abrégée `kescli -h`.

Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

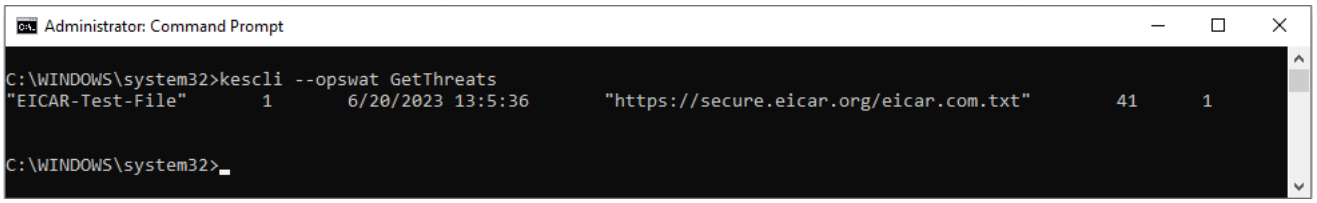
1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

   Vous pouvez ajouter le chemin du fichier exécutable à la variable système %PATH% pendant la mise en place d'applications.

3. Utilisez le modèle suivant pour exécuter la commande :

```
kescli <commande> [options]
```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



Administration de l'application via la ligne de commande

Scan. Analyse des logiciels malveillants

Exécution de la *Analyse des logiciels malveillants* (Analyse complète).

Pour exécuter la tâche, l'administrateur doit autoriser l'utilisation de tâches locales dans la stratégie.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Vous pouvez vérifier l'état d'achèvement de la tâche *Analyse des logiciels malveillants* 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	
`<scan scope>`	Liste de fichiers et de dossiers séparés par le symbole `;`. Par exemple, `"C:\Program Files (x86)\Example Folder"`.

Action en cas de détection d'une menace	
`0`	**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.
`1`	**Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. 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

Affichage des informations à propos de l'état d'achèvement de la tâche *Analyse des logiciels malveillants* (*Analyse complète*) :

- `1` : l'analyse est en cours.
- `0` : l'analyse n'est pas en cours.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat GetScanState
```

GetLastScanTime. Calcul du temps requis pour l'analyse

Affichage des informations à propos de la date et de l'heure d'achèvement de la dernière tâche *Analyse des logiciels malveillants* (*Analyse complète*).

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat GetLastScanTime
```

GetThreats. Collecte de données à propos des menaces détectées

Affichage de la 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.

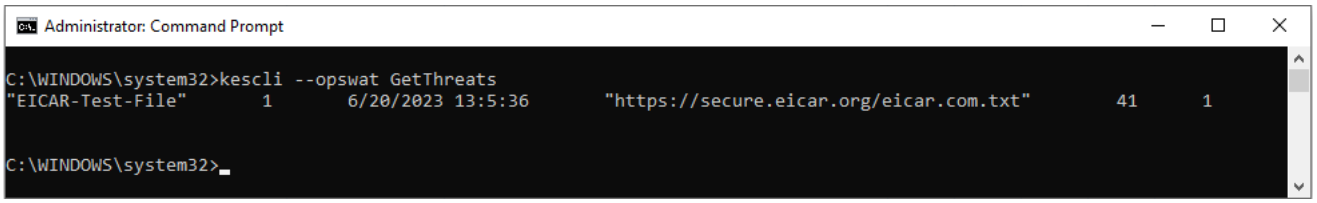
Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat GetThreats
```

Lorsque cette commande est exécutée, Kaspersky Endpoint Security envoie une réponse au format suivant :

```
<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>
```



Administration de l'application via la ligne de commande

Type d'objet	
0	Inconnu (Unknown).
1	Virus (Virware).
2	Chevaux de Troie (Trojware).
3	Programmes malveillants (Malware).
4	Programmes publicitaires (Adware).
5	Numéroteurs automatiques (Pornware).
6	Applications qui pourraient être utilisées par un cybercriminel pour nuire à l'ordinateur ou aux données de l'utilisateur (Riskware).
7	Objets compressés dont la méthode d'emballage peut être utilisée pour protéger du code malveillant (Packed)
20	Objets inconnus (Xfiles).
21	Applications connues (Software).
22	Fichiers cachés (Hidden).
23	Applications nécessitant une attention particulière (Pupware).
24	Comportement anormal (Anomaly).
30	Non déterminé (Undetect).
40	Bannières publicitaires (Banner).
50	Attaque réseau (Attack).
51	Accès au registre (Registry).
52	Activité suspecte (Suspicion).
60	Vulnérabilités (Vulnerability).
70	Phishing (Phishing).
80	Pièce jointe indésirable (Attachment).
90	Programme malveillant détecté par Kaspersky Security Network (Urgent).
100	Lien inconnu (Suspic URL).
110	Autre programme malveillant (Behavioral).

Action en cas de détection d'une menace	
0	Inconnu (unknown).
1	La menace a été éliminée (ok).
2	L'objet a été infecté et n'a pas été désinfecté (infected).
5	L'objet se trouve dans une archive et n'a pas été désinfecté (archive).
9	L'objet a été désinfecté (disinfected).
10	L'objet n'a pas été désinfecté (not disinfected).

11	L'objet a été supprimé (`deleted`).
13	Une copie de sauvegarde de l'objet a été créée (`backupped`).
15	L'objet a été déplacé vers la Sauvegarde (`quarantined`).
23	L'objet a été supprimé au redémarrage de l'ordinateur (`delete on reboot`).
25	L'objet a été désinfecté au redémarrage de l'ordinateur (`disinfect on reboot`).
29	L'objet a été déplacé vers la Sauvegarde par un utilisateur (`added by user`).
30	L'objet a été ajouté aux exclusions (`added to exclude`).
31	L'objet a été déplacé vers la Sauvegarde au redémarrage de l'ordinateur (`quarantine on reboot`).
36	Faux positif (`false alarm`).
38	Le processus a été interrompu (`terminated`).
40	L'objet n'a pas été détecté (`not found`).
41	Impossible de traiter la menace (`untreatable`).
42	L'objet a été restauré (`rolled back`).
43	L'objet a été créé à la suite d'une menace (`produced by threat`).
44	L'objet a été restauré au redémarrage de l'ordinateur (`roll back on reboot`).
`0xffffffff`	L'objet n'a pas été traité (`discarded`).

Niveau de danger de la menace	
`0`	Inconnu
`1`	Élevé
`2`	Analyse standard
`4`	Faible
`8`	Informations (inférieur à *Faible*)

UpdateDefinitions. Mise à jour des bases de données et des modules de l'application

Lancement de la tâche *Mise à jour des bases et des modules d'application* Kaspersky Endpoint Security utilise la source par défaut : les serveurs de mises à jour de Kaspersky.

Pour exécuter la tâche, l'administrateur doit autoriser l'utilisation de tâches locales dans la stratégie.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Cette commande ne peut pas être exécutée si l'application est installée en mode Light Agent.

Syntaxe de la commande

```
kescli --opswat UpdateDefinitions
```

Vous pouvez afficher la date et l'heure de publication des bases de données antivirus actuelles à l'aide de la commande `GetDefinitionsetState`.

GetDefinitionState. Définition de la date et de l'heure de la dernière mise à jour des bases de données

Affichage des informations sur la date et l'heure de la dernière mise à jour des bases de données antivirus utilisées.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat GetDefinitionState
```

EnableRTP. Activation de la protection

Activation des modules de protection de Kaspersky Endpoint Security sur l'ordinateur : 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.

> Pour activer les modules de protection, l'administrateur doit s'assurer que les paramètres de stratégie pertinents peuvent être modifiés (les attributs sont ouverts).

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

Syntaxe de la commande

```
kescli --opswat EnableRTP
```

Par conséquent, les modules de protection sont activés, même si vous avez interdit la modification des paramètres de l'application avec la protection par mot de passe.

Vous pouvez vérifier l'état de fonctionnement de la Protection contre les fichiers malicieux à l'aide de la commande `GetRealTimeProtectionState`.

GetRealTimeProtectionState. États de la Protection contre les fichiers malicieux

Affichage des informations à propos de l'état du module Protection contre les fichiers malicieux :

- `1` : le module est activé.
- `0` : le module est désactivé.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

```
Syntaxe de la commande
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. État de chiffrement des disques

Affichage des informations sur l'état de chiffrement du disque :

- `1` signifie que le disque est protégé par la technologie de chiffrement de disque Kaspersky ou BitLocker.
- `0` signifie que le disque n'est pas chiffré.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

```
Syntaxe de la commande
kescli --opswat GetEncryptionState
```

Version. Identification de la version de l'application

Affichage de la version de Kaspersky Endpoint Security for Windows.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.

```
Syntaxe de la commande
kescli --Version
```

Vous pouvez également utiliser la commande abrégée `-v`.

Commandes d'administration de Detection and Response

Vous pouvez utiliser la ligne de commande pour administrer les fonctionnalités intégrées des solutions Detection and Response (par exemple, Kaspersky Sandbox ou Kaspersky Endpoint Detection and Response Optimum). Vous pouvez administrer les solutions Detection and Response si l'administration à l'aide de la console Kaspersky Security Center n'est pas possible. 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 <command>`.

Pour gérer les fonctionnalités intégrées des solutions Detection and Response à l'aide 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 fichier exécutable de Kaspersky Endpoint Security.
3. Utilisez le modèle suivant pour exécuter la commande :

```
avp.com <command> [options]
```

En conséquence, Kaspersky Endpoint Security exécutera la commande.

SANDBOX. Gestion de Sandbox

Commandes relatives à l'administration du module Sandbox :

- Activation ou désactivation du module Sandbox.

  Les modules Sandbox permettent d'interagir avec la solution Kaspersky Sandbox et le module KATA Sandbox, qui fait partie de Kaspersky Anti Targeted Attack Platform.

- Configuration du module Kaspersky Sandbox :

  - Connexion de l'ordinateur aux serveurs Sandbox.

    Les serveurs utilisent des images virtuelles déployées des systèmes d'exploitation Microsoft Windows pour exécuter les objets qui doivent être analysés. Vous pouvez saisir une adresse IP (IPv4 ou IPv6) ou un nom de domaine pleinement qualifié. Pour en savoir plus sur le déploiement des images virtuelles et la configuration des serveurs Sandbox, consultez l'aide de Kaspersky Sandbox et l'aide de Kaspersky Anti Targeted Attack Platform.

  - Configuration du délai d'attente de la connexion avec le serveur.

    Délai d'attente de connexion du serveur Sandbox (pour Kaspersky Sandbox) ou du serveur Central Node (pour KATA). Une fois le délai d'attente configuré écoulé, Kaspersky Endpoint Security envoie une requête au serveur suivant. Vous pouvez augmenter le délai d'attente de la connexion avec le serveur si votre vitesse de connexion est faible ou si la connexion est instable. Le délai d'attente recommandé pour les demandes est de 0.5 seconde ou moins.

  - Configuration d'une connexion de confiance entre l'ordinateur et les serveurs.

    Pour configurer une connexion sécurisée avec le serveur Sandbox (pour Kaspersky Sandbox) ou le serveur Central Node (pour KATA), vous devez préparer un certificat TLS. Il faut ensuite ajouter le certificat à l'ordinateur à l'aide d'une stratégie. Vous devez également ajouter le certificat au serveur Sandbox (pour Kaspersky Sandbox) ou au serveur Central Node (pour KATA).

  - Configuration du mode d'intégration.

Vous devez sélectionner une solution dont Sandbox fait partie, c'est-à-dire Kaspersky Sandbox ou KATA Sandbox. *Kaspersky Sandbox* est une solution autonome de détection et de réponse de Kaspersky. *KATA Sandbox* est un module de la solution Kaspersky Anti Targeted Attack Platform. Une fois intégré à KATA Sandbox, le module peut fonctionner dans les modes suivants :

- **Manuel**. L'utilisateur envoie manuellement le fichier pour analyse à l'aide du menu contextuel (**Envoyer à la Sandbox**).
- **Automatique**. L'application détecte automatiquement les objets et les envoie à la Sandbox pour analyse.
- **Combiné**.

- Affichage des paramètres actuels du module.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Opération	
`stop`	Désactiver le module Sandbox.
`start`	Activer le module Sandbox.

`set`	Configurer le module Sandbox. Vous pouvez configurer les paramètres suivants :
	• Ajouter des serveurs Sandbox (`--servers`)
	• Ajoutez un certificat TLS (`--pinned-certificate`)
	• Ajouter un conteneur crypto (`--client-certificate`)
	• Définir un mot de passe pour le conteneur crypto (`--client-certificate-password`) ;
	• Définir le délai d'attente de connexion du serveur (`--timeout`)
	• Sélectionnez un mode d'intégration (`--mode`) :
	  • `KSB` : intégration avec Kaspersky Sandbox ;
	  • `KATAManual` : intégration manuelle à KATA Sandbox ;
	  • `KATAAuto` : intégration automatique à KATA Sandbox ;
	  • `KATAFull` : intégration combinée à KATA Sandbox.

`show`	Afficher les paramètres actuels du module. Vous obtenez la réponse suivante :
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autorisation	
`/login=<user name> /password=<password>`	Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

Exemple

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. Gestion de la prévention de l'exécution

Désactivation du module Prévention de l'exécution ou affichage des paramètres actuels du module, y compris la liste des règles pour la prévention de l'exécution.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com prevention disable
```

```
avp.com prevention /show
```

En exécutant la commande `prevention /show`, vous obtiendrez la réponse suivante :

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Valeurs de retour de la commande :

- `-1` signifie que la commande n'est pas prise en charge par la version de l'application installée sur l'ordinateur.
- `0` signifie que la commande a été correctement exécutée.
- `1` signifie qu'un argument obligatoire n'a pas été transmis à la commande.
- `2` signifie qu'une erreur générale s'est produite.

- 4 signifie qu'il y a eu une erreur de syntaxe.
- 9 : opération erronée (par exemple, une tentative de désactiver le module alors qu'il est déjà désactivé).

ISOLATION. Administration de l'isolation du réseau

Désactivation de l'isolation réseau de l'ordinateur ou affichage des paramètres actuels du module. Les paramètres du module comprennent également une liste des connexions réseau ajoutées aux exclusions.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Après avoir exécuté la commande `stat`, vous recevez la réponse suivante : `Network isolation on|off`.

RESTORE. Restauration des fichiers depuis la quarantaine

Restauration d'un fichier à partir de la Quarantaine vers son emplacement d'origine. La *Quarantaine* est un stockage local spécial sur l'ordinateur. L'utilisateur peut mettre en quarantaine les fichiers qu'il considère comme dangereux pour l'ordinateur. Les fichiers mis en quarantaine sont stockés dans un état chiffré et ne menacent pas la sécurité de l'appareil. Kaspersky Endpoint Security utilise la Quarantaine uniquement lorsqu'elle est intégrée aux solutions de détection et de réponse de Kaspersky. Dans d'autres cas, Kaspersky Endpoint Security place le fichier correspondant dans la Sauvegarde. Pour en savoir plus sur la gestion de la Quarantaine dans le cadre des solutions, veuillez consulter l'aide de Kaspersky Sandbox, l'aide de Kaspersky Endpoint Detection and Response Optimum, l'aide de Kaspersky Endpoint Detection and Response Expert, l'aide de Kaspersky Anti Targeted Attack Platform et l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Restaurer depuis la Sauvegarde**.

L'objet est mis en quarantaine sous le compte système (SYSTEM).

La restauration de fichiers depuis la quarantaine implique les considérations spéciales suivantes :

- Si le dossier de destination a été supprimé ou si l'utilisateur ne dispose pas de droits d'accès à ce dossier, l'application place le fichier dans le dossier `%DataRoot%\QB\Restored`. Ensuite, vous devez déplacer manuellement le fichier vers le dossier cible.
- L'application traite le nom du fichier à restaurer en respectant la casse. Si vous ne respectez pas la casse lors de la saisie du nom du fichier, l'application ne restaure pas le fichier.

- Si le dossier de destination contient déjà un fichier portant le même nom, l'application annule la restauration du fichier.

- Si vous utilisez la solution KATA (EDR), l'application enregistre une copie du fichier dans la Quarantaine après la restauration du fichier. Vous pouvez vider la Quarantaine manuellement. Dans le cas des solutions EDR Optimum et EDR Expert, l'application supprime le fichier après la restauration.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Paramètres avancés	
`/REPLACE`	Écraser le fichier existant.
`<file name>`	Nom du fichier à restaurer.

Autorisation	
`/login=<user name> /password=<password>`	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=samplePassword
```

Valeurs de retour de la commande :

- `-1` signifie que la commande n'est pas prise en charge par la version de l'application installée sur l'ordinateur.

- `0` signifie que la commande a été correctement exécutée.

- `1` signifie qu'un argument obligatoire n'a pas été transmis à la commande.

- `2` signifie qu'une erreur générale s'est produite.

- `4` signifie qu'il y a eu une erreur de syntaxe.

IOCSCAN. Rechercher d'indicateurs de compromission (IOC)

Lancement de la tâche *Analyse IOC* Un *indicateur de compromission (IOC)* est un ensemble de données concernant un objet ou une activité qui indique un accès non autorisé à l'ordinateur (compromission des données). Par exemple, de nombreuses tentatives infructueuses de se connecter au système peuvent constituer un indicateur de compromission. La tâche *Analyse IOC* permet de trouver des indicateurs de compromission sur l'ordinateur et de prendre des mesures de réponse aux menaces.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

L'analyse IOC est interrompue au bout de 128 correspondances avec les indicateurs de compromission décrits dans les fichiers IOC. Cette opération est nécessaire afin de limiter le nombre d'entrées dans le rapport de la tâche d'analyse IOC, d'en faciliter l'analyse et d'éviter tout débordement dû à la présence d'indicateurs de compromission formulés de manière imprécise qui peuvent générer un grand nombre de correspondances.

Syntaxe de la commande

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Fichiers IOC	
`<full path to the IOC file>`	Chemin d'accès complet au fichier IOC que vous souhaitez utiliser pour effectuer l'analyse. Vous pouvez indiquer plusieurs fichiers IOC séparés par des espaces. Le chemin d'accès complet au fichier IOC doit être saisi sans l'argument `/path`. Par exemple, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Chemin d'accès au dossier contenant les fichiers IOC que vous souhaitez utiliser pour effectuer l'analyse. Les *fichiers IOC* sont des fichiers contenant les ensembles d'indicateurs que l'application tente de faire correspondre pour compter une détection. Les fichiers IOC doivent être conformes standard OpenIOC. Par exemple, `C:\Users\Admin\Desktop\IOC`

Type de données pour l'analyse IOC	
`/process=on|off`	Analyser les données du processus lors de l'analyse IOC (terme ProcessItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les processus en cours d'exécution sur l'ordinateur lors de l'analyse. Si le fichier IOC contient des termes IOC du document IOC ProcessItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données de processus uniquement si le document IOC ProcessItem est décrit dans le fichier IOC fourni pour l'analyse.
`/hint=<full path to the executable file of the process|full path to the file>`	Analyser les données des fichiers lors de l'analyse IOC (termes ProcessItem et FileItem). Vous pouvez sélectionner un fichier d'une des manières suivantes : • `<full path to the executable file of the process>` : terme ProcessItem ; • `<full path to the file>` : terme FileItem.
`/registry=on|off`	Analyser les données du registre Windows lors de l'exécution d'une analyse IOC (terme RegistryItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le registre Windows. Si le fichier IOC contient des termes du document IOC RegistryItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le registre Windows uniquement si le document IOC RegistryItem est décrit dans le fichier IOC fourni pour l'analyse. Pour le type de données RegistryItem, Kaspersky Endpoint Security analyse un ensemble de clés de registre.
`/dnsentry=on|off`	Analyser les données relatives aux enregistrements dans le cache DNS local lors de l'analyse IOC (terme DnsEntryItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le cache DNS local. Si le fichier IOC contient des termes du document IOC DnsEntryItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le cache DNS local uniquement si le document IOC DnsEntryItem est décrit dans le fichier IOC fourni pour l'analyse.

`/arpentry=on|off`	Analyser les données relatives aux enregistrements de la table ARP lors de l'exécution de l'analyse IOC (terme ArpEntryItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le tableau ARP. Si le fichier IOC contient des termes du document IOC ArpEntryItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le tableau ARP uniquement si le document IOC ArpEntryItem est décrit dans le fichier IOC fourni pour l'analyse.
`/ports=on|off`	Analyser les données relatives aux ports ouverts à l'écoute lors de l'analyse IOC (terme PortItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas le tableau des connexions actives sur l'appareil. Si le fichier IOC contient des termes du document IOC PortItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le tableau des connexions actives uniquement si le document IOC PortItem est décrit dans le fichier IOC fourni pour l'analyse.
`/services=on|off`	Analyser les données relatives aux services installés sur l'appareil lors de l'analyse IOC (terme ServiceItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données relatives aux services installés sur l'appareil. Si le fichier IOC contient des termes du document IOC ServiceItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données de service uniquement si le document IOC ServiceItem est décrit dans le fichier IOC fourni pour l'analyse.
`/system=on|off`	Analyser les données de l'environnement lors de l'analyse IOC (terme SystemInfoItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données de l'environnement. Si le fichier IOC contient des termes du document IOC SystemInfoItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données de l'environnement uniquement si le document IOC SystemInfoItem est décrit dans le fichier IOC fourni pour l'analyse.
`/users=on|off`	Analyser les données relatives aux utilisateurs lors de l'analyse IOC (terme UserItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données relatives aux utilisateurs créées dans le système. Si le fichier IOC contient des termes du document IOC UserItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données relatives aux utilisateurs créées dans le système uniquement si le document IOC UserItem est décrit dans le fichier IOC fourni pour l'analyse.
`/volumes=on|off`	Analyser les données relatives aux volumes lors de l'analyse IOC (terme VolumeItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données relatives aux volumes sur l'appareil. Si le fichier IOC contient des termes du document IOC VolumeItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données relatives aux volumes uniquement si le document IOC VolumeItem est décrit dans le fichier IOC fourni pour l'analyse.
`/eventlog=on|off`	Analyser les données relatives aux enregistrements dans le journal des événements Windows lors de l'analyse IOC (terme EventLogItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les enregistrements du journal des événements Windows. Si le fichier IOC contient des termes du document IOC EventLogItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse le journal des événements Windows si le document IOC EventLogItem est décrit dans le fichier IOC fourni pour l'analyse. Pour le terme IOC EventLogItem\source, utilisez la valeur **Nom du fournisseur** du schéma XML de l'événement.

`/datetime=<event publication date>`	Prenez en considération la date à laquelle l'événement a été publié dans le journal des événements Windows pour déterminer la zone d'analyse IOC pour le document IOC correspondant. Lors de l'exécution d'une analyse IOC, Kaspersky Endpoint Security analyse les entrées du journal d'événements Windows publiées pendant la période allant de l'heure et de la date indiquées jusqu'au moment de l'exécution de la tâche. Kaspersky Endpoint Security permet d'indiquer la date de publication de l'événement comme valeur de l'argument. L'analyse est effectuée uniquement pour les événements publiés dans le journal des événements Windows après la date indiquée et avant l'exécution de l'analyse. Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les événements avec n'importe quelle date de publication. Le paramètre `TaskSettings::BaseSettings::EventLogItem::datetime` ne peut pas être modifié. Ce paramètre est utilisé uniquement si le document IOC EventLogItem est décrit dans le fichier IOC fourni pour l'analyse.
`/channel=<list of channels>`	Liste des noms de canaux (journaux) pour lesquels vous souhaitez effectuer une analyse IOC. Si l'argument est indiqué, Kaspersky Endpoint Security analyse les enregistrements publiés dans les journaux indiqués. Le terme EventLogItem doit être décrit dans le document IOC. Le nom du journal est indiqué sous forme de chaîne conformément au nom du journal (canal) indiqué dans les propriétés du journal (le paramètre Full Name) ou dans les propriétés de l'événement (le paramètre `<Channel></Channel>` dans le schéma xml de l'événement). Vous pouvez indiquer plusieurs canaux séparés par des espaces. Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les enregistrements pour les canaux `Application`, `System`, `Security`.
`/files=on|off`	Analyser les données des fichiers lors de l'analyse IOC (terme FileItem). Si la valeur de l'argument est `off`, Kaspersky Endpoint Security n'analyse pas les données des fichiers. Si le fichier IOC contient des termes du document IOC FileItem, ceux-ci sont ignorés (détectés comme ne présentant aucune correspondance). Si l'argument n'est pas indiqué, Kaspersky Endpoint Security analyse les données relatives aux fichiers uniquement si le document IOC FileItem est décrit dans le fichier IOC fourni pour l'analyse.
`/drives=<all|system|critical|custom>`	Définir la zone d'analyse IOC lors de l'analyse des données pour le document IOC FileItem. Vous pouvez définir les valeurs suivantes pour la zone d'analyse : • `<all>` pour toutes les zones d'actions de fichiers disponibles. • `<system>` pour les fichiers dans les dossiers où le système d'exploitation est installé. • `<critical>` pour les fichiers temporaires dans les dossiers de l'utilisateur et du système. • `<custom>` pour les fichiers dans les champs d'application définis par l'utilisateur (`/scope=<list of folders to scan>`). Si l'argument n'est pas indiqué, l'analyse est effectuée pour les zones critiques.
`/excludes=<list of exclusions>`	Définir la zone d'exclusion lors de l'analyse des données pour le document IOC FileItem. Vous pouvez indiquer plusieurs chemins séparés par des espaces.
`/scope=<list of folders to scan>`	Zone d'analyse IOC définie par l'utilisateur lors de l'analyse des données pour le document IOC FileItem (`/drives=custom`). Vous pouvez indiquer plusieurs chemins séparés par des espaces.
`/retro /<number of days>`	*Analyse IOC rétrospective* est un mode de la tâche *Analyse IOC* dans laquelle Kaspersky Endpoint Security recherche des indicateurs de compromission à l'aide des données pendant une certaine période. Ce mode est destiné à la recherche d'indicateurs de compromission à partir des données de télémétrie de l'ordinateur protégé, telles que l'activité réseau, les processus, les fichiers et d'autres données télémétriques. Vous pouvez définir une période de 1 à 14 jours. Par défaut, l'application recherche les indicateurs de compromission pendant une journée.
`/network=on|off`	Analyse des données du réseau (le terme NetworkItem).
`/url=on|off`	Analyse des données dans les journaux du navigateur (le terme UrlHistoryItem). L'analyse IOC rétrospective analyse les journaux des navigateurs suivants : Google Chrome, Mozilla Firefox, Microsoft Edge (version 79 ou ultérieure).
`/email`	Analyse des objets de messagerie (le terme EmailItem).
`/route`	Analyse des tables de routage et de transfert (le terme RouteEntryItem).

Valeurs de retour de la commande :

- `-1` signifie que la commande n'est pas prise en charge par la version de l'application installée sur l'ordinateur.
- `0` signifie que la commande a été correctement exécutée.

- 1 signifie qu'un argument obligatoire n'a pas été transmis à la commande.
- 2 signifie qu'une erreur générale s'est produite.
- 4 signifie qu'il y a eu une erreur de syntaxe.

Si la commande a été correctement exécutée (valeur de retour `0`) et que des indicateurs de compromission ont été détectés en cours de route, Kaspersky Endpoint Security envoie les informations suivantes sur le résultat de la tâche dans la ligne de commande :

`Uuid`	Identifiant du fichier IOC à partir de l'en-tête de la structure du fichier IOC (le tag `<ioc id="">`)
`Name`	Description du fichier IOC à partir de l'en-tête de la structure du fichier IOC (le tag `<description> </description>`)
`Matched Indicator Items`	Liste des identifiants de tous les indicateurs correspondants.
`Matched objects`	Données pour chaque document IOC pour lequel il y avait une correspondance.

MDRLICENSE. Activation MDR

Ajout du fichier de configuration BLOB pour activer Managed Detection and Response. Le fichier BLOB contient l'ID du client et des informations sur la licence de 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 l'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 ( ).

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Opération	
`/ADD <file name>`	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=<user name> /password= <password>`	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=samplePassword
```

```
Exemple
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Intégration d'EDR (KATA)

Commandes de gestion du module Endpoint Detection and Response (KATA) :

- Activation ou désactivation du module EDR (KATA).

  Le module EDR (KATA) assure l'interopérabilité avec la solution Kaspersky Anti Targeted Attack Platform.

- Configuration de la connexion aux serveurs Kaspersky Anti Targeted Attack Platform.

- Affichage des paramètres actuels du module.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

```
Syntaxe de la commande
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Opération	
`stop`	Désactivez le module EDR (KATA).
`start`	Activez le module EDR (KATA).
`set`	Configurez le module EDR (KATA). Vous pouvez configurer les paramètres suivants : • Ajouter des serveurs Central Node (`servers=<server address>:<port>`) • Ajoutez un certificat TLS (`server-certificate=<path to the TLS certificate>`) • Définir le délai d'attente de connexion du serveur Sandbox (`/timeout=<Central Node server connection timeout (s)>`) • Définir la période de synchronisation avec le serveur Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Afficher les paramètres actuels du module.

EDRExpertOnPrem. Intégration d'EDR Expert (on-premises)

Commandes de gestion de l'agent intégré permettant de configurer l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises) :

- Activation ou désactivation de l'agent EDR Expert (on-premises) intégré.
- Configuration des paramètres de connexion aux serveurs EDR Expert (on-premises).
- Affichage des paramètres actuels de l'agent intégré.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Opération	Description
`stop`	Désactivez l'agent EDR Expert (on-premises) intégré.
`start`	Activez l'agent EDR Expert (on-premises) intégré.

`set`	Configurez l'agent EDR Expert (on-premises) intégré.
	Vous pouvez configurer les paramètres de connexion suivants pour les *serveurs de réponse* :
	• `servers=<server address>:<port>`. Adresse du serveur de réponse (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Utilisez un conteneur cryptographique pour l'authentification bidirectionnelle. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée au format PKCS#12. Pour activer cette authentification, vous devez créer un conteneur crypto auprès d'une autorité de certification externe.
	• `timeout=<server connection timeout (s)>`. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.
	• `sync-period=<server synchronization period (min)>`. Fréquence des requêtes de synchronisation envoyées au serveur. Pendant la synchronisation, Kaspersky Endpoint Security reçoit les tâches de réponse aux menaces et envoie les résultats des tâches.
	Vous pouvez configurer les paramètres de connexion suivants pour les *serveurs de collecte des données télémétriques* :
	• `telemetry-servers=<server address:port>`. Adresse du serveur de collecte des données télémétriques (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password= <password to the PFX archive>`. Utilisez un conteneur cryptographique pour l'authentification bidirectionnelle. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée au format PKCS#12. Pour activer cette authentification, vous devez créer un conteneur crypto auprès d'une autorité de certification externe.
	• `telemetry-timeout=<server connection timeout (s)>`. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur.
	• `events-send-period=<seconds>`. Délai maximum lors de l'envoi des événements. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
	• `events-limit=<0|1>`. Limitez le nombre de requêtes. Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.
	• `events-per-hour=<number of events>`. Nombre maximum d'événements par heure. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.
	• `max-packet-length=<number of packets>`. Longueur maximale des paquets. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.
	• `telemetry-only-tagged-events=<0|1>`. Envoi de la télémétrie avec IOA uniquement. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements.
	Vous pouvez configurer les paramètres généraux suivants :
	• `mode=EDRKATA | EDRExpertOnPrem`. Basculement entre les solutions :
	  • `EDRKATA`. Endpoint Detection and Response Expert (version 7.1 ou version antérieure).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (version 8.0 ou version ultérieure). Valeur par défaut.
	• `login=<user name> password=<password>`. Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

`show`	Afficher les paramètres actuels du module.

KUMA. Intégration de KUMA

Commandes liées à l'administration de l'agent KUMA intégré :

- Activation ou désactivation de l'intégration de KUMA.

  L'agent KUMA intégré assure l'interopérabilité avec la solution Kaspersky Unified Monitoring and Analysis Platform.

- Configuration de la connexion aux serveurs de Kaspersky Unified Monitoring and Analysis Platform.

- Affichage des paramètres actuels du module.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Opération	
`stop`	Désactiver l'intégration de KUMA.
`start`	Activer l'intégration de KUMA.
`set`	Configurer l'agent KUMA intégré. Vous pouvez configurer les paramètres suivants : • Ajoutez des serveurs KUMA (`/servers=<protocol>://<server address>:<port>`) L'application prend en charge les protocoles de connexion serveur suivants : `tcp`, `udp`, `http` et `https`. • Ajoutez un certificat TLS (`/server-certificate=<path to the TLS certificate>`) • Définir le délai d'attente de connexion du serveur (`/timeout=<KUMA server connection timeout (s)>`) • Ajouter un conteneur crypto (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Configurez le délai de transmission des événements (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Afficher les paramètres actuels du module.

Autorisation	
`/login=<user name> /password=<password>`	Identifiants de compte utilisateur avec les autorisations requises pour la Protection par mot de passe.

Exemple

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. Exécution de l'analyse YARA

Exécution de la tâche *Lancer l'analyse YARA*. L'application analyse les fichiers et les objets à la recherche d'indicateurs d'attaques ciblées contre l'infrastructure informatique de l'entreprise à l'aide des bases de données de règles YARA. Les *règles YARA* sont des descriptions des signatures d'attaques ciblées et d'intrusions dans l'infrastructure informatique de l'entreprise que Kaspersky Endpoint Security utilise pour analyser les objets.

Pour lancer une analyse YARA, vous devez préparer des fichiers YARA décrivant les règles. Lors de la création de fichiers YARA, il faut tenir compte des exigences suivantes :

- Kaspersky Endpoint Security prend en charge les fichiers YARA présentant les extensions .YARA et .YAR qui respectent la norme ouverte YARA 4.2.3 pour la description des indicateurs de compromission.
- Seuls les fichiers avec des règles YARA peut être spécifié pour la tâche. La tâche *Lancer l'analyse YARA* ne prend pas en charge les autres types de règles.
- Si vous avez ajouté des fichiers YARA non pris en charge par Kaspersky Endpoint Security ou si les règles contiennent des erreurs de syntaxe, la tâche s'interrompt et le message d'erreur correspondant s'affiche.
- Les identifiants de tous les fichiers YARA utilisés dans une même tâche doivent être uniques. S'il y a des fichiers YARA avec le même identifiant, cela peut affecter les résultats de l'exécution de la tâche.
- L'analyse YARA est interrompue au bout de 128 correspondances avec les indicateurs décrits dans les règles YARA. Cette opération est nécessaire afin de limiter le nombre d'entrées dans le rapport d'analyse YARA, d'en faciliter l'analyse et d'éviter tout débordement dû à la présence de règles YARA formulées de manière imprécise qui peuvent générer un grand nombre de correspondances.

Kaspersky recommande de créer une règle par fichier YARA. Cette mesure permet d'améliorer la lisibilité des résultats de l'analyse.

Une analyse YARA peut prendre beaucoup de temps. En fonction de la taille du disque, des paramètres de la tâche et du nombre d'objets présents sur le disque, une analyse YARA peut durer de quelques minutes à plusieurs heures. L'application n'affiche pas d'indicateur de progression. Il n'est pas possible d'arrêter ni d'annuler une analyse YARA. Il est conseillé d'attendre les résultats de l'analyse YARA.

Syntaxe de la commande

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Fichiers YARA	
`<full path to the YARA file>`	Chemin d'accès complet au fichier YARA que vous souhaitez utiliser pour effectuer l'analyse. Vous pouvez indiquer les chemins d'accès à plusieurs fichiers YARA séparés par des espaces. Argument obligatoire si la valeur `/path=<path to the folder with YARA files>` n'est pas indiquée. Exemple : `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Chemin d'accès complet au dossier contenant les fichiers YARA que vous souhaitez utiliser pour effectuer l'analyse. Argument obligatoire si la valeur `<full path to the YARA file>` n'est pas indiquée. Exemple : `/path=C:\Users\Admin\Desktop\YARA`

Paramètres avancés	
`/fastScan=<on|off>`	Analyse YARA rapide. Pour chaque objet, l'application enregistre une occurrence de l'indicateur de détection. L'application masque également les doublons des indicateurs détectés dans le journal. L'analyse YARA rapide permet d'analyser plus rapidement les fichiers volumineux. Si le paramètre n'est pas défini, l'application exécute une analyse YARA standard. Dans ce mode, l'application enregistre les doublons des indicateurs détectés.
`/maxRules=<maximum number of scan rules>`	Limite du nombre de règles déclenchées uniques qui oblige l'application à arrêter l'analyse YARA lorsqu'elle est atteinte. Si la valeur de ce paramètre n'est pas précisée ou si `0` est spécifié, l'application analyse YARA sans limitations.
`/timeOut=<stop scan after the specified time in seconds>`	Combien de temps peut durer une analyse YARA, en secondes. À l'expiration de ce délai, l'application arrête l'analyse YARA. Si la valeur de ce paramètre n'est pas précisée ou si `0` est spécifié, l'application analyse YARA sans limitations.
`/recursive=<on|off>`	Cet argument lance une analyse récursive des sous-dossiers dans le cadre de l'analyse personnalisée `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Cet argument lance une analyse YARA des fichiers de la liste de dossiers indiquée. Vous pouvez indiquer plusieurs valeurs séparées par des espaces. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque de chemin d'accès à un dossier. Si le paramètre n'est pas défini, l'application effectue une analyse YARA de tous les disques locaux à l'exception des partages réseau, des disques dans le cloud et des supports amovibles.
`/scanMemory=<on|off>`	Analyser la mémoire de tous les processus en cours d'exécution.
`/scanProcess=<process name>`	Analyser la mémoire uniquement à la recherche de processus spécifiés. Indiquez les chemins d'accès complets, séparés par des espaces, aux fichiers exécutables des processus. Vous pouvez utiliser les caractères `*` et `?` pour saisir le masque.
`/maxSize=<file size in bytes>`	Limiter la taille du fichier pour l'analyse YARA. L'application ignore les fichiers volumineux.
`/includes=<list of objects to be scanned>>`	Modification de la zone d'analyse. Vous pouvez indiquer plusieurs valeurs séparées par des espaces. Les valeurs suivantes sont disponibles : • Nom du fichier • Extension de fichier La zone d'analyse doit être accompagnée du paramètre `/scanFolders`. Exemple : `/scanFolders C:\*.* /includes=*.exe *.dll` : l'application analyse tous les fichiers présentant les extensions .EXE et .DLL sur le disque C.
`/excludes=<list of objects to be scanned>`	Exclusion des fichiers de l'analyse YARA. Vous pouvez indiquer plusieurs valeurs séparées par des espaces. Les valeurs suivantes sont disponibles : • Chemin du fichier • Masque du chemin du fichier Les exclusions doivent être accompagnées du paramètre `/scanFolders`. Exemple : `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` : l'application ignore le fichier readme.txt, tous les fichiers du dossier C:\trusted ainsi que tous les fichiers portant l'extension .XML dans le dossier racine du disque C.
`/scanAutoruns=<on|off>`	Analyse YARA des objets de point d'exécution automatique.
`/excludeAutoruns=<list of autorun point areas to skip>`	Exclusion des objets de point d'exécution automatique de la zone d'analyse. Indiquez les chemins d'accès complets, séparés par des espaces, aux fichiers exécutables des processus. Vous pouvez utiliser les caractères `*` et `?` pour saisir le masque.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Si vous indiquez un chemin d'accès à un dossier, l'application enregistre les résultats de l'analyse à l'emplacement défini dans un fichier nommé yara_<nom de l'ordinateur>_<heure de fin de l'analyse>.txt. Si vous indiquez le chemin d'accès à un fichier TXT spécifique, l'application enregistre les résultats de l'analyse dans ce fichier. Par exemple, `/logFolder=C:\test` ou `/logFolder=C:\test\abc.txt`. Les résultats de l'analyse s'affichent en ligne de commande, que l'option `/logFolder` soit définie ou non.

Valeurs de retour de la commande :

- `-1` signifie que la commande n'est pas prise en charge par la version de l'application installée sur l'ordinateur.
- `0` signifie que la commande a été correctement exécutée.
- `1` signifie qu'un argument obligatoire n'a pas été transmis à la commande.
- `2` signifie qu'une erreur générale s'est produite.
- `4` signifie qu'il y a eu une erreur de syntaxe.
- `5` signifie qu'un ou plusieurs fichiers contenant les règles YARA spécifiées dans le paramètre sont introuvables.

Si la commande a été correctement exécutée (valeur de retour `0`) et que des indicateurs de compromission ont été détectés en cours de route, Kaspersky Endpoint Security envoie les informations suivantes sur le résultat de la tâche dans la ligne de commande :

`Started at <time>` `Finished at <time>`	Heure de début et heure de fin de l'analyse.
`Host name: <computer name>`	Le nom de l'ordinateur sur lequel l'objet a été détecté.
`Result: <error>`	Code d'erreur correspondant à l'erreur survenue lors de l'exécution de la tâche. S'il n'y a pas d'erreur, l'application affiche `0x00000000`.
`Comment: <comment text>`	Description de l'erreur survenue lors de l'exécution de la tâche. Par exemple, `Operation timeout`.
`Object Name:` ou `Process:` (lors de l'analyse de la mémoire vive)	Le nom de l'objet ou du processus sur lequel la règle YARA a été appliquée.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hachages de l'objet sur lequel la règle YARA a été appliquée.
`Rule Name`	Le nom de la règle YARA déclenchée.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Métadonnées définies dans la règle YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Correspondances trouvées au sein de l'objet qui remplissent les conditions de la règle YARA :
	• Décalage dans la mémoire de processus ou dans le fichier où une correspondance a été détectée (`Offset`).
	• Le nom de la chaîne correspondante dans la règle YARA (`String name`).
	• La chaîne correspondante dans la mémoire du processus ou dans le fichier (`String data`).

TELEMETRYFILTERS. Filtrage des événements à envoyer à KUMA

Par défaut, l'envoi d'événements au serveur KUMA est désactivé. Pour garantir le bon fonctionnement de KUMA, vous devez activer l'envoi de données télémétriques. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Pour améliorer les performances et optimiser la transmission des données vers le serveur KUMA, vous pouvez ajouter ou exclure manuellement des événements individuels de la télémétrie. Par exemple, vous pouvez exclure les événements Sysmon.

Vous pouvez exporter la liste des exclusions vers un fichier JSON à partir de la ligne de commande.

Si la commande ne contient que le nom du fichier vers lequel vous souhaitez exporter les paramètres, l'application place le fichier comme suit :

- Si le chemin d'accès à avp.com est ajouté à la variable système %PATH%, l'application place le fichier dans le dossier `C:\Windows\SysWOW64`.
- Si vous exécutez la commande à partir du dossier d'installation de l'application, l'exportation échouera, car l'autoprotection de l'application bloque la création d'un nouveau fichier dans le dossier de l'application. Pour exporter les paramètres de l'application dans un fichier, saisissez le chemin d'accès au fichier.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Opération	
`export`	Exportation des filtres d'événements à envoyer à KUMA.
`import`	Importation des filtres d'événements à envoyer à KUMA. Si des règles de filtrage des événements existent déjà sur l'ordinateur, Kaspersky Endpoint Security les remplace lors de l'importation.

Fichier pour l'exportation ou l'importation	
`<file name>`	Nom du fichier contenant les filtres d'événements à envoyer à KUMA. Vous pouvez également saisir le chemin d'accès au fichier. Vous pouvez exporter les filtres destinés à être envoyés à KUMA vers un fichier JSON.

Commandes d'administration du Light Agent

Vous pouvez gérer l'application en mode Light Agent pour protéger les environnements virtuels sur la ligne de commande. Vous pouvez administrer l'application en mode Light Agent si la gestion à l'aide de la console Kaspersky Security Center n'est pas possible. 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 <command>`.

Pour gérer l'application en mode Light Agent 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 <command> [options]
   ```

   En conséquence, Kaspersky Endpoint Security exécutera la commande.

L'application installée en mode Light Agent prend en charge presque toutes les Commandes AVP de l'application installée en mode Standard. En mode Light Agent, les tâches de mise à jour des bases antivirus et les tâches de gestion des clés de licence sont limitées.

KSVLAINFO. Définition du mode Light Agent

Détermination du mode Light Agent.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com KSVLAINFO
```

La commande affiche les informations suivantes sur la console :

- Mode Light Agent pour la protection des environnements virtuels : activé ou désactivé.

  Si le mode Light Agent est activé, l'application est utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent.

- Mode de protection VDI : activé ou désactivé.

  Le mode de protection VDI permet d'optimiser les performances de Kaspersky Endpoint Security sur les machines virtuelles non persistantes. Si le mode de protection VDI est activé, les mises à jour qui requièrent le redémarrage de la machine virtuelle protégée ne sont pas installées sur les machines virtuelles non persistantes. Lors de la récupération de mise à jour qui requiert le redémarrage, le Light Agent installée sur la machine virtuelle non persistante, envoie à Kaspersky Security Center un message sur la nécessité de mise à jour du modèle des machines virtuelles protégées.

- Type de machine virtuelle protégée : persistante ou non persistante.

- Rôle de la machine virtuelle protégée dans l'infrastructure virtuelle : serveur ou poste de travail.

- Identifiant : UUID.

VIISINFO. État de la connexion du Light Agent au Serveur d'intégration

Affichage des informations concernant la connexion du Light Agent au Serveur d'intégration.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com VIISINFO
```

La commande affiche les informations suivantes sur la console :

- Adresse du Serveur d'intégration avec lequel a été connecté le Light Agent.
- État de la connexion au Serveur d'intégration.
- Date et heure de la dernière connexion du Light Agent au Serveur d'intégration.

SVMINFO. État de la connexion du Light Agent au Serveur de protection

Affichage des informations sur la connexion du Light Agent au Serveur de protection.

Pour exécuter la commande, accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security. Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% et exécuter la commande sans naviguer jusqu'au dossier de l'application.

Syntaxe de la commande

```
avp.com SVMINFO
```

La commande affiche les informations suivantes sur la console :

- Adresse de la SVM à laquelle le Light Agent est connecté et emplacement de la SVM dans l'infrastructure virtuelle par rapport au Light Agent : locale ou non locale.
- Méthode de recherche des SVM utilisée par le Light Agent : à l'aide d'un Serveur d'intégration ou d'une liste personnalisée d'adresses de la SVM spécifiées manuellement.
- Liste des adresses SVM si la liste d'adresses SVM est sélectionnée comme méthode de recherche des SVM.
- Tag permettant de connecter le Light Agent à la SVM.
- Algorithme de sélection de la SVM : standard ou étendu. En cas d'utilisation de l'algorithme étendu de sélection de la SVM, le type de chemin d'accès à la SVM dans l'infrastructure virtuelle s'affiche également.
- État de protection de la connexion entre le Light Agent et le Serveur de protection.

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, `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security peut également afficher des informations supplémentaires sous la forme d'un code, par exemple, `error=8947906D` (cf. tableau ci-dessous).

Code d'erreur	Description
09479001	Cette clé est déjà utilisée
0947901D	La licence a expiré. La mise à jour des bases est inaccessible
89479002	Clé introuvable
89479003	Signature numérique corrompue ou introuvable
89479004	Les données sont corrompues
89479005	Le fichier clé est corrompu
89479006	La licence a expiré
89479007	Le fichier clé n'a pas été indiqué
89479008	Le fichier clé est incorrect
89479009	Impossible d'enregistrer les données
8947900A	Impossible de lire les 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	Les bases sont corrompues
89479011	Impossible d'appliquer un fichier clé incorrect pour ajouter une clé de réserve
89479012	Erreur système
89479013	La liste de refus des clés est corrompue
89479014	La signature du fichier ne correspond pas à la signature numérique de Kaspersky
89479015	Impossible d'utiliser une clé de licence d'essai comme clé de licence commerciale
89479016	La licence pour les tests bêta est requise pour utiliser la version bêta de l'application
89479017	Le fichier clé ne correspond pas à cette application. Impossible d'activer Kaspersky Endpoint Security for Windows à l'aide du fichier clé pour une autre application. Veuillez vérifier l'application installée
89479018	La clé de licence est bloquée par Kaspersky
89479019	L'application est déjà utilisée à l'aide d'une licence d'essai. Impossible d'ajouter à nouveau une clé pour une licence d'essai
8947901A	Le fichier clé est 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 correspondante a expiré
8947901E	La date de création ou d'application du fichier clé est incorrecte. Vérifiez la date de votre ordinateur
8947901F	Impossible d'ajouter une clé pour une licence d'essai si une autre licence similaire est toujours active
89479020	La liste de refus des clés est corrompue ou introuvable
89479021	La description des mises à jour est corrompue ou introuvable
89479022	La clé ne convient pas pour cette application
89479023	Impossible d'appliquer un fichier clé incorrect pour ajouter une clé de réserve
89479025	Une erreur s'est produite lors de l'envoi de la requête au serveur d'activation. Raisons probables : erreur de connexion Internet ou problèmes temporaires sur le serveur d'activation. Réessayez d'activer le programme à l'aide du code plus tard (dans 1 ou 2 heures). Si l'erreur se reproduit, contactez votre fournisseur d'accès Internet
89479026	Le code d'activation saisi dans la requête est invalide
89479027	Impossible d'obtenir l'état de l'objet

Code d'erreur	Description
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. Merci de vérifier votre date système
8947902A	La clé ne convient pas à cette application ou la licence a expiré
8947902B	Impossible d'obtenir le fichier clé. Le code d'activation saisi n'est pas correct
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	Une ressource indispensable sur le serveur d'activation est inaccessible. Le serveur d'activation a renvoyé l'erreur 404. Veuillez vérifier les paramètres de votre connexion Internet
89479030	Le serveur d'activation a renvoyé l'erreur 405
89479031	Le serveur d'activation a renvoyé l'erreur 406
89479032	Le serveur proxy requiert une authentification. Vérifier les paramètres du réseau
89479033	Le délai d'attente de la requête est dépassé
89479034	Le serveur d'activation a renvoyé l'erreur 409
89479035	Une ressource indispensable sur le serveur d'activation est inaccessible. Le serveur d'activation a renvoyé l'erreur 410. Veuillez vérifier les paramètres de votre connexion Internet
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 incorrecte de la passerelle. Veuillez vérifier les paramètres du réseau
8947903F	La ressource est temporairement inaccessible
89479040	La durée d'attente de la réponse de la passerelle est écoulée. Vérifiez les paramètres de réseau
89479041	Le protocole n'est pas pris en charge par le serveur
89479043	Erreur HTTP inconnue
89479044	Identifiant 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

Code d'erreur	Description
89479053	La licence correspondant à la clé ajoutée a déjà expiré
89479054	La date système de l'ordinateur est incorrecte. Veuillez vérifier la date de l'ordinateur
89479055	La licence d'essai a expiré
89479056	La période d'activation 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 d'essai comme clé de licence commerciale
8947905C	Code d'activation requis
89479062	Impossible de se connecter au serveur d'activation
89479064	Le serveur d'activation est inaccessible. Vérifiez les paramètres de connexion Internet et retentez d'activer l'application
89479065	Licence expirée
89479066	Impossible de remplacer la clé active par une clé de licence expirée
89479067	Impossible d'ajouter une clé de réserve si la licence correspondante expire avant la licence actuelle
89479068	Clé mise à jour pour abonnement manquante
8947906A	Le code d'activation est incorrect
8947906B	La clé est déjà active
8947906C	Les types de licence qui correspondent aux clés actives et de réserve ne correspondent pas
8947906D	La licence ne prend pas en charge le module
8947906E	Impossible d'ajouter une clé d'abonnement en tant que clé de réserve
89479213	Erreur générale du niveau de transport
89479214	Impossible de se connecter au serveur d'activation
89479215	Format d'adresse Internet incorrect
89479216	Impossible de transformer l'adresse du serveur proxy
89479217	Impossible de résoudre l'adresse du serveur. Vérifiez les paramètres de connexion Internet
89479218	La tentative de connexion au serveur s'est soldée sur une erreur
89479219	Accès interdit à distance
8947921A	Le délai de connexion de l'opération est dépassé
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
89479221	Erreur d'envoi des données
89479222	Erreur de réception de données
89479223	Problème lié au certificat SSL
89479224	Problème lié au chiffrement SSL
89479225	Problème lié au centre de certification SSL
89479226	Contenu du paquet réseau incorrect

Code d'erreur	Description
89479227	Refus d'accès du compte
89479228	Fichier de certificat SSL incorrect
89479229	Impossible de terminer la connexion SSL
8947922A	Erreur réitérée
8947922B	Fichier des certificats révoqués incorrect
8947922C	Erreur de demande du certificat SSL
89479401	Erreur inconnue du serveur
89479402	Erreur interne du serveur
89479403	La clé pour le code d'activation saisi est absente
89479404	La clé active est bloquée
89479405	Les paramètres obligatoires de la demande d'activation sont absents
89479406	Numéro ou mot de passe du client incorrect
89479407	Le code d'activation est incorrect
89479408	Le code d'activation ne correspond pas à cette application. Impossible d'activer Kaspersky Endpoint Security for Windows à l'aide du code d'activation pour une autre application. Veuillez vérifier l'application installée
89479409	Code d'activation requis
8947940B	La période d'activation a expiré
8947940C	Le nombre d'activations de l'application à l'aide de ce code d'activation est dépassé
8947940D	Format de l'identifiant de la demande incorrect
8947940E	Le code d'activation est déjà utilisé
8947940F	Impossible de renouveler le code d'activation de réserve
89479410	Le code d'activation ne correspond pas à cette région
89479411	Ce code d'activation n'est pas destiné à la version localisée de l'application utilisée
89479412	Le code d'activation est conçu pour la nouvelle version de cette application. Pour activer la version installée de l'application, il faut obtenir un autre code d'activation
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 serveur d'activation de version 1.0 est requis
89479418	Le format du code d'activation est incorrect
89479419	L'heure sur l'ordinateur n'est pas synchronisée avec l'heure sur le serveur d'activation
8947941A	Version de l'application incorrecte
8947941B	L'abonnement a expiré
8947941C	Le seuil du nombre d'activations est dépassé
8947941D	Signature du ticket incorrecte
8947941E	Des données complémentaires sont requises
8947941F	La vérification des données de l'utilisateur s'est soldée sur une erreur
89479420	L'abonnement n'est pas actif
89479421	Des opérations de maintenance sont actuellement effectuées sur le serveur d'activation

Code d'erreur	Description
89479501	Erreur imprévue
89479502	Un paramètre inadmissible a été transmis. Par exemple, la liste des adresses des serveurs d'activation est vide
89479503	Le code d'activation est incorrect (la somme de contrôle est incorrecte)
89479504	L'identifiant d'utilisateur est incorrect
89479505	Le mot de passe de l'utilisateur est incorrect
89479506	Le serveur d'activation a renvoyé une réponse incorrecte
89479507	L'exécution de la demande d'activation a été 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 `START`, `STOP`, `STATUS`, `STATISTICS` et `EXPORT`. 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.
- `AntiCryptor`
- `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
- `LogInspector` : Inspection des journaux
- `Mail_Monitoring` ou `EM` : Protection contre les menaces par emails
- `Rollback` – Annulation de la mise à jour (le profil ne peut pas être appliqué si l'application est installée en mode Light Agent)

- `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 (le profil ne peut pas être appliqué si l'application est installée en mode Light Agent)
- `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.

Préparation de l'installation de l'application avec prise en charge de l'API REST

L'interaction sécurisée de Kaspersky Endpoint Security avec le client REST nécessite la configuration de l'identification des requêtes. Pour ce faire, vous devez installer un certificat et signer ensuite la charge utile de chaque demande.

Pour créer un certificat, vous pouvez utiliser, par exemple, OpenSSL.

Exemple :

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilisez l'algorithme de chiffrement RSA avec une longueur de clé de 2048 bits ou plus.

Ainsi, vous obtiendrez un certificat `cert.pem` et une clé privée `key.pem`.

Installation de l'application avec prise en charge de l'API REST

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=<user name>`

     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 destiné à l'administration de l'application via l'API REST. Le port 6782 est utilisé par défaut. Assurez-vous que le port est disponible. Paramètre facultatif.

   - `RESTAPI_Certificate=<path to certificate>`

     Certificat pour l'identification des demandes (par exemple, `RESTAPI_Certificate=C:\cert.pem`).

     Vous pouvez installer le certificat après avoir installé l'application ou mettre à jour le certificat après son expiration.

     Installation d'un certificat pour l'identification des requêtes d'API REST

     1. Désactiver l'Autodéfense de Kaspersky Endpoint Security

        Le mécanisme d'Autodéfense empêche la modification et la suppression des fichiers de l'application sur le disque dur, des processus dans la mémoire et des clés de la base de registre système.

     2. Accédez à la clé de registre qui contient les paramètres de l'API REST : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`

     3. Saisissez le chemin d'accès au certificat, par exemple, `Certificate = C:\Folder\cert.pem`.

     4. Activez l'Autodéfense de Kaspersky Endpoint Security.

     5. Redémarrez l'application.

   - `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.

Exemple :
```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /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
```

Si vous avez installé l'application avec la prise en charge de l'API REST, Kaspersky Endpoint Security crée automatiquement une règle d'autorisation dans les paramètres du Contrôle Internet pour l'accès aux ressources Internet (*Règle de service pour l'API REST*). Cette règle est nécessaire pour permettre au client REST d'accéder à Kaspersky Endpoint Security à tout moment. Par exemple, si vous avez restreint l'accès des utilisateurs aux ressources Internet, cela n'affectera pas la gestion de l'application via l'API REST. Nous vous recommandons de ne pas supprimer la règle ni de modifier les paramètres de la *Règle de service pour l'API REST*. Si vous avez supprimé la règle, Kaspersky Endpoint Security la restaurera après le redémarrage de l'application.

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. Utilisez la structure de paramètres obtenue en réponse à la requête GET.

   Exemple :
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Enregistrez les paramètres de l'application (le payload) dans un JSON (payload.json).

5. Signez le JSON au format PKCS7.

   Exemple :
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
   ```

   Ainsi, vous obtenez un fichier signé contenant la charge utile de la requête (`signed_payload.pem`).

6. Modifiez les paramètres de l'application. Pour ce faire, envoyez une demande POST et joignez-y le fichier signé à la charge utile de la requête (`signed_payload.pem`).

L'application applique les nouveaux paramètres et envoie une réponse contenant les résultats de la configuration de l'application (la réponse peut être vide). Vous pouvez vérifier que les paramètres sont mis à jour en utilisant une requête GET.

Sources d'informations sur l'application

Cette section décrit les différentes sources d'informations sur l'application.

Vous pouvez choisir la source d'informations la plus pratique en fonction de l'importance et de l'urgence de votre problème.

Page Kaspersky Endpoint Security sur le site de Kaspersky

Sur la page de Kaspersky Endpoint Security, vous pouvez afficher des informations générales sur l'application ainsi que ses fonctions et caractéristiques.

La page de Kaspersky Endpoint Security contient un lien vers la boutique en ligne. Là, vous pouvez acheter ou renouveler l'application.

Page de Kaspersky Endpoint Security dans la Base de connaissances

La *Base de connaissances* est une section du site du support technique.

Sur la page de Kaspersky Endpoint Security dans la Base de connaissances, vous pouvez lire des articles qui fournissent des informations utiles, des recommandations ainsi que des réponses aux questions fréquemment posées concernant l'achat, l'installation et l'utilisation de l'application.

Les articles de la Base de connaissances permettent de répondre non seulement aux questions concernant Kaspersky Endpoint Security, mais également d'autres applications Kaspersky. Les articles de la Base de connaissances peuvent également contenir de nouveaux renseignements du support technique.

Discussion sur les applications Kaspersky dans le Forum

Si votre question ne requiert pas de réponse urgente, vous pouvez en discuter avec les experts de Kaspersky et d'autres utilisateurs dans notre Forum.

Dans le Forum, vous pouvez afficher les sujets existants, publier vos propres commentaires et créer des sujets de discussion.

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 trace 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 (inaccessible via les moyens standards de l'interface utilisateur) d'utilisation des modules spécifiques de l'application.
- 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. Si vous modifiez vous-même les paramètres des applications d'une manière qui n'est pas décrite dans l'aide en ligne ni dans les recommandations du Support Technique, vous risquez de provoquer des ralentissements et des pannes du système d'exploitation, de réduire le niveau de protection de votre ordinateur et de nuire à la disponibilité ainsi qu'à 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.14.2\Traces`.

Les fichiers de traçage sont nommés comme suit : `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.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.

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 modules 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 sont nommés comme suit : `KES<14.2_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 `shellex.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 Web Console, dans le dossier `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\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) ;
- Nom d'utilisateur et 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 des opérations de l'application

Le *traçage 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. Au cours du processus de traçage, l'application crée un ensemble de fichiers avec les données relatives au fonctionnement des différents modules d'application (par exemple, SRV.log, WD.log et autres).

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 .
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Outils de support**.
3. Utilisez le bouton **Activer le traçage des applications** pour activer ou désactiver le traçage du fonctionnement de l'application.
4. Dans la liste déroulante **Traçage**, sélectionnez un mode de traçage de l'application :
   - **Avec limitation de taille**. Enregistrer les résultats du traçage dans un nombre limité d'ensembles 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 d'ensembles de fichiers pour la rotation et la taille maximum de chaque ensemble de fichiers.

     Par défaut, l'application enregistre cinq ensembles de fichiers de traçage. La taille de chaque ensemble de fichiers est de 3 072 Mo. De cette façon, vous avez besoin de 15 Go d'espace libre sur le disque pour enregistrer les fichiers de traçage.
   - **Sans limitation**. Enregistrer un fichier de traçage (sans limite de taille).

5. Choisissez le niveau de traçage dans la liste déroulante **Niveau** :

   - **Normal** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application (option par défaut).

   - **Détaillé** signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.

   Des niveaux de traçage supplémentaires sont disponibles si vous gérez les paramètres de traçage des applications via la ligne de commande. 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**.

   Si le traçage des applications a été activé via la ligne de commande et qu'un niveau de traçage autre que **Normal** ou **Détaillé** a été défini, la liste déroulante **Niveau** est réglée sur **Normal**.

6. Pour arrêter le processus de traçage, retournez à la fenêtre **Outils de support** 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 relatifs au fonctionnement de l'application sont créés dans le dossier `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Une fois que les fichiers de traçage ont été créés, envoyez-les au Support Technique de Kaspersky.

Kaspersky Endpoint Security supprime automatiquement les fichiers de traçage quand l'application est supprimée. Vous pouvez également les supprimer manuellement. Pour ce faire, vous devez désactiver le traçage et arrêter l'application.

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. *Le traçage des performances est* enregistrement des événements dans le journal par l'application dans le but de diagnostiquer les 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 es 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 .

2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Outils de support**.

3. Utilisez le bouton **Activer le traçage des performances** pour activer ou désactiver le traçage des performances de l'application.

4. Dans la liste déroulante **Traçage**, sélectionnez un mode de traçage de l'application :

   - **Avec limitation de taille**. 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.

   - **Sans limitation**. 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 processus du système d'exploitation les plus importants 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 Outils de support et désactivez le traçage.

Le fichier de traçage des performances est créé dans le dossier `%ProgramData%\Kaspersky Lab\KES.14.2\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.14.2\Traces`.

Comment activer l'enregistrement des fichiers dump dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Données pour le débogage**.
5. Dans la fenêtre qui s'ouvre, cochez la case **Activer l'enregistrement des fichiers de vidage** pour activer ou désactiver l'enregistrement des fichiers dump de l'application.
6. Enregistrez vos modifications.

Comment activer l'enregistrement des fichiers dump dans Web Console et Cloud Console

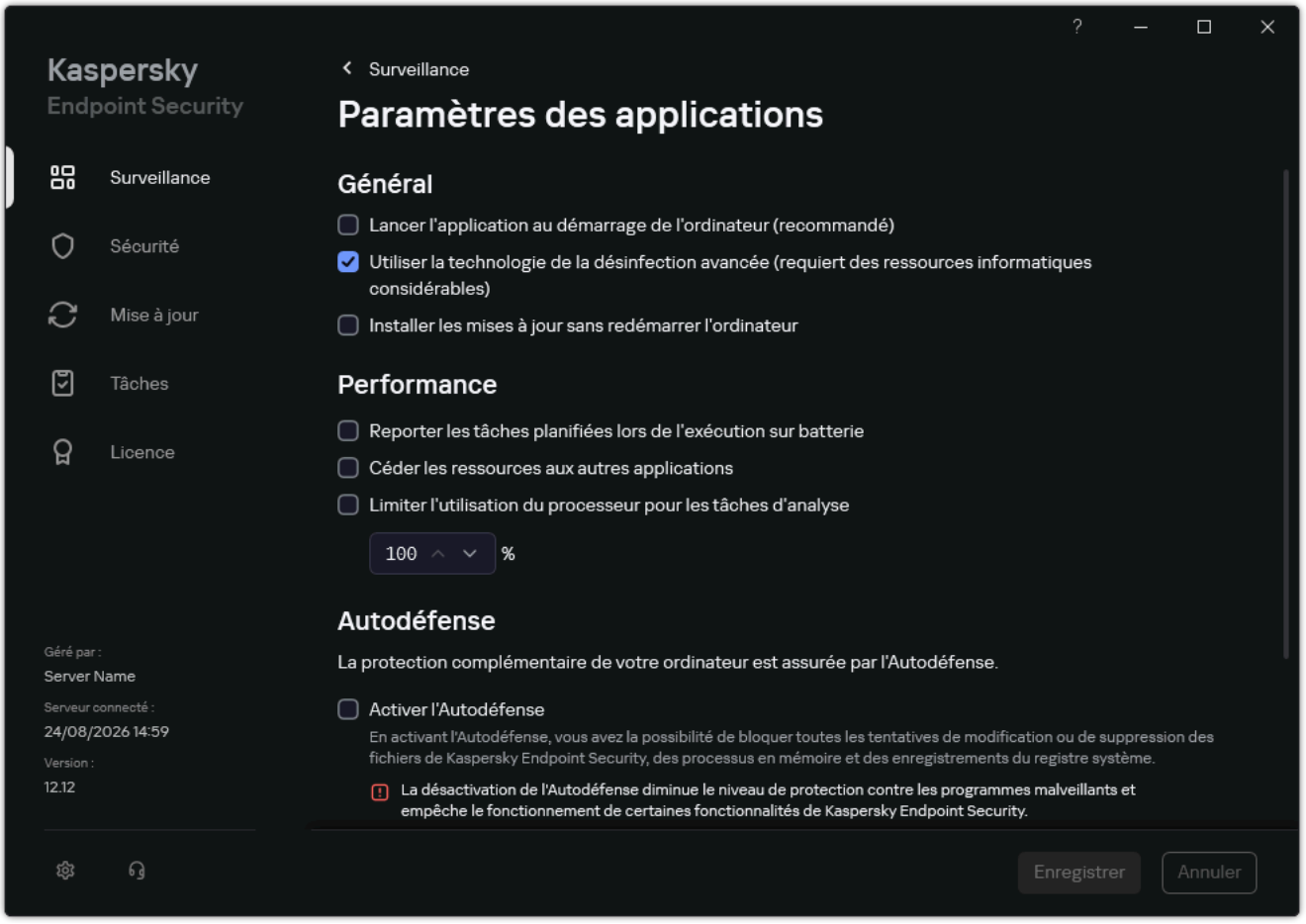
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Assistance technique**.
5. Dans le groupe **Données pour le débogage**, utilisez la case **Enregistrement des fichiers dump ACTIVÉ** pour activer ou désactiver l'enregistrement des fichiers de vidage de l'application.
6. Enregistrez vos modifications.

Comment activer l'enregistrement des fichiers dump 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

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.

Comment activer la protection des fichiers dump et des fichiers de traçage dans la Console d'administration (MMC)

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres généraux** → **Paramètres des applications**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Données pour le débogage**.
5. Dans la fenêtre qui s'ouvre, cochez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers.
6. Enregistrez vos modifications.

Comment activer la protection des fichiers dump et des fichiers de traçage dans Web Console et Cloud Console

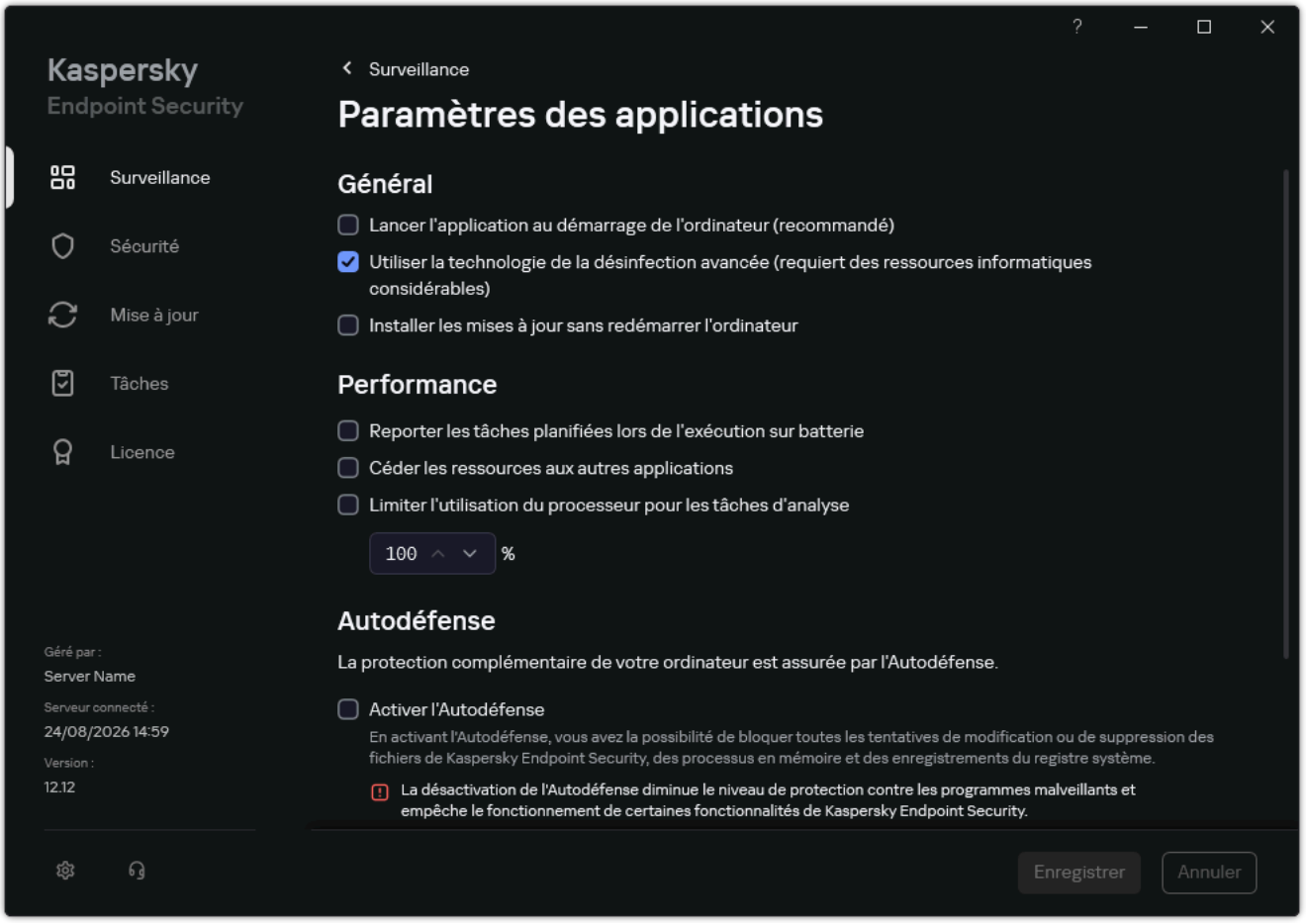
1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres généraux** → **Assistance technique**.
5. Dans le groupe **Données pour le débogage**, utilisez la case **Protection des fichiers de vidage et de traçage ACTIVÉE** pour activer ou désactiver la protection des fichiers.
6. Enregistrez vos modifications.

Comment activer la protection des fichiers dump et des fichiers de traçage 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** → **Paramètres des applications**.



Paramètres de Kaspersky Endpoint Security for Windows

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.

Obtention des données relatives au système d'exploitation (Kaspersky Get System Info)

Après l'installation de l'application Kaspersky Endpoint Security, le système d'exploitation ou l'application peuvent ne pas fonctionner correctement. Il existe un conflit entre l'application et le logiciel ou les pilotes des modules de l'ordinateur.

Afin de déterminer la cause du problème, le Support technique de Kaspersky a besoin d'un rapport créé par l'utilitaire Kaspersky Get System Info (ci-après, GSI). Pour en savoir plus sur l'utilisation de cet utilitaire, consultez la Base des connaissances de Kaspersky.

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.

- Les particularités de la prise en charge des systèmes d'exploitation Microsoft Windows 11 et Microsoft Windows Server 2022 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.

- 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).

- Lors de la suppression des modules individuels de l'application (par exemple, à l'aide de la tâche *Modification de la sélection des modules de l'application*), un redémarrage de l'ordinateur peut être nécessaire.

- Dans les propriétés de la tâche *Modification de la sélection des modules de l'application*, lors du changement de mode d'installation (**Mode séparé** / **Mode combiné**), la synchronisation de l'ensemble des modules entre les modes n'est pas prise en charge. L'application synchronise l'ensemble de modules entre les modes une fois que vous avez rouvert les propriétés de la tâche.

- 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.

- Si vous avez annulé la suppression de Kaspersky Endpoint Security, lancez la récupération de l'application après le redémarrage de l'ordinateur.

- L'application requiert Microsoft .NET Framework 4.0 ou une version ultérieure. Microsoft .NET Framework 4.6.1 présente des vulnérabilités. Si vous utilisez Microsoft .NET Framework 4.6.1, vous devez installer les mises à jour de sécurité. Pour en savoir plus sur les mises à jour de sécurité de Microsoft .NET Framework, consultez le site du Support technique de Microsoft.

- 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 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.

- 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.

- Lors de l'installation de Kaspersky Endpoint Security for Windows sur un serveur sur lequel sont installées les applications Kaspersky Security for Windows Server (KSWS) et Windows Defender, vous devez redémarrer le système. Un redémarrage du système est requis même si vous avez activé l'installation des applications sans redémarrage du système. Windows Defender pour Windows Server est inclus dans la liste des logiciels incompatibles avec Kaspersky Endpoint Security for Windows. Avant d'installer l'application, le programme d'installation supprime Windows Defender for Windows Server. La suppression d'un logiciel incompatible rend nécessaire un redémarrage du système.

- Avant d'installer Kaspersky Endpoint Security for Windows (KES) sur un serveur sur lequel Kaspersky Security for Windows Server (KSWS) est installé, vous devez désactiver la protection par mot de passe de KSWS. Après avoir migré de KSWS vers KES, activez la protection par mot de passe dans les paramètres de l'application.

- Pour installer l'application sur des ordinateurs fonctionnant sous Windows 7 ou Windows Server 2008 R2 sur lesquels le logiciel Veeam Backup & Replication est déployé, vous devrez peut-être redémarrer votre ordinateur et relancer l'installation.

- La migration de Kaspersky Small Office Security (KSOS) vers Kaspersky Endpoint Security (KES) avec le module Protection par mot de passe activé est disponible à partir de KSOS version 21.16.*.*. Pour migrer des versions antérieures de KSOS, vous devez désactiver le module Protection par mot de passe ou supprimer manuellement KSOS. La migration de KSOS vers KES avec un module Protection par mot de passe désactivé s'effectue correctement.

- Vous ne pouvez pas installer Kaspersky Endpoint Security sur un disque amovible de démarrage. Lors de l'installation, Kaspersky Endpoint Security affiche le message d'erreur suivant : *Vous avez choisi un dossier ou un disque incorrect. L'application doit être installée sur un disque dur local*. Si vous parvenez à installer l'application sur un disque amovible à l'aide d'outils tiers, il se peut que le système d'exploitation plante (BSOD) pendant le processus de démarrage. Cela signifie que Kaspersky Endpoint Security ne prend pas en charge Windows To Go ni les solutions similaires. Pour analyser un ordinateur à partir d'un disque amovible, vous pouvez utiliser l'application gratuite Kaspersky Rescue Disk.

- L'installation de Kaspersky Endpoint Security avec des modules réseau sur un serveur terminal avec des sessions RDP multi-utilisateurs implique certaines considérations particulières. Le système d'exploitation force la fermeture de toutes les sessions utilisateur après la fin de la session administrateur. Pour vous connecter au serveur du terminal, vous devez redémarrer le serveur ou vous connecter au système localement. Ce comportement est dicté par les particularités du fonctionnement du système d'exploitation Windows.

- Si les plug-ins Internet Kaspersky Endpoint Security for Windows (version 12.11.0.2004) et Kaspersky Endpoint Security for Linux (version 12.4.0.1354) sont installés dans Kaspersky Security Center 16.0 ou Kaspersky Security Center 16.1, la mise à jour du plug-in Internet Kaspersky Endpoint Security for Windows vers la version 12.11.0.6004 peut entraîner des dysfonctionnements dans les stratégies de Kaspersky Endpoint Security for Linux.

  Solution possible : accédez à la fenêtre **Configuration** → **Plug-ins Web** et supprimez les plug-ins Internet Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux et Unified Protection and Management Plug-in de la liste. Installez ensuite le plug-in Internet Kaspersky Endpoint Security for Linux, puis le plug-in Internet Kaspersky Endpoint Security for Windows.

- Dans Web Console, la liste des modules ne s'affiche pas correctement dans les propriétés du paquet d'installation de Kaspersky Endpoint Security 12.11 for Windows. La protection contre le chiffrement, module distinct, n'est pas disponible dans cette version de l'application. La protection des dossiers partagés contre la fonctionnalité de chiffrement externe est intégrée dans le module Détection comportementale. Dans Kaspersky Endpoint Security 12.12 for Windows, cette fonctionnalité est un module à part. En même temps, dans la Console d'administration (MMC), la liste des modules s'affiche correctement.

- Avec la version 7.0 ou ultérieure du plug-in Internet, la liste des modules sélectionnés par défaut pour l'installation ne s'affiche pas correctement dans les propriétés du paquet d'installation de Kaspersky Endpoint Security 14.1 et des versions antérieures. Si cette liste n'est pas modifiée lors de la création du paquet d'installation, l'application sera installée avec l'ensemble de modules par défaut défini pour la version correspondante de l'application.

Mise à jour de l'application

- 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 jour de Kaspersky Endpoint Security 11.0.0 ou 11.0.1 for Windows, les paramètres de la planification des tâches locales pour les tâches *Mise à jour des bases et des modules d'application*, *Analyse des zones critiques*, *Analyse personnalisée* et *Vérification de l'intégrité de l'application* ne sont pas enregistrés.

- Sur les ordinateurs fonctionnant sous Windows 10 version 1903 et 1909, les mises à jour 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 jour, il vous est conseillé de supprimer le module de chiffrement des fichiers.

- L'application nécessite Microsoft .NET Framework 4.0 ou une version ultérieure. Microsoft .NET Framework 4.6.1 présente des vulnérabilités. Si vous utilisez Microsoft .NET Framework 4.6.1, vous devez installer les mises à jour de sécurité. Pour en savoir plus sur les mises à jour de sécurité de Microsoft .NET Framework, consultez le site du Support technique de Microsoft.

- Lors de la mise à jour de Kaspersky Endpoint Security, l'application désactive l'utilisation de KSN jusqu'à ce que la Déclaration de Kaspersky Security Network soit acceptée. De plus, l'état de l'ordinateur peut être remplacé par *Critique* dans Kaspersky Security Center ; l'événement *Serveurs de KSN indisponibles* est reçu. Si vous utilisez Kaspersky Managed Detection and Response, vous recevrez des événements concernant les violations du fonctionnement de la solution. L'utilisation de KSN est nécessaire pour le fonctionnement de Kaspersky Managed Detection and Response. Kaspersky Endpoint Security permet l'utilisation de KSN après avoir appliqué la stratégie dans laquelle l'administrateur accepte les conditions d'utilisation de KSN. Une fois la Déclaration de Kaspersky Security Network acceptée, Kaspersky Endpoint Security reprend son fonctionnement.

- Une fois que vous aurez mis à jour Kaspersky Endpoint Security vers la version 11.10.0 ou une version ultérieure sans redémarrage, deux applications Kaspersky Endpoint Security seront installées sur l'ordinateur. Ne supprimez pas manuellement la version précédente de l'application. La version précédente sera supprimée automatiquement lors du redémarrage de l'ordinateur.

- Après la mise à jour de Kaspersky Endpoint Security sur un ordinateur fonctionnant sous Microsoft Windows 11, le menu contextuel du fichier peut afficher des éléments pour les versions précédentes et nouvelles de l'application. Redémarrez votre ordinateur deux fois pour garantir le bon fonctionnement du menu contextuel du fichier.

- Si l'autodéfense de l'application est désactivée et que tous les adaptateurs réseau sont arrêtés, les modules réseau de l'application ne fonctionneront pas entre la fin de la mise à jour de l'application et le redémarrage de l'ordinateur. Les modules réseau de l'application incluent la Protection contre les menaces Internet, la Protection contre les menaces par emails, la Protection contre les menaces réseau, le Pare-feu, la Prévention des intrusions et le Contrôle Internet. Redémarrez l'ordinateur pour que l'application fonctionne correctement.

- Le module Protection BadUSB ne fonctionne pas entre la fin de la mise à jour de l'application et le redémarrage de l'ordinateur. Redémarrez l'ordinateur pour que l'application fonctionne correctement.

- L'application ne peut pas être mise à jour si le processus de mise à jour précédent n'est pas terminé. Redémarrez l'ordinateur pour que l'application fonctionne correctement.

- Après la mise à jour de l'application à partir de versions antérieures à Kaspersky Endpoint Security 11 for Windows, l'ordinateur doit être redémarré.

- Si vous administrez Kaspersky Endpoint Security à l'aide de Kaspersky Security Center Cloud Console, la mise à jour locale de l'application n'est pas autorisée. Lors de la mise à jour locale de l'application, il n'est pas possible d'accepter le contrat de traitement des données pour Kaspersky Security Center Cloud Console.

Prise en charge de l'architecture ARM

- L'installation de Kaspersky Endpoint Security en mode Light Agent sur des machines virtuelles basées sur l'architecture ARM n'est pas prise en charge.

- Kaspersky Disk Encryption n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

- Le chiffrement des fichiers n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

- Le chiffrement des disques amovibles n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

- Sur les ordinateurs exécutant Windows 11 pour Arm64, EDR Agent n'est pas compatible avec Bitdefender Endpoint Security Tools.

- Les fonctionnalités de protection du signal audio et d'accès à la webcam ne sont pas prises en charge sur les ordinateurs équipés d'un processeur ARM.

- Sur les ordinateurs équipés d'un processeur ARM, l'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2016, Outlook 2021, Outlook 2024 et Outlook 365 pour ARM64.

- Kaspersky Endpoint Security n'envoie pas les objets destinés à l'architecture ARM à Kaspersky Sandbox.

- La gestion de l'impression n'est pas prise en charge sur les ordinateurs basés sur l'architecture ARM.

- Sur les ordinateurs basés sur l'architecture ARM, la tâche *Analyse IOC* prend en charge uniquement les fichiers d'email provenant des clients de messagerie suivants : les versions 32 bits et 64 bits d'Outlook 2016, ainsi que les versions 2021, 2024 et 365 d'Outlook pour Arm64.

- Sur les ordinateurs exécutant Windows 11 pour Arm64, l'authentification par jeton peut être indisponible, car le système d'exploitation ne parvient pas à détecter de certificat valide sur le jeton. Ce comportement est dû à la manière dont le système d'exploitation interagit avec le logiciel du jeton. Par exemple, il se peut que le système d'exploitation ne dispose pas des pilotes nécessaires au fonctionnement du jeton. Dans ce cas, Kaspersky Endpoint Security ne prend pas non plus en charge l'authentification par jeton (Protection par mot de passe). Vous pouvez utiliser d'autres méthodes d'authentification, telles que les identifiants de l'utilisateur.

Prise en charge de plateformes de serveurs

- Sur les serveurs où la *déduplication des données* est activée, vous devez ajouter le fichier fsdmhost.exe à la liste des applications de confiance. Cela permet d'optimiser les performances de l'application et d'éviter une charge excessive sur le processeur.

- Prise en charge du système de fichiers ReFS avec des restrictions :

  - Kaspersky Endpoint Security peut traiter les événements de désinfection des menaces de façon incorrecte. Par exemple, si l'application a supprimé un fichier malveillant, le rapport peut contenir une entrée L'objet n'a pas été traité. En même temps, Kaspersky Endpoint Security désinfecte les menaces en fonction des paramètres de l'application. Kaspersky Endpoint Security peut également créer un doublon de l'événement *L'objet sera désinfecté au redémarrage* pour le même objet.

  - La Protection contre les fichiers malicieux peut ignorer certaines menaces. En même temps, l'Analyse des logiciels malveillants fonctionne correctement.

  - Après le lancement de la tâche *Analyse des logiciels malveillants*, les exclusions d'analyse ajoutées avec iChecker sont réinitialisées lorsque le serveur est redémarré.

  - La technologie iSwift n'est pas prise en charge. Kaspersky Endpoint Security ne tient pas compte des exclusions d'analyse ajoutées à l'aide de la technologie iSwift.

  - 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.

  - Kaspersky Endpoint Security peut afficher de manière incorrecte les notifications de désinfection des menaces. Par exemple, l'application peut afficher une notification de menace pour une menace précédemment désinfectée.

- Pas de prise en charge du chiffrement des fichiers et de la technologie de chiffrement du disque sur les plateformes pour serveurs. Parallèlement, Kaspersky Endpoint Security peut traiter de manière incorrecte les événements de chiffrement des données.

- Les systèmes d'exploitation des serveurs n'affichent aucun avertissement concernant la nécessité de procéder à une désinfection avancée.

- Le systèmes 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.

- Kaspersky Endpoint Security installé sur un serveur sur lequel est déployé Microsoft Data Protection Manager (DPM) peut provoquer un dysfonctionnement de DPM. Ce problème est lié aux limitations du fonctionnement de DPM. Pour éliminer les dysfonctionnements, vous devez ajouter les disques locaux du serveur aux exclusions pour le module Protection contre les fichiers malicieux et les tâches *Analyse des logiciels malveillants*.

- Le mode Server Core est pris en charge avec des limitations :
  - L'interface utilisateur graphique locale n'est pas disponible, y compris les notifications, les notifications contextuelles et d'autres commandes d'interface. L'application ne peut pas afficher les fenêtres d'invite, y compris les fenêtres suivantes :
    - Demande de confirmation de la mise à jour de la version de l'application et du module ;
    - Redémarrage de l'ordinateur requis ;
    - Demande d'informations d'authentification sur le serveur proxy ;
    - Demande d'accès à un appareil (contrôle des appareils).
  - Les modules suivants ne sont pas disponibles : Protection contre les menaces Internet, Protection contre les menaces par emails, Contrôle Internet, Protection BadUSB.
  - Anti-Bridging n'est pas disponible.
  - Vous ne pouvez accepter la déclaration de Kaspersky Security Network que dans la stratégie d'application de la console de Kaspersky Security Center.
  - Le chiffrement de disque BitLocker n'est disponible qu'avec Trusted Platform Module (TPM). Un PIN / mot de passe ne peut pas être utilisé pour le chiffrement, car l'application est incapable d'afficher la fenêtre d'invite du mot de passe pour l'authentification avant le démarrage. Si le système d'exploitation prend en charge la norme FIPS (Federal Information Processing Standard), connectez un disque amovible pour enregistrer la clé de chiffrement avant de commencer à chiffrer le disque.

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.
- Les systèmes d'exploitation Windows 10 Enterprise multisession et Windows 11 Enterprise multisession sont pris en charge avec les restrictions suivantes :
  - Kaspersky Endpoint Security désinfecte les menaces actives sans en informer l'utilisateur, tout comme lors de la désinfection des menaces actives sur les serveurs. Comme le système d'exploitation continue de fonctionner en mode multisession, les autres utilisateurs actifs peuvent perdre leurs données si la menace n'est pas immédiatement résolue.
  - 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 sur laquelle Kaspersky Endpoint Security for Windows et l'Agent d'administration de Kaspersky Security Center sont préinstallés, ajoutez les types d'exclusions suivants au fichier de configuration :

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  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.

- Kaspersky Endpoint Security est compatible avec l'hyperviseur VMware ESXi avec les restrictions suivantes :

  - Kaspersky Endpoint Security peut être incompatible avec les pilotes Guest Introspection (vnetWFP.sys, vnetFLT.sys et autres). Pour résoudre les problèmes d'incompatibilité, mettez à jour les pilotes vers la dernière version ou désinstallez les pilotes.

  - Dans certains cas, les tentatives de suppression en toute sécurité d'un disque amovible sur une machine virtuelle peuvent échouer. Essayez de déconnecter de nouveau l'appareil en toute sécurité.

- L'installation de Kaspersky Endpoint Security sur des machines virtuelles avec l'agent Citrix VDA peut entraîner une erreur de compatibilité. Cela s'explique par la compatibilité limitée de Citrix Provisioning Services avec les solutions antivirus. Pour en savoir plus sur les bonnes pratiques d'utilisation des solutions antivirus avec Citrix Provisioning Services, consultez le site d'assistance de Citrix.

- Kaspersky Endpoint Security ignore l'analyse du disque amovible si le disque est connecté à la machine virtuelle sur l'hyperviseur Citrix (la tâche *Analyse des disques amovibles*). Sur de tels appareils, le système d'exploitation détecte le disque amovible connecté comme un disque réseau. Dans de tels cas, vous pouvez utiliser la tâche *Analyse personnalisée*. Le comportement de l'application en mode standard et en mode Light Agent est le même.

- Si Kaspersky Endpoint Security est installé sur une machine virtuelle dans une infrastructure qui utilise la technologie Citrix App Layering, les fichiers détectés par l'application comme étant infectés avec l'état *L'objet sera supprimé au redémarrage* ne seront pas automatiquement supprimés lors du redémarrage de la machine virtuelle.

  Pour supprimer ces fichiers, vous devez monter le fichier VHDX contenant la User Layer sur l'ordinateur de l'administrateur de Citrix App Layering, puis lancer une analyse des logiciels malveillants sur le disque monté.

- Avant de créer un instantané de catégorie principale d'une machine virtuelle sur laquelle Kaspersky Endpoint Security est installé, il est recommandé d'arrêter la machine virtuelle et de créer un instantané « à froid ». Si vous créez un instantané pendant que la machine virtuelle est en cours d'exécution (un instantané « à chaud »), le bon fonctionnement de l'application n'est pas garanti.

Compatibilité avec Kaspersky Security Center

- Dans Kaspersky Security Center Web Console version 14.1 et antérieures, les noms des zones de fonctionnalité des modules Inspection des journaux et Contrôle de l'intégrité des fichiers ne sont pas correctement affichés dans la section des paramètres des autorisations d'accès des utilisateurs des propriétés du Serveur d'administration.

- Une fois que l'application a été réparée, la protection de la connexion de l'ordinateur au Serveur d'administration est désactivée. Après avoir réparé l'application, exécutez de nouveau la tâche *Protection de la connexion au Serveur d'administration*.

- Dans la Console d'administration de Kaspersky Security Center, la fenêtre **Sélectionner un utilisateur ou un groupe d'utilisateurs** n'affiche que les 50 000 premiers utilisateurs de la liste des utilisateurs de Kaspersky Security Center. Consultez l'aide de Kaspersky Security Center pour plus de détails.

- Lors de la recherche d'appareils administrés dans la Console d'administration de Kaspersky Security Center, l'onglet **Modules de l'application** peut afficher simultanément plusieurs variantes du nom d'un même module d'application, y compris les noms correspondant à d'anciennes versions de Kaspersky Endpoint Security. Les noms de certains modules peuvent également être en double.

  Pour la recherche par module, il suffit de sélectionner une des variantes présentées. Pour plus de détails sur la recherche d'appareils, consultez l'aide de Kaspersky Security Center.

- Dans Kaspersky Security Center Web Console 15.1 Update 2, lorsque le plug-in Internet de Kaspersky Endpoint Security for Windows version 12.11 ou ultérieure et Unified Protection and Management Plug-in sont installés, les conditions d'activation du profil de la stratégie ne fonctionnent pas. Kaspersky Security Center n'ajoute pas à la console les nouveaux appareils qui remplissent les conditions d'activation du profil.

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.

- 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. Cela est dû au fait qu'au cours du processus d'installation, l'application active d'abord la licence d'évaluation intégrée. Elle requiert un accès à Internet.

- Pendant la période d'essai, l'installation de toute mise à jour 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. Cela est dû au fait qu'au cours du processus d'installation de la mise à jour, l'application active d'abord la licence d'évaluation intégrée. Elle requiert un accès à Internet.

- 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 14.2 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.

Protection contre les menaces par emails

- Lors de l'analyse des emails avec l'extension Protection contre les menaces par emails pour Microsoft Outlook, nous vous recommandons d'utiliser le mode Exchange mis en cache (Use Cached Exchange Mode).

- Kaspersky Endpoint Security ne prend pas en charge la version 64 bits du client de messagerie Microsoft Outlook. Autrement dit, Kaspersky Endpoint Security n'analyse pas les fichiers Microsoft Outlook (fichiers PST et OST) si une version 64 bits de Microsoft Outlook est installée sur l'ordinateur, même si la messagerie est incluse dans la zone d'analyse.

- Kaspersky Endpoint Security ne prend pas en charge le nouveau client de messagerie Microsoft Outlook.

- Si vous avez désactivé la désinfection des menaces détectées par la Protection contre les menaces par emails et reçu un email infecté dans votre boîte aux lettres Outlook, la Protection contre les menaces Internet peut bloquer la communication avec le serveur Exchange via MAPI. La Protection contre les menaces Internet génère alors un événement de détection de menace et l'envoie à Kaspersky Security Center. Pour rétablir la connexion entre l'ordinateur et le serveur Exchange, vous devez supprimer manuellement l'email infecté de la boîte aux lettres Outlook.

  Lors de la mise à jour de la version de l'application sans redémarrage de l'ordinateur, le niveau de la Protection contre les menaces par emails est temporairement réduit (pendant une minute au maximum). Si vous recevez un email infecté dans votre boîte aux lettres Outlook pendant la mise à jour de l'application, la Protection contre les menaces Internet bloque également la connexion au serveur Exchange via MAPI. Pour rétablir la connexion, supprimez l'email infecté de la boîte aux lettres Outlook.

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 jusqu'à 100 Mo.

- L'application restaure les fichiers portant les extensions suivantes : odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, 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 procès au niveau du noyau du système d'exploitation.

Pare-feu

- Si une règle de paquet réseau ou une règle de réseau d'application spécifie des noms DNS, Kaspersky Endpoint Security peut envoyer des requêtes au serveur DNS afin de déterminer les adresses IP de ces ressources. Le Pare-feu utilise les adresses IP pour surveiller l'activité réseau. Par conséquent, l'application convertit les noms DNS en adresses IP. Il est recommandé d'utiliser les noms DNS dans les règles uniquement pour les ordinateurs du réseau local ou les services internes.

- Pour définir une règle pour toutes les adresses IPv6, ajoutez la plage d'adresses ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Le Pare-Feu ne prend pas en charge le masque ::/0.

- 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.

- 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.

- Lors de l'importation de règles pour les paquets du pare-feu, Kaspersky Endpoint Security peut modifier les noms des règles. L'application détermine des règles avec des ensembles identiques de paramètres généraux : protocole, direction, ports distants et locaux, 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. Ainsi, Kaspersky Endpoint Security importe toutes les règles de paquets, mais le nom des règles qui ont des paramètres principaux identiques peut être modifié.

- Si vous avez activé les rapports d'événements de l'application dans une règle réseau, lorsque vous déplacez l'application vers un groupe de confiance différent, les restrictions de ce groupe de confiance ne seront pas appliquées. Ainsi, si l'application se trouve dans le groupe De confiance, elle n'aura aucune restriction de réseau. Vous avez ensuite activé les rapports d'événements pour cette application et l'avez déplacée vers le groupe *Douteuses*. Le pare-feu n'appliquera pas de restrictions de réseau pour cette application. Nous vous recommandons d'abord de déplacer l'application vers le groupe de confiance approprié, puis d'activer le rapport d'événements. Si cette méthode ne convient pas, vous pouvez configurer manuellement des restrictions pour l'application dans les paramètres des règles réseau. La restriction ne s'applique qu'à l'interface locale de l'application. Le déplacement de l'application entre les groupes de confiance dans la stratégie fonctionne.

- Les modules Pare-feu et Prévention des intrusions ont des paramètres communs : privilèges des applications et ressources protégées. Si vous modifiez ces paramètres pour le pare-feu, Kaspersky Endpoint Security applique automatiquement les nouveaux paramètres à la Prévention des intrusions. Si, par exemple, vous avez autorisé la modification des paramètres généraux de la stratégie du pare-feu (le cadenas est ouvert), les paramètres de la Prévention des intrusions seront également modifiables.

- 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 la 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.

- Si vous avez interdit toute activité réseau à l'aide du pare-feu, le module Protection contre les menaces réseau peut détecter une attaque de type Analyse des ports. Cela peut être dû au fait que l'application lance la Protection contre les menaces réseau avant le pare-feu pour détecter toute activité suspecte sur le réseau.

Protection BadUSB

- Kaspersky Endpoint Security réinitialise le délai d'expiration du blocage de l'appareil USB quand l'ordinateur est verrouillé (par exemple, délai de verrouillage de l'écran écoulé). Cela veut dire que si vous saisissez un code erroné d'autorisation d'appareil USB à plusieurs reprises et si l'application la bloque, Kaspersky Endpoint Security vous permet de réaliser une nouvelle tentative d'autorisation en déverrouillant l'ordinateur. Dans ce cas, Kaspersky Endpoint Security ne bloque pas l'appareil USB pendant la durée définie via Paramètres du module Protection BadUSB.

- Kaspersky Endpoint Security réinitialise le délai d'expiration de blocage de l'appareil USB quand la protection de l'ordinateur est suspendue. Cela veut dire que si vous saisissez un code erroné d'autorisation d'appareil USB à plusieurs reprises et si l'application la bloque, Kaspersky Endpoint Security vous permet de réaliser une nouvelle tentative d'autorisation après avoir rétabli la protection de l'ordinateur. Dans ce cas, Kaspersky Endpoint Security ne bloque pas l'appareil USB pendant la durée définie via Paramètres du module Protection BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security ne prend pas en charge HTTPS lors de la connexion au proxy KSN (case **Utiliser HTTPS** cochée dans les paramètres de connexion du proxy KSN) si l'adresse du serveur comporte des lettres non latines (symboles non-ASCII).

- Dans Kaspersky Security Center, lors du passage de Kaspersky Security Network mondial à Kaspersky Security Network privé (KPSN), 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.

- À partir de Kaspersky Endpoint Security 12.9 for Windows, lors du passage de KPSN à KSN global, vous devez reconfirmer votre accord avec la Déclaration de Kaspersky Security Network. Pour ce faire, vous devez activer l'utilisation de Kaspersky Security Network dans les propriétés de la stratégie ou dans l'interface de l'application et accepter la Déclaration de Kaspersky Security Network. Si vous avez déjà utilisé KSN global, vous devez d'abord désactiver l'utilisation de KSN, le réactiver et confirmer votre accord avec la Déclaration de Kaspersky Security Network. Si vous n'êtes pas d'accord avec la Déclaration de Kaspersky Security Network, l'application ne pourra pas accéder aux données de Kaspersky Security Network.

- Kaspersky Endpoint Security n'envoie pas de fichiers texte (comme les fichiers TXT, CSV, LOG et DOCX sans macros) à Kaspersky Security Network pour analyse. L'application envoie pour analyse les fichiers susceptibles de présenter des menaces pour KSN. Ces fichiers comprennent des fichiers exécutables ou des fichiers susceptibles de contenir du code exécutable (comme les macros dans les fichiers DOCX). D'autres modules de l'application sont chargés d'analyser les fichiers texte. Vous pouvez également vérifier manuellement la réputation d'un fichier texte à partir du menu contextuel du fichier. Si un fichier texte est classé comme *Douteuse (Kaspersky Security Network)*, l'application ignore l'action définie pour les menaces détectées.

Contrôle des applications

- Lorsque vous utilisez les règles du Contrôle des applications, il n'est pas recommandé d'ajouter plus de 100 000 conditions d'inclusion et d'exclusion au total pour les applications de différentes catégories, à condition que Kaspersky Endpoint Security soit exécuté sur un ordinateur qui répond à la configuration matérielle minimale requise et fonctionne sous Microsoft Windows 10.

- Seules les archives au format ZIP sont prises en charge lors de l'utilisation des règles du Contrôle des applications dans Kaspersky Security Center Web Console. Les archives dans d'autres formats, comme RAR ou 7z, ne sont pas prises en charge. Il n'existe aucune restriction de ce type si vous travaillez avec des règles du Contrôle des applications dans la Console d'administration (MMC).

- Lorsque vous utilisez les règles du Contrôle des applications dans Kaspersky Security Center Web Console, la taille maximale prise en charge d'un fichier téléchargé est de 104 Mo. Il n'existe aucune restriction de ce type si vous travaillez avec des règles du Contrôle des applications dans la Console d'administration (MMC).

- 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.

- Si vous avez ajouté de nouvelles *règles prédéfinies pour le Contrôle des applications* lors de la mise à jour de Kaspersky Endpoint Security, vous ne pouvez pas appliquer ces règles aux versions antérieures de l'application.

- 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.

- Lorsque vous ajoutez l'application standard Bloc-notes à une règle de contrôle des applications pour Windows 11, il n'est pas recommandé de préciser le chemin d'accès à l'application. Sur les ordinateurs exécutant Windows 11, le système d'exploitation utilise l'application Metro Notepad située dans le dossier `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. Dans les versions précédentes du système d'exploitation, le Bloc-notes se trouve dans les dossiers suivants :

  - `C:\Windows\notepad.exe`

  - `C:\Windows\System32\notepad.exe`

  - `C:\Windows\SysWOW64\notepad.exe`

  Lorsque vous ajoutez le Bloc-notes à une règle de contrôle des applications, vous pouvez spécifier le nom de l'application et le hash du fichier à partir des propriétés de l'application en cours d'exécution, par exemple.

- Lors de la migration de la stratégie KSWS vers le profil de stratégie KES, l'Assistant de conversion de masse des stratégies et des tâches (Assistant de migration) renomme les catégories d'applications si le nom des catégories contient des caractères interdits : `'` `*` `<` `>` `?` `\` `:` `|`. L'Assistant de migration remplace ces caractères par les caractères `_`. Par exemple, la catégorie d'applications `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` est renommée en `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Contrôle des appareils

- Kaspersky Endpoint Security peut enregistrer les événements de connexion et de déconnexion de l'appareil externe. Les services Windows utilisent le compte d'utilisateur système pour connecter et déconnecter les appareils. Il est donc impossible de savoir quel utilisateur connecte ou déconnecte l'appareil. Kaspersky Endpoint Security définit le compte utilisateur SYSTÈME dans l'événement.

- 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.

- 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. Kaspersky Endpoint Security enregistre les événements de déconnexion uniquement pour les types d'appareils suivants : Appareils portables (MTP), Disques amovibles, Disquettes et Lecteurs de CD/DVD. Pour les autres types d'appareils, l'application n'enregistre pas les événements de déconnexion. L'application enregistre l'opération de connexion de l'appareil à l'ordinateur pour tous les types d'appareils.

- 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.

- Lorsque l'application est mise à jour sans redémarrage de l'ordinateur, le Contrôle des appareils n'applique pas de règles d'accès aux appareils reconnectés. Toutefois, si l'appareil était connecté avant la mise à jour, le Contrôle des appareils applique correctement les règles. Redémarrez l'ordinateur pour que l'application fonctionne correctement avec les appareils reconnectés.

- Sur les ordinateurs sur lesquels Kaspersky Endpoint Security version 12.0 est installé, le mode d'accès à l'imprimante **Autoriser et ne pas enregistrer** pour le type d'appareil **Imprimantes réseau** est appelé **Dépend du bus de connexion** si la stratégie de Kaspersky Endpoint Security version 12.1 est appliquée sur l'ordinateur. Dans ces modes, l'application effectue les mêmes actions. Dans Kaspersky Endpoint Security version 12.1, le mode d'accès aux imprimantes réseau est correctement nommé **Autoriser et ne pas enregistrer**.

- À partir de Kaspersky Endpoint Security 12.0 for Windows, l'application permet de configurer les règles d'impression pour les imprimantes (contrôle d'impression). Après avoir installé l'application avec le contrôle d'impression ou mis à jour l'application vers une version avec un contrôle d'impression, vous devez redémarrer l'ordinateur. Jusqu'au redémarrage de l'ordinateur, Kaspersky Endpoint Security n'applique pas les règles d'impression et ne peut contrôler que l'accès aux imprimantes. Si le redémarrage de l'ordinateur a une incidence négative sur les flux de travail de votre organisation, vous pouvez redémarrer uniquement le service spoolsv (Print Spooler). La gestion de l'impression n'est pas prise en charge sur les ordinateurs basés sur l'architecture ARM.

- À partir de Kaspersky Endpoint Security 12.0 for Windows, le protocole WPA3 est pris en charge par l'application pour les appareils de type **Wi-Fi**. Si une stratégie de Kaspersky Endpoint Security version 12.2 est appliquée sur un ordinateur, le protocole WPA2 est sélectionné sur les ordinateurs disposant de Kaspersky Endpoint Security version 11.11.0 ou une version antérieure ; le protocole WPA2 / WPA3 est sélectionné pour les versions 12.0 à 12.1 ; le protocole WPA3 est sélectionné pour les versions 12.2 et les versions ultérieures.

- Les appareils Apple sont classés comme appareils portables (MTP) et appareils iTunes. Le système d'exploitation peut identifier de manière incorrecte la connexion de l'appareil Apple et ne pas déterminer l'appareil Apple en tant qu'appareil portable (MTP). Par conséquent, l'appareil Apple sera indisponible dans le gestionnaire de fichiers, mais accessible dans l'application iTunes. Par conséquent, Kaspersky Endpoint Security contrôlera l'accès à l'appareil Apple uniquement dans l'application iTunes. Pour accéder à votre appareil Apple en tant qu'appareil portable (MTP), vous devez accéder au Gestionnaire d'appareils et supprimer le pilote USB de l'appareil mobile Apple de la liste des contrôleurs USB. Après le redémarrage de l'ordinateur, le système d'exploitation identifiera l'appareil Apple en tant qu'appareil portable (MTP) et appareil iTunes. Kaspersky Endpoint Security contrôlera l'accès à l'appareil à la fois dans l'application iTunes et dans le gestionnaire de fichiers.

- Dans Kaspersky Endpoint Security 12.3 for Windows, les paramètres d'accès sont différents pour le type d'appareil **Bluetooth**. Si vous avez défini la valeur **Dépend du bus de connexion** dans la version précédente de l'application, puis après la mise à jour de l'application vers la version 12.3, la valeur configurée devient **Autoriser et ne pas enregistrer**. Cette action ne modifie pas le comportement de l'appareil.

- Le Contrôle des appareils prend en charge les appareils Bluetooth uniquement via la pile Bluetooth de Microsoft Windows. Le Contrôle des appareils peut ne pas fonctionner correctement avec des piles Bluetooth tierces.

- Si l'appareil Bluetooth masque ou usurpe sa classe d'appareil (COD), le Contrôle des appareils peut ne pas fonctionner correctement.

- Sur les ordinateurs Windows 7 ou Windows 8 équipés de certains pilotes de dongle Bluetooth Realtek, il peut être impossible d'autoriser uniquement la connexion d'appareils Bluetooth en tant qu'appareils de saisie (classe HID). Autrement dit, si vous interdisez l'accès aux appareils Bluetooth dans les paramètres de l'application et ajoutez des appareils de saisie aux exclusions, le contrôle des appareils peut empêcher l'accès à tous les appareils Bluetooth.

Contrôle Internet

- Les formats OGV et WEBM ne sont pas pris en charge.

- Le protocole RTMP n'est pas pris en charge.

- Le Contrôle Internet prend en charge uniquement l'environnement WSL1. L'application ne contrôle pas le trafic WSL2.

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 **Rapport sur les déclenchements des 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.

- Kaspersky Security Center 15.1 ne peut pas générer de rapport **Rapport sur l'état des règles du Contrôle évolutif des anomalies** détaillé pour une règle spécifique.

- Les règles du Contrôle évolutif des anomalies sont disponibles uniquement dans la langue d'installation du plug-in Internet. Si vous changez la langue de l'interface, Web Console affiche une liste de règles vide. Pour accéder aux règles, rétablissez la langue d'installation du plug-in Internet comme langue de l'interface.

Chiffrement de disque (FDE)

- Kaspersky Disk Encryption n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

- Le chiffrement de disque BitLocker n'est pas pris en charge sur les ordinateurs exécutant Windows Home.

- Avec le chiffrement de disque BitLocker, l'utilisateur peut modifier manuellement le mot de passe d'authentification à l'aide de l'API Windows. Dans ce cas, BitLocker ignore les exigences relatives aux mots de passe définies dans la stratégie de Kaspersky Endpoint Security. En d'autres termes, l'utilisateur peut définir n'importe quel mot de passe.

- 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.

- Plusieurs agents de téléchargement ne peuvent pas coexister sur un seul ordinateur chiffré.

- Tentative de restauration d'une image d'un disque GPT de démarrage à l'état non chiffré, le système d'exploitation peut rendre le système d'exploitation inopérant. Pour éviter cela, suivez les recommandations suivantes :

  - Déchiffrez complètement le disque avant de restaurer l'image à partir d'une sauvegarde.

  - Utilisez la copie secteur par secteur lors de la création de l'image.

  - Supprimez les données des premiers secteurs du disque chiffré avant de restaurer l'image et réinitialisez le disque.

- 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 `<domain>/<Windows account name>`, 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 `Ivanov` de l'utilisateur local `Ivanov` dispose d'un compte d'Agent d'authentification portant le nom `Ivanov/Ivanov` et qu'un compte a été créé pour cet utilisateur. Si le nom de l'ordinateur `Ivanov` a été changé en `Ivanov-PC`, vous devez changer le nom du compte de l'Agent d'authentification pour l'utilisateur `Ivanov` de `Ivanov/Ivanov` à `Ivanov-PC/Ivanov`. 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, `Ivanov/Ivanov`).

- 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. 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.

- Le chiffrement des disques est incompatible avec la technologie Intel Rapid Start.

- Le chiffrement des disques est incompatible avec la technologie ExpressCache.

- 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 n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

- Le chiffrement des fichiers et des dossiers n'est pas pris en charge sous les systèmes d'exploitation 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.

- L'application ne prend en charge le chiffrement des fichiers que sur les appareils dotés des systèmes de fichiers NTFS et FAT32. Si un fichier chiffré est transféré vers un appareil doté d'un système de fichiers non pris en charge (par exemple, exFAT), le fichier sur cet appareil ne sera pas chiffré et pourra être modifié.

- 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.

- Lors de la copie du fichier déchiffré, par exemple, sur un support amovible, le fichier peut rester chiffré. En effet, lorsque le gestionnaire de fichiers (par exemple, explorer.exe) tente d'accéder au fichier chiffré, il enregistre le hachage du fichier dans une liste spéciale du processus. Après avoir déchiffré le fichier, lorsque le gestionnaire de fichiers tente d'y accéder, le processus recherche le hachage du fichier dans la liste. Si le hachage est trouvé, Kaspersky Endpoint Security laisse le fichier sous forme chiffrée. Pour éviter cela, vous devez effacer la liste du processus. Le système d'exploitation efface automatiquement la liste des processus au fur et à mesure qu'elle se remplit. Vous pouvez également vider la liste manuellement. Pour ce faire, vous pouvez redémarrer l'ordinateur, redémarrer le processus que vous utilisez pour accéder au fichier (par exemple, explorer.exe) ou utiliser un gestionnaire de fichiers différent que vous n'avez pas utilisé pour accéder au fichier chiffré.

- 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.

- Avant de décompresser une archive chiffrée, assurez-vous d'avoir suffisamment d'espace disque libre pour accueillir les fichiers décompressés. Si vous ne disposez pas de suffisamment d'espace disque, la décompression de l'archive peut s'achever, mais les fichiers peuvent être corrompus. Dans ce cas, il est possible que Kaspersky Endpoint Security n'affiche aucun message d'erreur.

- 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.

- Vous ne pouvez pas utiliser le Gestionnaire de fichiers portable pour accéder à un disque amovible si les conditions suivantes sont vraies simultanément :

  - 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.

  L'accès est impossible, 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.

- 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.

- 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 Client-Side Caching n'est pas prise en charge. Le chiffrement des fichiers en mode hors ligne, tout comme la technologie Branch Caching via SMB pour les serveurs, ne sont également pas pris 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.

- 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.

- 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.

- Kaspersky Endpoint Security ne chiffre pas les fichiers qui se trouvent dans le stockage cloud OneDrive ou dans d'autres dossiers dont le nom est OneDrive. Kaspersky Endpoint Security bloque également la copie des fichiers chiffrés vers les dossiers OneDrive si ces fichiers ne sont pas ajoutés à la règle de déchiffrement.

- 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.

- Il n'est pas recommandé de chiffrer les fichiers temporaires, car cela peut entraîner une perte de données. Par exemple, Microsoft Word crée des fichiers temporaires lors du traitement d'un document. Si les fichiers temporaires sont chiffrés, mais que le fichier d'origine ne l'est pas, l'utilisateur peut recevoir une erreur *Accès refusé* lors de la tentative d'enregistrement du document. De plus, Microsoft Word peut enregistrer le fichier, mais il ne sera pas possible d'ouvrir le document la prochaine fois, c'est-à-dire que les données seront perdues. Pour éviter la perte de données, vous devez exclure le dossier des fichiers temporaires des règles de chiffrement.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Vous ne pouvez pas analyser un objet mis en quarantaine à la suite de la tâche *Placer le fichier en Quarantaine*.

- Il n'est pas possible de mettre en quarantaine un Alternate Data Stream dont la taille est supérieure à 4 Mo. Kaspersky Endpoint Security ignore les flux de données alternatifs de cette taille sans en informer l'utilisateur.

- Kaspersky Endpoint Security n'exécute pas de tâches *Analyse IOC* sur les disques réseau si le chemin d'accès au dossier dans les propriétés de la tâche commence par une lettre de disque. Kaspersky Endpoint Security prend uniquement en charge le format de chemin d'accès UNC pour les tâches *Analyse IOC* sur les disques réseau. Par exemple, `\\server\shared_folder`.

- Pour assurer le bon fonctionnement de la tâche *Analyse IOC* utilisant les conditions EmailItem, le plug-in Internet de Kaspersky Endpoint Security doit être mis à jour vers la dernière version.

- Sur les ordinateurs basés sur l'architecture ARM, la tâche *Analyse IOC* prend en charge uniquement les fichiers d'email provenant des clients de messagerie suivants : les versions 32 bits et 64 bits d'Outlook 2016, ainsi que les versions 2021, 2024 et 365 d'Outlook pour Arm64.

- L'importation d'un fichier de configuration d'une application se termine par une erreur si le paramètre d'intégration avec Kaspersky Sandbox est activé dans le fichier de configuration. Avant d'exporter les paramètres de l'application, désactivez Kaspersky Sandbox. Ensuite, effectuez la procédure d'exportation/importation. Après avoir importé le fichier de configuration, activez Kaspersky Sandbox.

- Lors de l'importation d'une stratégie depuis un fichier KLP, la valeur du paramètre qui détermine l'acceptation des conditions générales du Contrat Kaspersky Detection and Response Expert n'est pas appliquée. Par conséquent, après l'importation de la stratégie, Kaspersky Endpoint Security n'exécute pas les fonctions de l'Agent EDR. Pour que l'Agent EDR fonctionne, ouvrez la stratégie, modifiez n'importe quel paramètre, puis enregistrez les paramètres de la stratégie.

- Lorsqu'un indicateur de compromission est détecté lors de l'exécution de la tâche *Analyse IOC*, l'application met en quarantaine un fichier uniquement pour le terme FileItem. La mise en quarantaine d'un fichier pour d'autres termes n'est pas prise en charge.

- Le plug-in Internet de Kaspersky Endpoint Security for Windows 11.7.0 ou une version ultérieure est nécessaire pour gérer les détails des alertes. Les détails de l'alerte sont nécessaires lorsqu'on utilise les solutions Endpoint Detection and Response (EDR Optimum et EDR Expert). Les détails des alertes sont disponibles uniquement dans Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console.

- La migration de la configuration [KES+KEA] vers la configuration [KES+agent intégré] peut se terminer par une erreur de suppression de l'application Kaspersky Endpoint Agent. L'erreur de suppression de l'application est corrigée dans la dernière version de Kaspersky Endpoint Agent. Pour supprimer Kaspersky Endpoint Agent, redémarrez l'ordinateur et créez une tâche de suppression d'application.

- La configuration [KES+KEA+agent intégré] n'est pas prise en charge. Une telle configuration perturbe l'interaction entre les applications et la solution Detection and Response déployée au sein de votre organisation. De plus, l'utilisation de Kaspersky Endpoint Agent et de l'agent intégré sur le même ordinateur peut entraîner une duplication des données télémétriques ainsi qu'une augmentation de la charge sur l'ordinateur et le réseau. Après la migration vers la configuration [KES+agent intégré], assurez-vous que Kaspersky Endpoint Agent a été supprimé de l'ordinateur. Si Kaspersky Endpoint Agent continue de fonctionner après la migration, désinstallez l'application manuellement (par exemple, à l'aide de la tâche *Désinstallation à distance d'une application*).

  Le programme d'installation vous permet de déployer Kaspersky Endpoint Agent sur un ordinateur sur lequel Kaspersky Endpoint Security et l'agent intégré sont installés. Kaspersky Endpoint Agent et l'agent intégré peuvent également être installés sur un ordinateur grâce à la tâche *Modification de la sélection des modules de l'application*. Le comportement dépend des versions de Kaspersky Endpoint Security et de Kaspersky Endpoint Agent.

- Lors de la génération des détails de l'alerte, l'application fournit des informations sur la menace détectée, y compris les hachages des fichiers modifiés. Kaspersky Endpoint Security calcule le hachage du fichier tout en générant les détails de l'alerte. Gardez à l'esprit que le hachage d'origine du fichier lorsque l'événement de modification du fichier a été généré peut différer du hachage calculé lors de la génération des détails de l'alerte.

- L'agent intégré, EDR (KATA), reprend l'isolation réseau d'un ordinateur après un redémarrage de l'ordinateur, même si la période d'isolation a expiré. Pour éviter l'isolation répétée de l'ordinateur, vous devez désactiver l'isolation réseau dans la console Kaspersky Anti Targeted Attack Platform.

- Nous vous recommandons de mettre à jour l'application une fois l'isolation du réseau terminée. Après la mise à jour de Kaspersky Endpoint Security, l'isolation du réseau peut être arrêtée.

- Les agents intégrés pour EDR (KATA), EDR Optimum et EDR Expert ne sont pas compatibles entre eux. Par conséquent, l'activation de l'agent intégré EDR avec une licence autonome pour le module complémentaire de Kaspersky Endpoint Detection and Response peut être ignorée si vous avez activé Kaspersky Endpoint Security avec une fonctionnalité EDR différente. Par exemple, l'activation de l'agent intégré EDR (KATA) avec une licence autonome est ignorée si vous avez activé Kaspersky Endpoint Security avec la licence [KES+EDR Optimum].

- Dans Kaspersky Endpoint Security version 12.1, l'agent EDR (KATA) intégré ne prend pas en charge les métafichiers suivants pour la tâche *Obtenir les métafichiers NTFS* : $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Une prise en charge de ces métafichiers a été ajoutée à Kaspersky Endpoint Security version 12.2.

- Lors de la migration de Kaspersky Endpoint Agent vers Kaspersky Endpoint Security pour la solution Kaspersky Anti Targeted Attack Platform (EDR), vous pouvez rencontrer des erreurs lors de la connexion de l'ordinateur aux serveurs de Central Node. La raison en est que l'Assistant de migration de Web Console ignore les paramètres de stratégie suivants et ne les migre pas :

  - Interdiction de modification des paramètres **Paramètres de connexion** (« cadenas »).

    Par défaut, les paramètres peuvent être modifiés (le « cadenas » est ouvert). Par conséquent, les paramètres ne sont pas appliqués sur l'ordinateur. Vous devez interdire la modification des paramètres et fermer le « cadenas ».

  - Conteneur crypto.

    Si vous utilisez l'authentification bidirectionnelle pour vous connecter aux serveurs de Central Node, vous devez rajouter le conteneur crypto. L'Assistant de migration migre correctement le certificat TLS du serveur.

  L'Assistant de migration des stratégies et des tâches de la Console d'administration (MMC) migre tous les paramètres de la solution Kaspersky Anti Targeted Attack Platform (EDR).

- L'état d'activation de l'application s'affiche de manière incorrecte lorsque l'application est installée en mode Endpoint Detection and Response Agent pour prendre en charge la solution Kaspersky Managed Detection and Response sans connexion à Kaspersky Security Center. Après le téléchargement du fichier BLOB, la zone de notification de la barre des tâches de Windows affiche un état incorrect : *Application non activée*. Cependant, l'interface de l'application affiche correctement l'état d'activation. Redémarrez l'ordinateur pour que l'application fonctionne correctement.

- Kaspersky Endpoint Security permet l'intégration à la solution Kaspersky Anti Targeted Attack Platform à l'aide du module EDR (KATA) ou Endpoint Sensor (non pris en charge). Notez que vous pouvez uniquement utiliser un des modules pour interagir avec Kaspersky Anti Targeted Attack Platform. Pour consulter l'état du module, ouvrez les propriétés de l'ordinateur dans la Console d'administration (MMC), dans la section **Applications**, ouvrez les propriétés de Kaspersky Endpoint Security for Windows et accédez à la section **Modules**. Les considérations particulières suivantes s'appliquent à l'affichage de l'état du module pour l'interaction avec Kaspersky Anti Targeted Attack Platform :

  - Pour le plug-in d'administration 12.0 et les versions antérieures, l'application affiche l'état actuel d'**Endpoint Sensor**. Dans Kaspersky Endpoint Security 12.0 et les versions antérieures, le module EDR (KATA) n'est pas disponible. Le module EDR (KATA) a été introduit dans la version 12.1.

  - Pour le plug-in d'administration 12.1 et les versions ultérieures, l'application affiche l'état général d'**Endpoint Detection and Response (KATA)**, qui peut indiquer soit l'état d'Endpoint Sensor, soit l'état du module EDR (KATA). Tout dépend de la version de l'application installée sur l'ordinateur de l'utilisateur et des modules disponibles que vous pouvez utiliser pour interagir avec Kaspersky Anti Targeted Attack Platform.

- À partir de Kaspersky Endpoint Security version 12.6 et toute version ultérieure, Kaspersky Security Center Web Console version 14.2 et les versions antérieures n'affichent pas correctement le nom du module **Endpoint Detection and Response (KATA)** dans les propriétés de l'ordinateur. Au lieu du module **Endpoint Detection and Response (KATA)**, l'application affiche le nom du module **Endpoint Detection and Response Expert (KATA EDR)**. Pour consulter la liste des modules, ouvrez les propriétés de l'ordinateur dans Web Console, dans l'onglet **Applications**, ouvrez les propriétés de Kaspersky Endpoint Security for Windows et accédez à la section **Modules**. À partir de la version 15.1 de Kaspersky Security Center Web Console, l'application affiche correctement le nom du module.

- Lors de la mise à jour du plug-in d'administration de Kaspersky Endpoint Detection and Response vers la version 15.3 installé dans les versions 14.0-14.2 de Web Console, les détails de l'alerte s'affichent de manière incorrecte. Pour que les informations sur les alertes fonctionnent correctement, redémarrez le Serveur d'administration de Kaspersky Security Center.

- Le plug-in d'administration de Kaspersky Endpoint Detection and Response versions 15.4 et ultérieures ne prend pas en charge Kaspersky Security Center version 14.0. Après la mise à jour du plug-in d'administration, les détails de l'alerte ne s'affichent pas correctement.

- Les solutions de classe Kaspersky Extended Detection and Response (XDR) version 1.4 ne prennent pas en charge le plug-in Web de Kaspersky Endpoint Security for Windows version 12.12 ni toute version ultérieure. Vous pouvez soit conserver la version actuelle du plug-in Web, soit mettre à jour la solution XDR vers la version 2.0 ou une version ultérieure.

- Kaspersky Endpoint Security n'envoie pas les objets destinés à l'architecture ARM à Kaspersky Sandbox.

- Au total, Kaspersky Endpoint Security prend en charge jusqu'à 10 000 règles de filtrage des événements d'inclusion et d'exclusion EDR Expert (on-premises).

- Les règles de filtrage des événements d'EDR Expert (on-premises) ne seront pas transmises de la stratégie aux appareils administrés exécutant Kaspersky Endpoint Security version 14.0 ou toute version antérieure si la limite autorisée pour le nombre de règles de filtrage stockées est dépassée. L'application affichera un avertissement correspondant.

- Les versions 12.11 à 14.1 de Kaspersky Endpoint Security for Windows ne prennent pas en charge les événements de télémétrie EDR Expert (on-premises) suivants :

  - LDAP Attribute Change

  - GPO Change

- SCCM Local Config Mismatch
- SCCM Config Change
- SCCM Deployment Task
- Smb Connection Open

À partir de la version 14.2, Kaspersky Endpoint Security prend en charge tous ces événements de télémétrie EDR Expert (on-premises), à l'exception de LDAP Attribute Change.

Autres restrictions

- Les systèmes d'exploitation Windows, à partir de la version 11 24H2, prennent en charge le UDP Receive Segment Coalescing Offload (URO). La technologie est activée par défaut si la carte réseau compatible et les pilotes sont installées sur l'ordinateur. La désactivation d'URO sur l'ordinateur d'un utilisateur peut réduire considérablement les performances de l'application.
- Kaspersky Endpoint Security prend en charge le sous-système WSL (Windows Subsystem for Linux) avec certaines restrictions :
  - WSL 1. L'application surveille le trafic réseau et détecte les menaces via le protocole HTTP / HTTPS. Étant donné que Kaspersky Endpoint Security utilise son propre certificat pour analyser les connexions HTTPS sécurisées, le fonctionnement de certaines applications tierces peut être interrompu.
  - WSL 2. L'application ne prend pas en charge WSL 2.
- 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.
- Il se peut que les adresses Internet qui sont ajoutées à la liste des adresses de confiance soient traitées de manière incorrecte.
- Dans la console de Kaspersky Security Center, il est impossible d'enregistrer un fichier sur le disque à partir du dossier **Avancé** → **Stockages** → **Menaces actives**. Pour enregistrer le fichier, vous devez désinfecter le fichier infecté. Lors de la désinfection, l'application enregistre une copie du fichier dans la Sauvegarde. Vous pouvez maintenant enregistrer le fichier sur le disque à partir du dossier **Avancé** → **Stockages** → **Sauvegarde**.
- L'héritage des paramètres de transfert de données au Serveur d'administration (**Paramètres généraux** → **Rapports et stockage** → **Transfert des données au Serveur d'administration**) diffère de l'héritage des autres paramètres. Si vous avez autorisé la modification des paramètres de transmission des données dans la stratégie (le « cadenas » est ouvert), ces paramètres seront réinitialisés aux valeurs par défaut dans les propriétés de l'ordinateur local dans la console s'ils n'ont pas été définis précédemment. Si ces paramètres ont été définis auparavant, leurs valeurs sont restaurées. Lors de la suppression d'une stratégie, les paramètres sont hérités de la même manière. Dans ces cas, les autres paramètres des propriétés de l'ordinateur local sont hérités de la stratégie.

- 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 empêche la communication via le protocole QUIC. Les navigateurs utilisent le protocole de transport standard (TLS ou SSL), que la prise en charge de QUIC soit activée ou non dans le navigateur.

- Des erreurs de connexion TLS peuvent se produire lorsque des logiciels tiers fonctionnent avec la bibliothèque Libcurl. Cela peut être lié au certificat Kaspersky utilisé par Kaspersky Endpoint Security pour analyser les connexions chiffrées. Pour continuer à travailler, vous pouvez désactiver la validation des certificats pour les logiciels tiers (non recommandé) ou ajouter un corps de certificat Kaspersky au stockage des certificats cURL. Pour en savoir plus, consultez la Base de connaissances de Kaspersky.

- 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.

- 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 de l'application et dans le rapport de Kaspersky Security Center.

- Le rapport de Kaspersky Security Center 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.

- Il n'est pas possible d'activer l'affichage de toutes les entrées de rapport dans Kaspersky Security Center Web Console. Dans Web Console, vous pouvez uniquement modifier le nombre d'entrées affichées dans les rapports. Par défaut, Kaspersky Security Center Web Console afficher 1 000 entrées de rapport. Vous pouvez activer l'affichage de toutes les entrées de rapport dans la Console d'administration (MMC).

- Il n'est pas possible de définir l'affichage de plus de 1 000 dans Kaspersky Security Center Console. Si vous définissez une valeur supérieure à 1 000, Kaspersky Security Center Console n'affichera que 1 000 entrées de rapport.

- 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 Windows Safe Mode.
- Nous ne pouvons pas garantir que la fonctionnalité Audio Control fonctionnera jusqu'au premier redémarrage après l'installation de l'application.
- Dans la Console d'administration (MMC), dans les paramètres de Prévention des intrusions de la fenêtre de configuration des autorisations de l'application, le bouton **Supprimer** n'est pas disponible. Vous pouvez supprimer une application d'un groupe de confiance via le menu contextuel de l'application.
- Dans l'interface locale de l'application, dans les paramètres de Prévention des intrusions, les autorisations de l'application et les ressources protégées ne sont pas consultables si l'ordinateur est administré par une stratégie. Les commandes de défilement, de recherche, de filtre et d'autres fenêtres ne sont pas disponibles. Vous pouvez consulter les autorisations de l'application dans les propriétés de la stratégie dans Kaspersky Security Center Console.
- 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 journalisation dump n'est pas prise en charge pour les processus pico.
- La désactivation de l'option **Désactiver la gestion externe des services systèmes** 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\`.
- Si vous utilisez des stratégies de restriction logicielle (Software Restriction Policies, SRP), l'ordinateur peut ne pas se charger (écran noir). Pour éviter les dysfonctionnements, vous devez autoriser l'utilisation des bibliothèques d'applications dans les propriétés des SRP. Dans les propriétés des SRP, ajoutez la règle avec le niveau de sécurité **Sans restriction** pour le fichier khkum.dll (élément de menu **Nouvelle règle de hachage**). Le fichier se trouve dans le dossier `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Si vous avez choisi cette méthode, vous devez en outre décocher la case **Télécharger les mises à jour des modules de l'application** dans les paramètres de la tâche *Mise à jour* pour Kaspersky Endpoint Security. Pour en savoir plus à propos de l'utilisation des SRP, consultez la documentation de Microsoft.

  Vous pouvez également désactiver les SRP et utiliser le module Contrôle des applications de Kaspersky Endpoint Security pour contrôler l'utilisation des applications.
- Si l'ordinateur appartient à un domaine sous Windows Group Policy Object (Group Policy Object, GPO) avec le paramètre DriverLoadPolicy défini sur 8 (Good only), le redémarrage de l'ordinateur avec Kaspersky Endpoint Security installé provoque un écran bleu de la mort. Pour éviter un échec, le paramètre Early Launch Antimalware (lancement anticipé anti-application malveillante) dans la stratégie de groupe doit être défini sur 1 (Good and unknown). Les paramètres ELAM se trouvent dans la stratégie sous : **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.
- 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.

- 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).

- Si Kaspersky Endpoint Security est installé sur un serveur SGBD SQL Server, l'application envoie des requêtes à l'instance du serveur. Cette opération est nécessaire pour analyser les travaux de l'agent SQL Server et empêcher l'exécution de tâches malveillantes. Kaspersky Endpoint Security utilise le compte utilisateur SQL Server pour analyser les tâches. L'application envoie des requêtes au serveur lors de l'analyse de la mémoire système et après la mise à jour des bases antivirus.

- La compatibilité de Kaspersky Endpoint Security et du logiciel Secret Net Studio est limitée :

  - L'application Kaspersky Endpoint Security n'est pas compatible avec le module Antivirus du logiciel Secret Net Studio.

    L'application ne peut pas être installée sur un ordinateur où Secret Net Studio est déployé avec le module Antivirus. Pour rendre l'interopérabilité possible, vous devez supprimer le module Antivirus de Secret Net Studio.

  - L'application Kaspersky Endpoint Security n'est pas compatible avec le module de protection du disque et de chiffrement des données du logiciel Secret Net Studio.

    L'application ne peut pas être installée sur un ordinateur où Secret Net Studio est déployé avec le module de protection du disque et de chiffrement des données. Pour rendre l'interopérabilité possible, vous devez supprimer le module de protection du disque et de chiffrement des données de Secret Net Studio.

  - Secret Net Studio n'est pas compatible avec le module Chiffrement des fichiers (FLE) de Kaspersky Endpoint Security.

    Lorsque vous installez Kaspersky Endpoint Security avec le module Chiffrement des fichiers (FLE), Secret Net Studio peut s'exécuter avec des erreurs. Pour assurer l'interopérabilité, vous devez supprimer le module Chiffrement des fichiers (FLE) de Kaspersky Endpoint Security.

- Lors de l'importation des règles du Contrôle de l'intégrité du système, l'application vérifie l'identifiant et le nom de la règle. Si les identifiants des règles sont les mêmes, Kaspersky Endpoint Security remplace les règles existantes par la nouvelle règle. Lors de l'exportation des règles, l'application attribue automatiquement les identifiants. Des règles avec des identifiants identiques peuvent exister, par exemple, si vous avez modifié manuellement les fichiers XML de règles exportés. Si les identifiants des règles sont uniques mais que les noms des règles sont les mêmes, Kaspersky Endpoint Security ajoute la mention `(1)` et ainsi de suite au nom de la règle.

- À partir de la version 12.11 de Kaspersky Endpoint Security for Windows, il n'est plus possible d'afficher les paramètres d'une stratégie parent ouverte dans un groupe enfant dans Web Console. Web Console affiche également un avertissement : *Cette stratégie est héritée. Vous pouvez modifier ses paramètres uniquement dans le groupe d'administration dans lequel elle a été créée*.

- Les notifications contextuelles de plus de 256 caractères ne s'affichent pas dans la Console d'administration (MMC).

- Les noms des modules dans la stratégie et dans le paquet d'installation peuvent être différents. Par exemple, Endpoint Detection and Response Expert (on-premises) peut être désigné sous les noms suivants : Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) ou Kaspersky Anti Targeted Attack Platform Integration. Les noms des modules peuvent également varier en fonction de la version de l'application.

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.

Authentification Kerberos

Mécanisme d'authentification mutuelle par le client et le serveur avant l'établissement d'une connexion entre eux, qui permet de communiquer sur des réseaux non sécurisés. Le mécanisme repose sur un ticket que l'utilisateur obtient auprès d'un centre d'authentification de confiance.

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 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.

Cloud Discovery

Cloud Discovery gère l'accès des utilisateurs aux services cloud. Les services cloud comprennent, par exemple, Microsoft Teams, Salesforce et Microsoft Office 365. Les services cloud sont regroupés en catégories, par exemple : *stockage de fichiers*, *messagerie*, *email*.

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.

Fichier IOC

Un fichier contenant un ensemble d'indicateurs de compromission (IOC) que l'application tente de faire correspondre pour comptabiliser une détection. La probabilité de détection peut être plus élevée si, à l'issue de l'analyse, des correspondances exactes avec plusieurs fichiers IOC sont trouvées pour l'objet.

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.

IOC

Un indicateur de compromission. Un ensemble de données concernant une activité ou un objet malveillant.

Light Agent

Module Kaspersky Endpoint Security for Virtualization Light Agent. S'installe sur chaque machine virtuelle qu'il faut protéger.

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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` 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.

OpenIOC

Standard ouvert de description des indicateurs de compromis (IOC) reposant sur XML et comprenant plus de 500 indicateurs de compromis différents.

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.

Serveur d'intégration.

Module Kaspersky Endpoint Security for Virtualization Light Agent. Interagit entre les modules de Kaspersky Endpoint Security et l'infrastructure virtuelle.

SVM

Machine virtuelle sécurisée : machine virtuelle spéciale sur laquelle le service du serveur d'analyse (le Serveur de protection, un module de Kaspersky Endpoint Security for Virtualization Light Agent) est installé.

Tâche

Fonctions exécutées par l'application de Kaspersky sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'appareil, 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 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 vous permet d'empêcher l'infection du système de fichiers de l'ordinateur. Par défaut, le module Protection contre les fichiers malicieux réside en permanence dans la mémoire vive (RAM) de l'ordinateur et analyse en temps réel tous les fichiers ouverts, enregistrés ou exécutés. Ce module analyse les fichiers sur tous les disques de l'ordinateur, y compris 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 un utilisateur ou une 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.

Lorsque vous essayez d'accéder à un fichier dont le contenu se trouve dans le stockage cloud 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 *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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 *niveaux de sécurité* : • **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.
Types de fichiers *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	**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, l'application 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, l'application analyse uniquement les fichiers infectables. Le format du fichier sera déterminé sur la base de son extension.

Paramètre	Description
Zone d'analyse	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. 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 seulement exclure l'objet (par exemple, les disques amovibles) de l'analyse.
Machine learning et analyse sur la base de signature *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.
Analyse heuristique *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.
Action en cas de détection d'une menace	**Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application supprime le fichier. **Désinfecter ; bloquer si la désinfection est impossible**. Si cette option est sélectionnée, l'application essaie de désinfecter automatiquement les fichiers infectés détectés. Si la désinfection échoue, l'application bloque ce fichier. **Interdire**. Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer. Avant de tenter de désinfecter ou de supprimer un fichier infecté, l'application 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.
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 des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les paquets de distribution	Analyse des paquets de distribution des applications tierces.
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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Analyser les fichiers au format de messagerie	Analyse les fichiers au format de messagerie. L'application analyse les fichiers MSG et EML. Les fichiers au format de messagerie incluent également des objets OLE et des fichiers MHT. Kaspersky Endpoint Security analyse les fichiers au format de messagerie dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Ne pas décompresser les fichiers composés volumineux	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.

Paramètre	Description
Décompresser les fichiers composés en arrière-plan	Si la case est cochée, l'application 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. L'application 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, l'application permet d'accéder aux fichiers composés uniquement après la décompression et l'analyse des fichiers de n'importe quelle taille.
Mode d'analyse *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	Kaspersky Endpoint Security analyse les fichiers auxquels accède l'utilisateur, le système d'exploitation ou une application fonctionnant sous le compte de l'utilisateur. **Mode intelligent**. 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. **Ouverture et 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. **Ouverture**. 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. **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.
Utiliser la technologie iSwift *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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 iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.
Utiliser la technologie iChecker *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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).
Suspendre la Protection contre les fichiers malicieux *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.
Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows	Si une menace est détectée à l'intérieur d'un conteneur, l'application applique l'action sélectionnée pour le module de Protection contre les menaces sur les fichiers. **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté. **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.

Protection contre les menaces Internet

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants depuis Internet et 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.

Pour utiliser la Protection contre les menaces Internet, vous devez procéder à la configuration initiale de l'application :

- Pour contrôler le trafic HTTPS, activez l'analyse des connexions sécurisées (activé par défaut).
- Sélectionnez les ports que Kaspersky Endpoint Security doit surveiller (par défaut, l'application surveille tous les ports).
- Sélectionnez les applications dont vous souhaitez que Kaspersky Endpoint Security contrôle le trafic. La plupart des navigateurs sont déjà présents dans la liste des applications recommandées par Kaspersky. Si votre navigateur ne figure pas dans la liste, ajoutez-le manuellement.
- Nous vous recommandons d'injecter un script d'interaction avec les pages Internet dans le trafic Internet (par défaut, l'injection de script est désactivée). Ce script permet d'enregistrer les événements de la Protection contre les menaces Internet pour le journal des événements de l'application, le journal des événements du système d'exploitation et les rapports.

Lorsqu'un utilisateur tente d'ouvrir un site Internet malveillant ou de phishing, Kaspersky Endpoint Security bloque l'accès et affiche un avertissement.

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Niveau de sécurité *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	L'application peut appliquer différents groupes de paramètres pour le module Protection contre les menaces Internet. Ces groupes de paramètres stockés dans l'application sont appelés *niveaux de sécurité* : • **Élevé**. Niveau de sécurité du trafic Internet auquel le module Protection contre les menaces Internet garantit l'analyse maximale du trafic Internet transmis à un 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 l'application 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. • **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	**Bloquer**. 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. **Informer**. 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.
Vérifier l'adresse Internet par rapport à la base de données des adresses Internet malveillantes *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.
Utiliser l'analyse heuristique *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.

Paramètre	Description
Vérifier l'adresse Internet par rapport à la base de données des adresses Internet de phishing *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.
Ne pas analyser le trafic Internet en provenance des adresses URL de confiance	Si cette option est sélectionnée, 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. Vous pouvez également créer une liste générale d'exclusions pour les connexions chiffrées. Dans ce cas, Kaspersky Endpoint Security n'analyse pas le trafic HTTPS des URL de confiance lorsque les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet fonctionnent.

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 protège l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et d'une analyse heuristique.

La Protection contre les menaces par emails peut analyser les messages entrants et sortants. L'application prend en charge les protocoles POP3, SMTP, IMAP et NNTP dans les clients de messagerie suivants :

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pour analyser le trafic dans les clients de messagerie Mozilla Thunderbird, MyOffice Mail et R7-Office Organizer, vous devez ajouter le certificat Kaspersky à la liste de certificats et sélectionner la propre liste de certificats.

La Protection contre les menaces par emails ne prend pas en charge d'autres protocoles et clients de messagerie.

La Protection contre les menaces par emails peut ne pas toujours être en mesure d'accéder aux messages *au niveau du protocole* (par exemple, lors de l'utilisation de la solution Microsoft Exchange). Pour cette raison, la Protection contre les menaces par emails inclut une extension pour Microsoft Office Outlook. L'extension permet d'analyser les messages *au niveau du client de messagerie*. L'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2010, 2013, 2016, 2019, 2021, 2024 et 365. Sur les ordinateurs équipés d'un processeur ARM, l'extension Protection contre les menaces par emails prend en charge les versions 32 bits et 64 bits d'Outlook 2016, Outlook 2021, Outlook 2024 et Outlook 365 pour ARM64.

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 ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*.

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Niveau de sécurité *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	L'application 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 *niveaux de sécurité* : • **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. Le niveau de sécurité Élevé pour la protection de la messagerie 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 l'application et la sécurité de la messagerie. 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 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 de la messagerie est recommandé pour un travail en environnement bien protégé. Exemple de cet environnement : réseau local d'entreprise avec un système centralisé de protection du courrier.
Action en cas de détection d'une menace	**Désinfecter ; supprimer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant ou sortant, l'application 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, l'application le supprime. L'application ajoute des informations relatives à l'action réalisée dans l'objet du message, par exemple, *[Le message a été traité] <objet du message>*. **Désinfecter ; bloquer si la désinfection est impossible**. Si un objet infecté est détecté dans un message entrant, l'application 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, l'application ajoute un avertissement à l'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, l'application tente de désinfecter l'objet détecté. Si l'objet ne peut pas être désinfecté, l'application bloque l'envoi du message et le client de messagerie affiche une erreur. **Interdire**. Si un objet infecté est détecté dans un message entrant, l'application ajoute un avertissement à l'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, l'application bloque l'envoi du message et le client de messagerie affiche une erreur.
Zone de protection *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	La *Zone d'analyse* 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.
Analyser le trafic POP3, SMTP, NNTP et IMAP	Analyse par le module Protection contre les menaces par emails du trafic de messagerie transmis par les protocoles POP3, SMTP, NNTP et IMAP.
Connecter l'extension Microsoft Outlook	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 des emails à l'aide d'une extension pour Microsoft Outlook, il est recommandé d'utiliser 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 .
Analyse heuristique *(disponible uniquement dans la Console d'administration (MMC) et dans l'interface de Kaspersky Endpoint Security)*	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.

Paramètre	Description
Analyser les archives jointes	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive). Si pendant l'analyse, l'application 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.
Analyser les fichiers joints 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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
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 de vérification 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.
Filtre des pièces jointes	Le filtre des pièces jointes ne s'applique pas aux emails sortants. **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. **Renommer les pièces jointes de types 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. **Supprimer les pièces jointes de types indiqués**. Si cette option est sélectionnée, le module Protection contre les menaces par emails supprime les fichiers joints des types de messages électroniques indiqués. Vous pouvez indiquer les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.

Protection contre les menaces réseau

Le module *Protection contre les menaces réseau* (également appelé Intrusion Detection System, IDS) surveille le trafic réseau entrant pour détecter les activités caractéristiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, l'application 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 l'application. 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
Traiter l'analyse des ports et l'inondation des réseaux comme des attaques	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. Si cette case est cochée, Kaspersky Endpoint Security surveille le trafic réseau pour détecter ces attaques. Si une attaque est détectée, l'application en informe l'utilisateur et envoie l'événement correspondant à Kaspersky Security Center. L'application fournit des informations à propos de l'ordinateur attaquant, nécessaires pour réagir rapidement aux menaces. 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.
Bloquer les appareils attaquants pendant X min	Si cette option est activée, le module Protection contre les menaces réseau 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. Le temps minimum qu'un ordinateur attaquant doit passer dans la liste du groupe est d'une minute. La durée maximale est de 999 minutes. 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.
Exclusions	La liste contient les adresses IP à l'origine des attaques réseau que le module Prévention des intrusions ne bloque pas. Vous pouvez ajouter une adresse IP avec un port et un protocole spécifiés. L'application n'ajoute pas au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions.
Protection contre le MAC spoofing	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.

Pare-feu

Le module Pare-feu bloque les connexions non autorisées à un 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 l'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. 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 de réseau pour les applications fonctionnent d'une manière particulière. La règle de réseau pour les applications inclut des règles d'accès basées sur l'état du réseau : *Réseau public*, *Réseau local*, *Réseau de confiance*. 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.

Types de connexions réseau

Le Pare-feu permet de surveiller l'activité du réseau en fonction du type de connexion réseau. Kaspersky Endpoint Security obtient le type de connexion réseau via le système d'exploitation de l'ordinateur. Le type de connexion réseau dans le système d'exploitation est défini par l'utilisateur lors de la configuration de la connexion. Vous pouvez modifier le type de connexion réseau dans les paramètres de Kaspersky Endpoint Security. Le Pare-feu contrôle l'activité réseau en fonction du type de réseau spécifié dans les paramètres de Kaspersky Endpoint Security, et non pas du système d'exploitation.

Les types de connexion réseau suivants sont disponibles :

- **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 le type *Réseau public* au réseau Internet. Vous ne pouvez pas modifier le type de 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 un 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	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. 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. 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. Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau pour les applications.
Réseaux disponibles	Le tableau qui contient les informations sur les connexions réseau que le Pare-feu a détectées sur l'ordinateur de l'utilisateur. Le réseau Internet reçoit par défaut l'état *Réseau public*. Vous ne pouvez pas modifier l'état du réseau Internet.
Règles pour les applications	**Application**. 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. 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. **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.

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 un ordinateur et que le système d'exploitation le reconnait 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 correctement saisi, l'application enregistre les paramètres d'identification, à savoir le VID/PID du clavier et le numéro du port auquel il est connecté, 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. Vous pouvez configurer le nombre de tentatives de saisie du code numérique. En cas de plusieurs saisies erronées du code numérique ou si la fenêtre d'autorisation de clavier (cf. Illustration ci-dessous) est fermée, l'application bloque la saisie depuis ce clavier. Si la durée de blocage de l'appareil USB arrive à échéance 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.

Autorisation de clavier

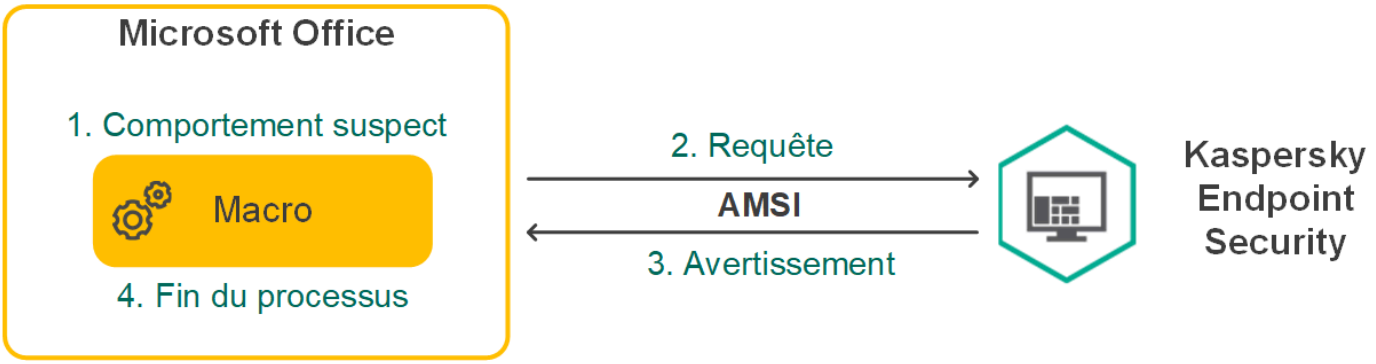
Paramètres du module Protection BadUSB

Paramètre	Description
Interdire l'utilisation du Clavier virtuel pour l'autorisation des appareils USB	Si le commutateur est activé, l'application bloque l'utilisation du clavier virtuel pour autoriser l'appareil USB à partir duquel la saisie du code d'autorisation est impossible.
Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB	Si ce commutateur est activé, l'application n'affiche pas le code-barres dans la notification d'authentification du lecteur de code-barres.
Nombre maximal de tentatives d'autorisation des appareils USB	Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Endpoint Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation.
Délai d'attente lorsque le nombre maximal de tentatives est atteint	La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).

Protection AMSI

Le module Protection AMSI est destiné à prendre en charge 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, veuillez consulter 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, une application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt l'action).



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 protection AMSI ne refuse pas les demandes provenant d'applications tierces pour lesquelles l'intégration continue avec le module de protection AMSI est activée.

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/Enterprise multi-session
- Windows 11 Home/Pro/Pro for Workstations/Education/Enterprise/Enterprise multi-session
- Windows Server 2016 Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2019 Essentials/Standard/Datacenter (y compris le mode Server Core) ;
- Windows Server 2022 Standard/Datacenter/Datacenter: Azure Edition (y compris le mode Server Core) ;
- Serveur Windows 2025 Standard/Datacenter.

Paramètres de protection AMSI

Paramètre	Description
Analyser les archives	Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).
Analyser les paquets de distribution	Analyse des paquets de distribution des applications tierces.
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. L'application analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.
Ne pas décompresser les fichiers composés volumineux	Si la case est cochée, l'application n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie. Si la case est décochée, l'application analyse les fichiers composés, quelle que soit leur taille. L'application analyse les fichiers volumineux extraits des archives, que la case soit cochée ou non.

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.

Le module Protection contre les Exploits surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus.

Paramètres du module Protection contre les Exploits

Paramètre	Description
En cas de détection d'un exploit	**Bloquer**. 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. **Informer**. 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.
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 repose sur les modèles de comportement dangereux et garantit la protection proactive de l'ordinateur.

Le module Détection comportementale surveille en outre les ports réseau à la recherche de processus applicatifs susceptibles de menacer la sécurité de l'ordinateur. L'application obtient des informations sur de tels processus auprès des bases antivirus.

Paramètres du module Détection comportementale

Paramètre	Description
Action exécutée lors de la détection d'une activité malveillante	**Supprimer**. 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. **Bloquer**. Si cette option est sélectionnée, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application. **Informer**. 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.

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 *privilèges 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 module 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. 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.

Paramètre	Description
Privilèges des applications	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. 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. Les privilèges d'accès de l'application figurent dans les tableaux suivants : • **Fichiers et base de registre**. Tableau des droits d'accès aux ressources du système d'exploitation et aux données personnelles pour les applications appartenant au groupe de confiance. • **Privilèges**. Tableau des droits d'accès aux processus et aux ressources du système d'exploitation pour les applications appartenant au groupe de confiance. • **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	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.
Groupe de confiance pour les programmes lancés 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 règles pour les programmes inconnus jusqu'ici de 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. 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.
Supprimer les règles pour les programmes qui n'ont pas été lancés depuis plus de X jours (de 1 à 90)	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 : • 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. 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. Au prochain lancement de l'application, Kaspersky Endpoint Security l'examine comme au premier lancement.
Groupe de confiance pour les applications non incluses dans d'autres groupes	La liste déroulante dont les éléments déterminent le groupe de confiance dans lequel Kaspersky Endpoint Security va placer l'application inconnue. Vous avez le choix entre les options suivantes : • **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 l'analyse des logiciels malveillants.

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.

La fonctionnalité KSN peut ne pas être disponible dans le logiciel aux États-Unis.

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 à Kaspersky Security Network, Kaspersky Endpoint Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés. Pour en savoir plus sur la configuration de l'accès à KSN, consultez l'aide de Kaspersky Security Center.

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.

L'infrastructure des bases de données de réputation de Kaspersky

Kaspersky Endpoint Security prend en charge les solutions d'infrastructure suivantes pour utiliser les bases de données de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky 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.

- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

Paramètre	Description
Activer le mode étendu de 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. Quelle que soit la position du commutateur, Kaspersky Endpoint Security utilise KSN pour détecter les menaces.
Activer le mode Cloud	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. 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. Kaspersky Endpoint Security télécharge la version allégée des bases antivirus lors de la première mise à jour après que la case a été cochée. Si le commutateur est désactivé, Kaspersky Endpoint Security utilise la version complète des bases antivirus. Kaspersky Endpoint Security télécharge la version complète des bases antivirus lors de la première mise à jour après que la case a été décochée.
État de l'ordinateur en cas d'indisponibilité de KSN *(disponible uniquement dans Kaspersky Security Center Console)*	Liste déroulante dont les éléments déterminent l'état de l'ordinateur dans Kaspersky Security Center quand les serveurs KSN ne sont pas accessibles.
Utiliser le Serveur d'administration comme serveur proxy KSN *(disponible uniquement dans Kaspersky Security Center Console)*	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 Kaspersky Security Network si le serveur proxy KSN n'est pas disponible *(disponible uniquement dans Kaspersky Security Center Console)*	Si la case est cochée, Kaspersky Endpoint Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).

Inspection des journaux

Ce module est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs. Ce module n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail.

L'inspection des journaux surveille l'intégrité de l'environnement protégé en fonction de l'analyse du journal des événements Windows. Lorsque l'application détecte des signes de comportement atypique dans le système, elle en informe l'administrateur, car ce comportement peut indiquer une tentative de cyberattaque.

Kaspersky Endpoint Security analyse les journaux d'événements Windows et détecte les violations conformément aux règles. Le module inclut des règles prédéfinies. Les règles prédéfinies sont alimentées par une analyse heuristique. Vous pouvez également ajouter vos propres règles (règles personnalisées). Lorsqu'une règle se déclenche, l'application crée un événement avec l'état *Critique* (voir la figure ci-dessous).

Si vous souhaitez utiliser l'inspection des journaux, assurez-vous que les paramètres de sécurité de la stratégie d'audit sont configurés et que le système enregistre les événements pertinents (pour en savoir plus, consultez le site du Support Technique Microsoft).

Notification d'inspection des journaux

Paramètres de l'Inspection des journaux

Paramètre	Description
Règles prédéfinies	Liste des règles d'Inspection des journaux. Les règles prédéfinies incluent des modèles d'activité anormale sur l'ordinateur protégé. Une activité anormale peut signifier une tentative d'attaque.
Règles personnalisées	Liste des règles d'Inspection des journaux ajoutées par l'utilisateur. Vous pouvez définir vos propres critères de déclenchement de règle d'inspection des journaux. Pour ce faire, vous devez entrer un ID d'événement et sélectionner une source d'événement. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Vous pouvez également spécifier le journal d'une application tierce.

Protection contre le chiffrement

Le module Protection contre le chiffrement 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.

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.

Paramètre	Description
Exclusions par nom ou par adresse IP	**Exclusions par nom ou par adresse IP**. La liste des ordinateurs pour lesquels les tentatives de chiffrement des dossiers partagés ne sont pas traquées. 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 . **Exclusions selon un masque**. Exclusions de la zone de protection. L'exclusion d'un dossier de la zone de protection 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. 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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
Action en cas de détection d'une menace	• **Informer**. Si cette option est sélectionnée, lors de la détection d'une tentative de modification des fichiers dans les dossiers partagés, Kaspersky Endpoint Security ajoute des informations sur cette tentative à la liste des menaces actives, ajoute une entrée aux rapports locaux de l'interface de l'application et envoie des informations à Kaspersky Security Center sur l'activité malveillante détectée. • **Bloquer la connexion pendant (min) N min**. Si cette option est sélectionnée, lorsque Kaspersky Endpoint Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés. Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant (min) X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.
Zone de protection	La *zone de protection* est une liste de chemins d'accès aux dossiers partagés, dans laquelle Kaspersky Endpoint Security surveille l'activité des fichiers. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque. Par défaut, l'application identifie automatiquement les dossiers partagés et surveille l'activité des fichiers dans tous les dossiers.

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).

Pour utiliser le Contrôle Internet, vous devez procéder à la configuration initiale de l'application :

- Pour contrôler le trafic HTTPS, activez l'analyse des connexions sécurisées (activé par défaut).
- Sélectionnez les ports que Kaspersky Endpoint Security doit surveiller (par défaut, l'application surveille tous les ports).

- Sélectionnez les applications dont vous souhaitez que Kaspersky Endpoint Security contrôle le trafic. La plupart des navigateurs sont déjà présents dans la liste des applications recommandées par Kaspersky. Si votre navigateur ne figure pas dans la liste, ajoutez-le manuellement.

- Nous vous recommandons d'injecter un script d'interaction avec les pages Internet dans le trafic Internet (par défaut, l'injection de script est désactivée). 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.

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 graphiques*.

- **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 des suites bureautiques* uniquement pour la catégorie de sites *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.

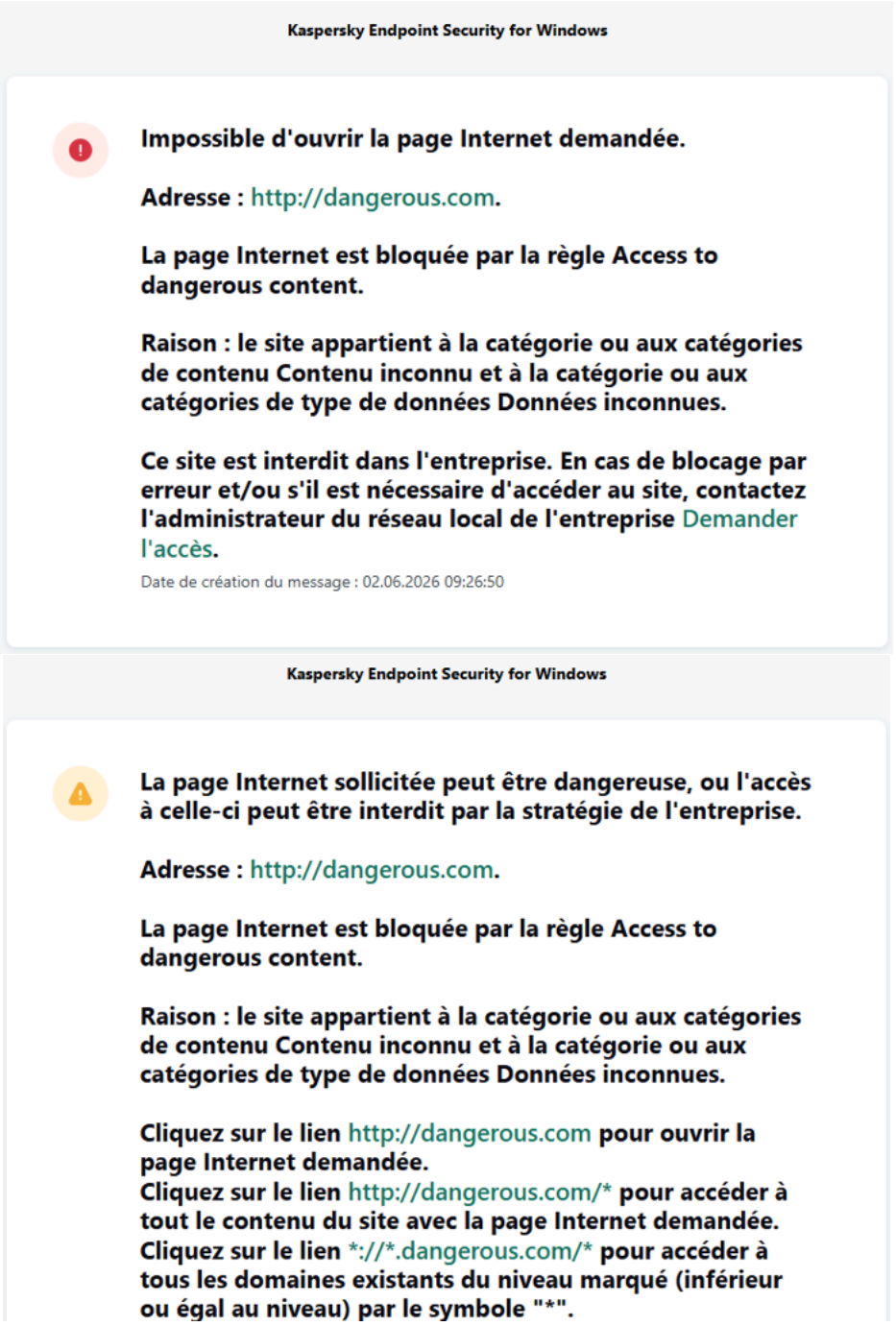
  Par exemple, vous pouvez limiter l'accès à Internet via un navigateur pour tous les utilisateurs de l'entreprise, à l'exception du service informatique.

- 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 *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.



Notifications du Contrôle Internet

Paramètre	Description
Règles d'accès aux sites	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 *règle par défaut* est une règle d'accès aux sites Internet qui ne figurent dans aucune des règles. Les options suivantes existent : • **Autoriser tout sauf la liste des règles**, également connue sous le mode liste de refus pour les sites Internet interdits. • **Interdire tout sauf la liste des règles**, également connue sous le mode liste d'autorisation pour les sites Internet autorisés.
Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée	Si la case est cochée, le Contrôle Internet met fin à la connexion aux ressources Internet bloquées immédiatement après l'application de la stratégie. Le navigateur arrête immédiatement le téléchargement des données à partir de la page Internet. Lorsque vous actualisez la page Internet ou accédez à une autre page Internet interdite, l'application affiche un avertissement. Le Contrôle Internet permet de déconnecter immédiatement des ressources Internet uniquement dans les navigateurs Internet. Pour les autres applications, le Contrôle Internet restreint uniquement les nouvelles connexions. Si la case est décochée, le Contrôle Internet restreint les nouvelles connexions aux ressources Internet interdites. Le Contrôle Internet ne met pas fin aux connexions actives.
Modèles	**Avertissement**. 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. **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 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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée. Des variables spéciales sont prévues pour la gestion du modèle du message, (par exemple, `%USER_NAME%`). Les variables permettent d'utiliser un seul modèle de message pour différents ordinateurs.
Enregistrer les données relatives aux visites des pages autorisées dans le journal	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. Navigateurs prenant en charge la fonction de surveillance : Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. La surveillance de l'activité des utilisateurs ne fonctionne pas dans les autres navigateurs. Il se peut que la surveillance de l'activité des utilisateurs sur Internet requiert davantage de ressources informatiques lors du déchiffrement du trafic HTTPS.

Contrôle des appareils

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à un 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.

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 **Avancé** → **Stockages** → **Matériel**.

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 – ⊘.
  - Selon les règles (imprimantes et appareils portables uniquement) – .
  - Dépend du bus de connexion (sauf Wi-Fi) – .
  - Interdire avec des exceptions (Wi-Fi uniquement) – .

- **Bus de connexion**. Un *bus de connexion* est une interface qui permet de connecter des appareils à l'ordinateur (USB, FireWire, etc.). Si le mode **Dépend du bus de connexion** est sélectionné pour le type d'appareil, l'application autorise ou interdit l'accès à l'appareil en fonction de l'interface de connexion (par exemple, 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 en fonction des données suivantes :

  - **Appareils en fonction de l'identifiant**. 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'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers.

  - **Appareils en fonction du modèle**. Chaque appareil possède un Vendor ID (VID) et un 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.

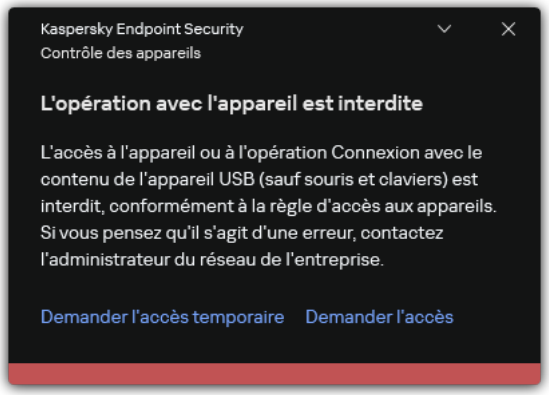
  - **Appareils en fonction du masque de l'identifiant**. Si vous utilisez plusieurs appareils avec des identifiants similaires, vous pouvez ajouter des appareils à la liste de confiance à l'aide de masques. Le caractère `*` remplace n'importe quelle combinaison de caractères. Kaspersky Endpoint Security 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 des PID similaires (par exemple, des appareils du même fabricant), vous pouvez ajouter des appareils à la liste 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.

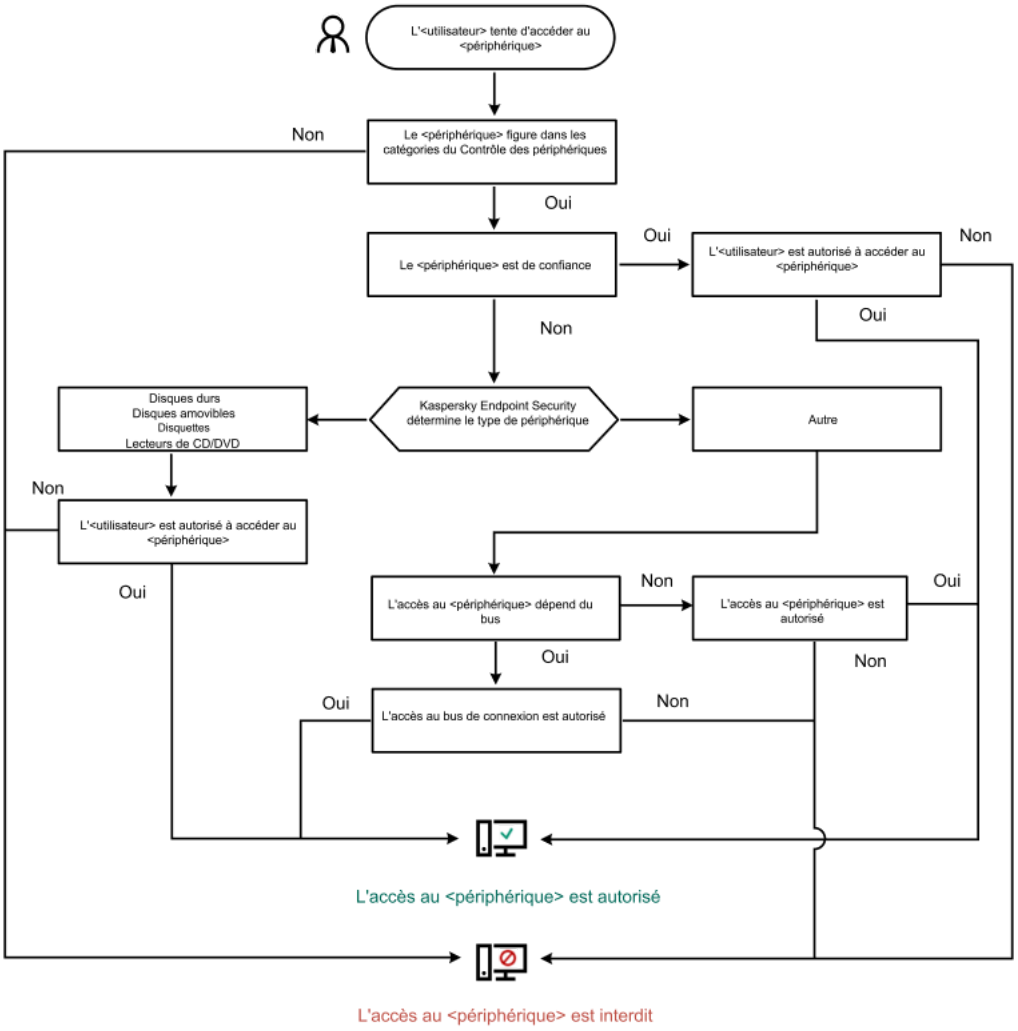
Quand l'appareil se connecte à un ordinateur auquel l'accès est interdit par le Contrôle des appareils, Kaspersky Endpoint Security bloque l'accès et affiche une notification (cf. ill. ci-dessous).



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.

Paramètre	Description
Autoriser les demandes d'accès temporaire *(disponible uniquement dans Kaspersky Security Center Console)*	Si la case est cochée, alors le bouton **Demander l'accès** dans l'interface locale de Kaspersky Endpoint Security est accessible. Cette bouton permet à l'utilisateur de demander un accès temporaire à l'appareil bloqué.
Appareils et réseaux Wi-Fi	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.
Bus de connexion	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. Kaspersky Endpoint Security autorise ou interdit l'accès aux appareils selon le type de connexion au bus si le mode **Dépend du bus de connexion** est sélectionné.
Appareils de confiance	Liste des appareils de confiance et des utilisateurs autorisés à accéder à ceux-ci.
Regrouper les valeurs après l'héritage *(disponible uniquement dans Kaspersky Security Center Console)*	Ce paramètre permet de fusionner la liste des appareils 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. 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'appareils de confiance commune pour l'ensemble de l'organisation. Les éléments de liste hérités dans une stratégie enfant ne peuvent pas être supprimés ni modifiés. Les éléments de la liste des appareils 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. 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. 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. Cette fonctionnalité permet également de fusionner des listes dans des profils de stratégie. Pour fusionner des listes, activez l'héritage des paramètres d'un profil de priorité inférieure dans le profil de priorité la plus élevée. Pour en savoir plus sur les priorités du profil de stratégie, consultez l'aide de Kaspersky Security Center.
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. 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. 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. 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. Anti-Bridging est compatible avec les types d'appareil suivants : carte réseau, Wi-Fi et modem.
Modèles des messages	**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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'accès à l'appareil**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

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* ou une autre catégorie), 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. L'administrateur peut créer de nombreuses règles. Une application peut correspondre aux critères de plusieurs règles. Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Kaspersky Endpoint Security vérifie si une application correspond à une règle à chaque démarrage. Kaspersky Endpoint Security compare l'application de manière séquentielle à toutes les règles du Contrôle des applications.

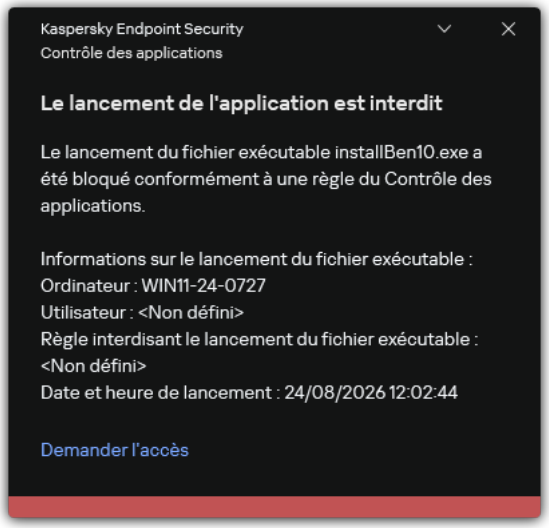
3. Sélection du mode de fonctionnement du Contrôle des applications.

   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.

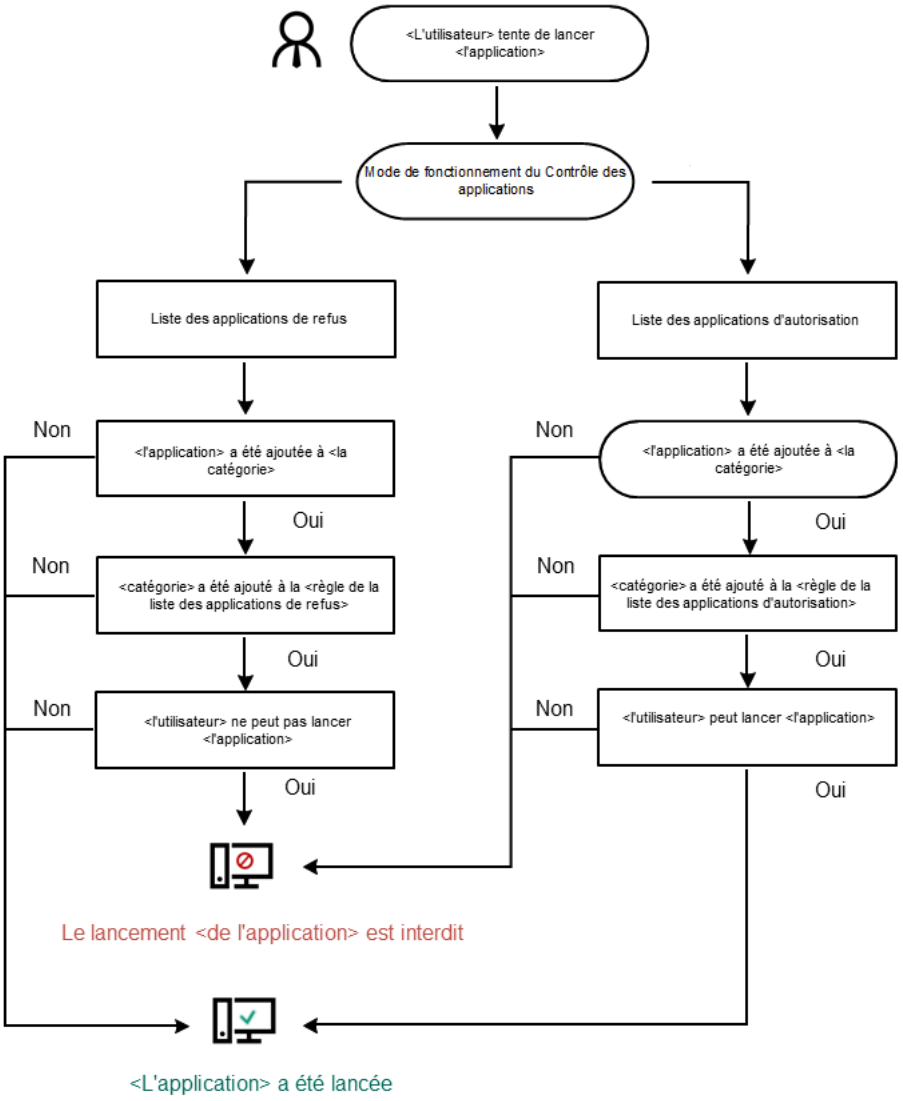
  Les règles de Contrôle des applications créées dans la Console d'administration de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.

- 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

Paramètre	Description
Action exécutée lors du lancement d'applications bloquées par des règles	**Appliquer les règles**. Kaspersky Endpoint Security gère le démarrage des applications selon le mode sélectionné. **Tester les règles**. 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 de l'application dans le rapport.
Mode de contrôle de démarrage de l'application	Vous avez le choix entre les 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. Le choix du mode **Liste d'autorisation** entraîne la création automatique de deux règles du Contrôle des applications : • **Catégorie principale**. • **Programmes de mise à jour de confiance**. Il est impossible de modifier les paramètres et de supprimer les règles créées automatiquement. Vous pouvez activer ou désactiver ces règles.
Surveiller le chargement des modules DLL	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. Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Catégorie principale** ou toute autre règle qui contient la catégorie KL "**Catégorie principale\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 **Catégorie principale** est désactivée peut provoquer l'instabilité du système d'exploitation. 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.
Utiliser une vérification stricte de la signature numérique	Vous pouvez sélectionner un certificat comme condition de déclenchement d'une règle du Contrôle des applications. Si cette case est cochée, Kaspersky Endpoint Security applique les règles aux applications signées avec des certificats provenant uniquement du magasin de certificats du système de confiance. Les applications signées avec de tels certificats sont également considérées comme de confiance par les modules de protection, par exemple la tâche *Analyse des logiciels malveillants*. En revanche, si vous spécifiez un certificat provenant d'un autre magasin dans une règle de Contrôle des applications, Kaspersky Endpoint Security n'applique pas une telle règle. Si la case est décochée, Kaspersky Endpoint Security applique les règles aux applications signées à l'aide d'un certificat provenant du Magasin de certificats racines de confiance de Windows. Ces applications ne font pas partie de la zone de confiance. Les modules de protection surveillent l'activité de telles applications.
Modèles de messages sur le blocage d'applications	**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. **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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction du lancement de l'application**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Contrôle évolutif des anomalies

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 suite 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 les 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 **Déclenchements de règles dans le mode Apprentissage intelligent**.

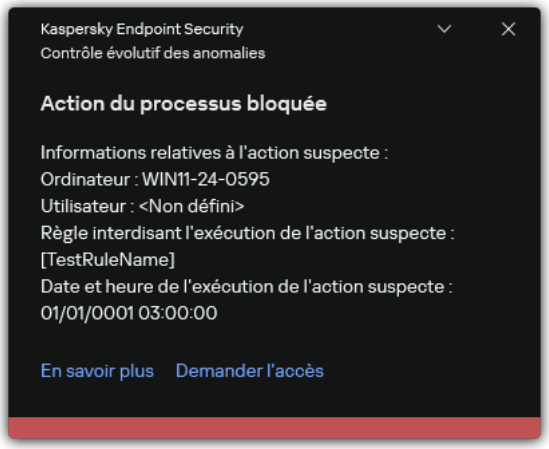
2. Analyse du rapport sur les déclenchements des règles

   L'administrateur analyse le rapport sur le déclenchement des règles ou le contenu du stockage **Déclenchements de règles dans le mode Apprentissage intelligent**. 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 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 **Déclenchements de règles dans le mode Apprentissage intelligent**. Nous vous recommandons de vérifier le rapport sur le déclenchement des règles et le contenu du stockage **Déclenchements de règles dans le mode Apprentissage intelligent**.

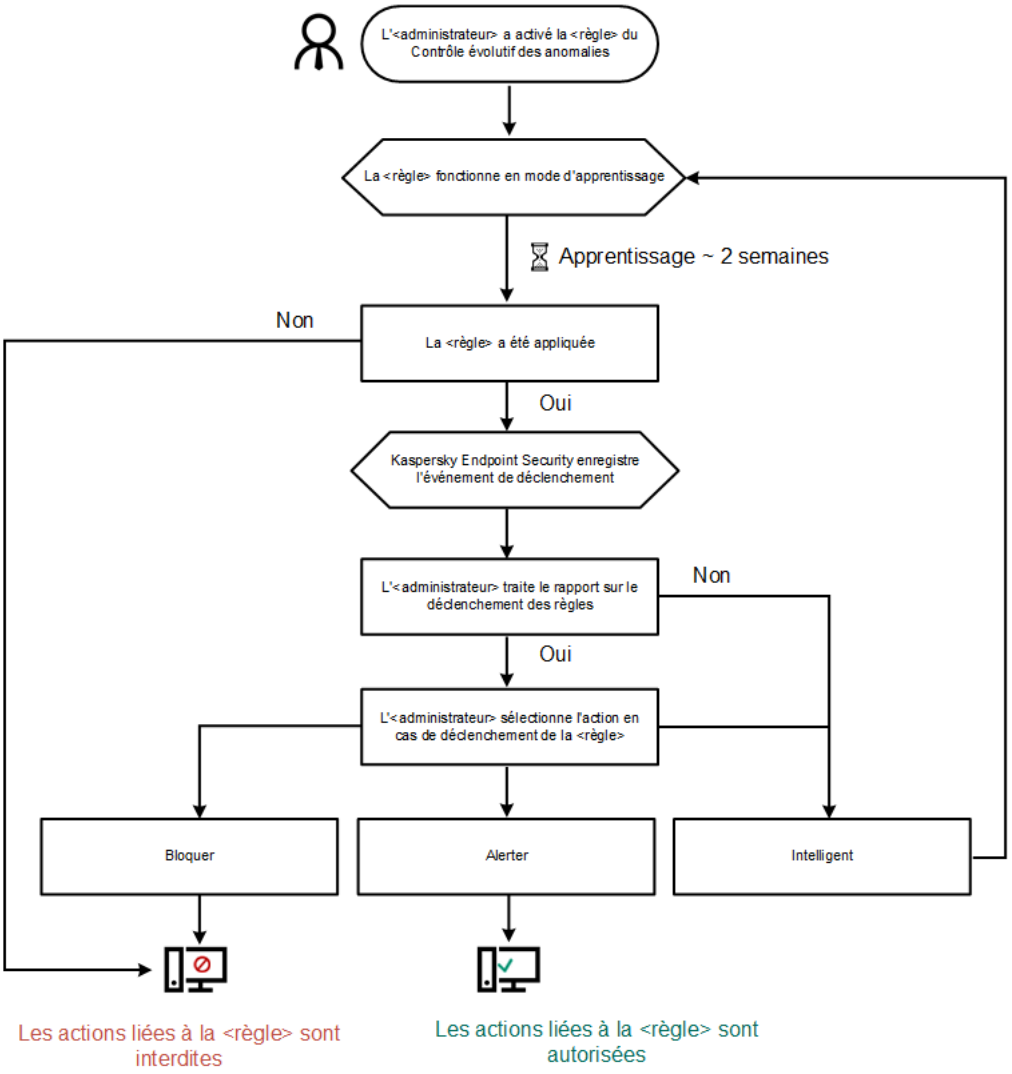
Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



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 du Contrôle évolutif des anomalies *(disponible uniquement dans Kaspersky Security Center Console)*	Ce rapport contient des informations sur l'état des règles de détection du Contrôle évolutif des anomalies (par exemple, les états *Désactivé* ou *Bloquer*). Le rapport est créé pour tous les groupes d'administration.
Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies *(disponible uniquement dans Kaspersky Security Center Console)*	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.

Paramètre	Description
Règles	Tableau des règles du Contrôle évolutif des anomalies Ces règles sont créées par les experts de Kaspersky sur la base des scénarios typiques d'action malveillantes.
Modèles	**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. Après que l'utilisateur a demandé l'autorisation d'accès, Kaspersky Endpoint Security envoie un événement à Kaspersky Security Center : **Message envoyé à l'administrateur sur l'interdiction de l'action de l'application**. La description de l'événement contient un message adressé à l'administrateur avec des variables substituées. Vous pouvez consulter ces événements dans la console de Kaspersky Security Center à l'aide de la sélection d'événements prédéfinie **Requêtes des utilisateurs**. Si votre organisation n'a pas déployé Kaspersky Security Center ou s'il n'y a pas de connexion au Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

Contrôle de l'intégrité du système

Ce module est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous le système d'exploitation Windows pour serveurs. Ce module n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur tournant sous le système d'exploitation Windows pour postes de travail.

À partir de la version 12.6, Kaspersky Endpoint Security for Windows inclut le module Contrôle de l'intégrité du système au lieu du module Contrôle de l'intégrité des fichiers. Le module Contrôle de l'intégrité du système inclut toutes les fonctionnalités du Contrôle de l'intégrité des fichiers et permet également de surveiller les modifications apportées au registre et la connexion d'appareils externes.

Le module Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Endpoint Security génère les événements correspondants et en informe l'administrateur. Le Contrôle de l'intégrité du système peut fonctionner en mode temps réel et peut également effectuer des vérifications de l'intégrité du système sur demande.

Contrôle de l'intégrité du système en temps réel

En mode temps réel, le Contrôle de l'intégrité du système suit les modifications apportées aux objets que vous avez inclus dans le champ d'application du module (la *zone de surveillance*). Le Contrôle de l'intégrité du système permet également de bloquer en temps réel l'accès non autorisé à ces objets.

Vérification de l'intégrité du système sur demande

La Vérification de l'intégrité du système sur demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Pour exécuter la tâche *Vérification de l'intégrité du système*, vous devez configurer la zone d'application du module (la *zone de surveillance*) et créer une référence. Une *référence* est un état enregistré des objets dans le système, que l'application utilise comme référence lors de la comparaison avec l'état actuel.

Paramètres du Contrôle de l'intégrité du système

Paramètre	Description
Mode de fonctionnement des règles de blocage	• **Bloquer**. Dans ce mode, le Contrôle de l'intégrité du système bloque les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant. • **Informer**. Dans ce mode, le Contrôle de l'intégrité du système autorise les actions avec les fichiers et les clés de registre provenant de la zone de surveillance et génère un événement correspondant.
Contrôle de l'intégrité du système en temps réel	En mode temps réel, le Contrôle de l'intégrité du système suit les modifications apportées aux objets que vous avez inclus dans le champ d'application du module (la *zone de surveillance*). Le Contrôle de l'intégrité du système permet également de bloquer en temps réel l'accès non autorisé à ces objets.
Surveiller les appareils	Le Contrôle de l'intégrité du système surveille la connexion et la déconnexion des appareils externes.
Surveiller les fichiers et le registre	Le Contrôle de l'intégrité du système surveille les modifications apportées aux fichiers, aux dossiers et au registre.
Vérification de l'intégrité du système	La Vérification de l'intégrité du système sur demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Pour exécuter la tâche *Vérification de l'intégrité du système*, vous devez configurer la zone d'application du module (la *zone de surveillance*) et créer une référence. Une *référence* est un état enregistré des objets dans le système, que l'application utilise comme référence lors de la comparaison avec l'état actuel.

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 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 trois unités fonctionnelles :

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Vous pouvez acheter l'ensemble des unités fonctionnelles ou des unités fonctionnelles individuelles 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.

Sandbox

Kaspersky Endpoint Security for Windows inclut un agent intégré permettant l'intégration avec la solution Kaspersky Sandbox. Le module *Sandbox* détecte et bloque automatiquement les menaces avancées sur les ordinateurs. Sandbox analyse le comportement des objets pour détecter les activités malveillantes et les activités caractéristiques d'attaques ciblées sur l'infrastructure informatique de l'organisation. Sandbox analyse les objets sur des serveurs spéciaux sur lesquels des images virtuelles des systèmes d'exploitation Microsoft Windows (serveurs Sandbox) ont été déployées. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Sandbox et Kaspersky Anti Targeted Attack Platform.

À partir de la version 12.7, Kaspersky Endpoint Security for Windows prend en charge le module Sandbox qui fait partie de la solution Kaspersky Anti Targeted Attack Platform. Contrairement à la solution Kaspersky Sandbox, le module KATA Sandbox permet non seulement d'analyser les fichiers automatiquement, mais aussi manuellement depuis le menu contextuel du fichier.

KATA Sandbox requiert Kaspersky Anti Targeted Attack Platform 7.0 ou une version ultérieure pour être déployé.

Le module peut être administré uniquement à l'aide de Kaspersky Security Center Web Console. Vous ne pouvez pas gérer ce module à l'aide de la Console d'administration (MMC).

Paramètres du module Sandbox

Paramètre	Description
Mode d'intégration	**Kaspersky Sandbox**. Intégration avec la solution Kaspersky Sandbox. L'application envoie les fichiers à analyser dans Kaspersky Sandbox uniquement en mode automatique. **KATA Sandbox**. Intégration au module Sandbox de la solution Kaspersky Anti Targeted Attack Platform. Vous pouvez sélectionner le mode d'envoi des fichiers pour analyse : • **Manuel**. L'utilisateur envoie manuellement le fichier pour analyse à l'aide du menu contextuel (**Envoyer à la Sandbox**). • **Automatique**. L'application détecte automatiquement les objets et les envoie à la Sandbox pour analyse. • **Combiné**.
Paramètres de connexion au serveur	**Délai d'attente (ms.)**. Délai d'attente de connexion du serveur Sandbox (pour Kaspersky Sandbox) ou du serveur Central Node (pour KATA). Une fois le délai d'attente configuré écoulé, Kaspersky Endpoint Security envoie une requête au serveur suivant. Vous pouvez augmenter le délai d'attente de la connexion avec le serveur si votre vitesse de connexion est faible ou si la connexion est instable. Le délai d'attente recommandé pour les demandes est de 0.5 seconde ou moins. **File d'attente des requêtes**. Taille du dossier de la file d'attente des requêtes. Lors de l'envoi de plusieurs objets à l'analyse dans Sandbox, Kaspersky Endpoint Security crée une file d'attente des requêtes. Par défaut, la taille du dossier de la file d'attente des requêtes est limitée à 100 Mo. Lorsque la taille maximale est atteinte, Sandbox cesse d'ajouter de nouvelles requêtes à la file d'attente et envoie l'événement correspondant à Kaspersky Security Center. Vous pouvez configurer la taille du dossier de la file d'attente des requêtes en fonction de la configuration de votre serveur. **Certificat TLS du serveur**. Pour configurer une connexion sécurisée avec le serveur Sandbox (pour Kaspersky Sandbox) ou le serveur Central Node (pour KATA), vous devez préparer un certificat TLS. Il faut ensuite ajouter le certificat à l'ordinateur à l'aide d'une stratégie. Vous devez également ajouter le certificat au serveur Sandbox (pour Kaspersky Sandbox) ou au serveur Central Node (pour KATA). **Utiliser l'authentification bidirectionnelle** (uniquement pour KATA Sandbox). Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe.
Connexion aux serveurs Sandbox	**Kaspersky Sandbox**. Paramètres de connexion du serveur Sandbox. Les serveurs utilisent des images virtuelles déployées des systèmes d'exploitation Microsoft Windows pour exécuter les objets qui doivent être analysés. Vous pouvez saisir une adresse IP (IPv4 ou IPv6) ou un nom de domaine pleinement qualifié. **KATA Sandbox**. Paramètres de connexion au serveur Central Node. Central Node choisit les paramètres optimaux pour analyser et répartir la charge entre les serveurs Sandbox.
Action en cas de détection d'une menace	**Placer la copie en Quarantaine, supprimer l'objet**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime l'objet malveillant trouvé sur l'ordinateur. Avant de supprimer l'objet, Kaspersky Endpoint Security crée une copie de sauvegarde au cas où l'objet devrait être restauré ultérieurement. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine. **Lancer l'Analyse des zones critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage. **Créer la tâche Analyse IOC**. Si cette option est sélectionnée, Kaspersky Endpoint Security crée automatiquement la tâche *Analyse IOC (tâche autonome d'analyse IOC)*. Pour cette tâche, vous pouvez configurer le mode d'exécution, la zone d'analyse et l'action en cas de détection d'un IOC (*Placer la copie en Quarantaine, supprimer l'objet* ou *Lancer l'Analyse des zones critiques*). Pour modifier les autres paramètres de la tâche *Analyse IOC*, accédez aux paramètres de la tâche.
Zone de l'analyse IOC	**Zones de fichiers critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security effectue une analyse IOC uniquement dans les zones de fichiers critiques de l'ordinateur : la mémoire du noyau et les secteurs d'amorçage. **Zones de fichiers sur le disque système de l'ordinateur**. Si cette option est sélectionnée, Kaspersky Endpoint Security effectue une analyse IOC sur le disque système de l'ordinateur.
Exécuter la tâche Analyse IOC	**Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer la tâche *Analyse IOC* manuellement à tout moment. **Automatiquement**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute automatiquement la tâche *Analyse IOC* après la détection d'une menace. **Exécuter uniquement lorsque l'ordinateur est inactif**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute la tâche *Analyse IOC* si l'écran de veille est actif ou si l'écran est verrouillé. Si l'utilisateur déverrouille l'ordinateur, Kaspersky Endpoint Security interrompt la tâche. Cela signifie que la tâche peut prendre plusieurs jours.

Managed Detection and Response

Kaspersky Endpoint Security for Windows prend en charge l'intégration avec la solution Managed Detection and Response. La solution *Kaspersky Managed Detection and Response (MDR)* détecte et analyse automatiquement les incidents de sécurité dans votre infrastructure. Pour ce faire, MDR utilise les données de télémétrie reçues des terminaux et Machine learning. MDR envoie les données de l'incident aux experts de Kaspersky. Les experts peuvent alors traiter l'incident et, par exemple, ajouter une nouvelle entrée dans les bases antivirus. Les experts peuvent également émettre des recommandations sur le traitement de l'incident et, par exemple, suggérer d'isoler l'ordinateur du réseau. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Managed Detection and Response.

Paramètres de Managed Detection and Response

Paramètre	Description
Fichier de configuration MDR	Le fichier BLOB contient l'ID du client et des informations sur la licence de 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 l'aide de Kaspersky Managed Detection and Response.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Optimum (ci-après également « EDR Optimum »). À partir de la version 11.8.0, Kaspersky Endpoint Security for Windows inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Expert (ci-après également « EDR Expert »). *Kaspersky Endpoint Detection and Response* est une gamme de solutions destinées à protéger l'infrastructure informatique des entreprises contre les cybermenaces avancées. La fonctionnalité des solutions combine la détection automatique des menaces avec la capacité de réagir à ces menaces pour contrer les attaques avancées, notamment les nouveaux exploits, les ransomwares, les attaques sans fichier ainsi que les méthodes utilisant des outils système légitimes. EDR Expert offre davantage de fonctionnalités de surveillance et de réponse aux menaces que EDR Optimum. Pour en savoir plus à propos des solutions, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response passe en revue et analyse le développement des menaces et fournit au *personnel de sécurité* ou à l'*administrateur* les informations sur l'attaque potentielle qui sont nécessaires pour assurer une réponse rapide. Kaspersky Endpoint Detection and Response affiche les détails de l'alerte dans une nouvelle fenêtre. Une *alerte* est un événement dans l'infrastructure informatique de l'entreprise que l'application a identifié comme inhabituel ou suspect et qui peut présenter une menace de sécurité pour l'infrastructure informatique de l'entreprise. Les *Détails de l'alerte* sont un outil permettant de visualiser l'ensemble des informations collectées sur une menace détectée. Les détails de l'alerte reprennent par exemple l'histoire des fichiers qui apparaissent sur l'ordinateur. Pour en savoir plus à propos de la gestion des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum et l'aide de Kaspersky Endpoint Detection and Response Expert.

Vous pouvez configurer le module Endpoint Detection and Response Optimum dans Web Console et Cloud Console. Les paramètres du module Endpoint Detection and Response Expert (cloud) sont disponibles uniquement dans Cloud Console.

Paramètre	Description
Activer la journalisation avancée de l'activité du système	La télémétrie étendue améliore la précision de la détection IOC, mais utilise plus de ressources de l'ordinateur. Nous recommandons d'activer la télémétrie étendue sur l'ordinateur pour analyser les IOC de manière rétrospective. *Analyse IOC rétrospective* est un mode de la tâche *Analyse IOC* dans laquelle Kaspersky Endpoint Security recherche des indicateurs de compromission à l'aide des données pendant une certaine période. Ce mode est destiné à la recherche d'indicateurs de compromission à partir des données de télémétrie de l'ordinateur protégé, telles que l'activité réseau, les processus, les fichiers et d'autres données télémétriques. Si la télémétrie étendue est désactivée, Kaspersky Endpoint Security peut alterner les informations relatives aux indicateurs de compromission détectés.
Isolement du réseau	Isolation automatique de l'ordinateur du réseau en réponse aux menaces détectées. Lorsque l'isolation du réseau est activée, l'application coupe toutes les connexions actives et bloque toutes les nouvelles connexions TCP/IP sur l'ordinateur. L'application ne laisse actives que les connexions suivantes : • Les connexions indiquées dans Exclusions de l'isolation du réseau. • Les connexions amorcées par les services de Kaspersky Endpoint Security. • Les connexions amorcées par l'Agent d'administration de Kaspersky Security Center.
Déverrouiller automatiquement l'appareil isolé dans (heures)	L'isolation du réseau peut être désactivée automatiquement après un certain temps ou manuellement. Par défaut, Kaspersky Endpoint Security désactive l'isolation du réseau 5 heures après le début de l'isolation.
Exclusions d'isolement du réseau	Liste des règles pour les exclusions de l'isolation du réseau. Les connexions réseau qui correspondent aux règles ne sont pas bloquées sur les ordinateurs lorsque l'isolation du réseau est activée. Pour configurer les exclusions d'isolation du réseau, vous pouvez utiliser une liste de *profils réseau standard*. Par défaut, les exclusions comprennent les profils réseau contenant des règles qui assurent le fonctionnement ininterrompu des appareils avec les rôles de serveur DNS/DHCP et de client DNS/DHCP. Vous pouvez également modifier les paramètres des profils réseau standard ou définir des exclusions manuellement. Les exclusions définies dans les propriétés de la stratégie sont appliquées uniquement si l'isolation du réseau est activée automatiquement en réponse à une menace détectée. Les exclusions définies dans les propriétés de l'ordinateur sont appliquées uniquement si l'isolation du réseau est activée manuellement dans les propriétés de l'ordinateur dans la console Kaspersky Security Center ou dans les détails de l'alerte.
Prévention de l'exécution	Contrôlez l'exécution des fichiers exécutables et des scripts ainsi que l'ouverture des fichiers au format Office. Par exemple, vous pouvez empêcher l'exécution d'applications considérées comme étant non sécurisées sur l'ordinateur sélectionné. La prévention de l'exécution prend en charge un ensemble d'extensions de fichier Office et un ensemble d'interpréteurs de scripts. Pour utiliser le module Prévention de l'exécution, vous devez ajouter des règles de prévention de l'exécution. La *règle de prévention de l'exécution* est un ensemble de critères que l'application prend en compte lorsqu'elle réagit à l'exécution d'un objet, par exemple lorsqu'elle bloque l'exécution d'un objet. L'application identifie les fichiers par leur chemin d'accès ou leurs sommes de contrôle calculées à l'aide des algorithmes de hachage MD5 et SHA256.
Action sur l'exécution ou l'ouverture d'un objet interdit	**Bloquer et ajouter au journal des événements**. Dans ce mode, l'application bloque l'exécution des objets ou l'ouverture des documents qui correspondent aux critères des règles de prévention. L'application publie également un événement sur les tentatives d'exécution d'objets ou d'ouverture de documents dans le journal des événements Windows et dans le journal des événements de Kaspersky Security Center. **Ajouter au journal des événements**. Dans ce mode, Kaspersky Endpoint Security publie un événement sur les tentatives d'exécution d'objets exécutables ou d'ouverture de documents qui correspondent aux critères de la règle de prévention dans le journal des événements Windows et dans Kaspersky Security Center, mais ne bloque pas la tentative d'exécution ni d'ouverture de l'objet ou du document. Ce mode est sélectionné par défaut.
Règles de prévention de l'exécution	La *règle de prévention de l'exécution* est un ensemble de critères que l'application prend en compte lorsqu'elle réagit à l'exécution d'un objet, par exemple lorsqu'elle bloque l'exécution d'un objet. L'application identifie les fichiers par leur chemin d'accès ou leurs sommes de contrôle calculées à l'aide des algorithmes de hachage MD5 et SHA256.

Paramètre	Description
Cloud Sandbox	*Cloud Sandbox* est une technologie qui vous permet de détecter les menaces avancées sur les ordinateurs. Kaspersky Endpoint Security transmet automatiquement les fichiers détectés à Cloud Sandbox pour analyse. Cloud Sandbox exécute ces fichiers dans un environnement isolé pour identifier les activités malveillantes et décider de leur réputation. Les données de ces fichiers sont ensuite envoyées à Kaspersky Security Network. Par conséquent, si Cloud Sandbox a détecté un fichier malveillant, Kaspersky Endpoint Security effectuera l'action appropriée pour éliminer cette menace sur tous les ordinateurs où ce fichier est détecté. La technologie Cloud Sandbox est activée en permanence et est disponible pour tous les utilisateurs de Kaspersky Security Network, quel que soit le type de licence qu'ils utilisent. Si cette case est cochée, Kaspersky Endpoint Security activera le compteur des menaces détectées à l'aide de Cloud Sandbox dans la fenêtre principale de l'application sous **Technologies de détection des menaces**. Kaspersky Endpoint Security indiquera également la technologie de détection des menaces de Cloud Sandbox dans les événements des applications et dans le *Rapport sur les menaces* de la console de Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows prend en charge l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* est une solution de cybersécurité d'entreprise qui comprend des applications Kaspersky permettant à une organisation de se défendre contre la plupart des types de cyber-risques et de faire face aux scénarios de propagation des menaces les plus importants. Les modules EDR Expert (on-premises) sont déployés sur Open Single Management Platform (OSMP). Cette plateforme exécute des scénarios multiplateformes dans une interface unique et permet d'intégrer des applications Kaspersky avec des applications tierces dans un système de sécurité complet.

L'un des éléments centraux de la solution est *SIEM*. Le SIEM suit les événements provenant de tous les modules et les met en corrélation les uns avec les autres à l'aide de règles définies par le fournisseur et l'utilisateur. EDR Expert (on-premises) examine les données télémétriques et les journaux reçus de l'infrastructure de l'entreprise pour détecter automatiquement les attaques et permet d'enquêter sur les incidents à l'aide d'un graphique d'enquête unifié qui combine tous les événements collectés dans EDR Expert (on-premises), y compris les événements provenant des applications Kaspersky et des produits de sécurité informatique tiers.

Pour la réponse aux incidents avancés, EDR Expert (on-premises) utilise des scénarios prédéfinis et définis par l'utilisateur. Vous pouvez également utiliser des actions de réponse à partir d'applications tierces et des scénarios de réponse qui impliquent plusieurs applications.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows fonctionne avec le module Kaspersky Endpoint Detection and Response dans le cadre de la solution Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *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 trois unités fonctionnelles :

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Vous pouvez acheter l'ensemble des unités fonctionnelles ou des unités fonctionnelles individuelles séparément. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les informations relatives aux événements survenus sur l'ordinateur (données de télémétrie) sont envoyées au serveur Kaspersky Anti Targeted Attack Platform. Dans ce cas, Kaspersky Endpoint Security envoie également au serveur Kaspersky Anti Targeted Attack Platform des informations relatives aux menaces découvertes par l'application ainsi que des informations relatives aux résultats du traitement de ces menaces.

L'intégration de EDR (KATA) et NDR (KATA) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la console Kaspersky Anti Targeted Attack Platform, y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Paramètres d'Endpoint Detection and Response Expert (on-premises)

Paramètre	Description
Connexion aux serveurs de collecte de données télémétriques	Un *serveur de collection de télémétrie* est un serveur qui fait partie d'une solution SIEM et qui collecte, normalise, corrèle, analyse et stocke les informations relatives aux événements qui se produisent sur l'ordinateur. Configurez les éléments suivants pour la connexion aux serveurs de collecte des données télémétriques (KUMA) : • **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur. • **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe. Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.
Adresse et **Port** (serveurs de collecte de données télémétriques)	Paramètres de connexion aux serveurs de collecte de données télémétriques. Vous pouvez saisir une adresse IP (IPv4 ou IPv6). Vous pouvez ajouter plusieurs adresses de serveur de collecte de données télémétriques. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.
Envoyer les données télémétriques aux serveurs de collecte de données télémétriques	Cette fonctionnalité permet de désactiver complètement l'envoi de télémétrie au serveur KATA. Par exemple, si vous utilisez Kaspersky Anti Targeted Attack Platform avec une autre solution qui utilise également la télémétrie, vous pouvez désactiver l'envoi de la télémétrie pour KATA (EDR). Cela vous permet d'optimiser la charge du serveur pour ces solutions. Si vous avez déployé la solution Managed Detection and Response et KATA (EDR), vous pouvez utiliser la télémétrie MDR et créer des tâches Threat Response dans KATA (EDR). • **Envoyer la télémétrie avec l'IOA uniquement**. Cela permet d'optimiser la télémétrie et d'envoyer uniquement la télémétrie avec IOA. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. L'application compare le comportement actuel du système à ces règles et enregistre les événements qui indiquent une attaque ciblée. L'application utilise la technologie d'*analyse en continu* qui permet de suivre en temps réel ces événements. • **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes. • **Limiter le nombre de paquets d'événements par transmission**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements. Cette fonction permet de désactiver la mise en mémoire tampon des événements avant la synchronisation avec le serveur.
Activer la limitation des demandes	Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Configurez les paramètres de la télémétrie : • **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure. • **Pourcentage de la limite d'événement excédentaire**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

Paramètre	Description
Envoyer une demande de synchronisation au serveur toutes les (min.)	Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.
Connexion aux serveurs de réponse	Un *serveur de réponse* est un serveur pour la réception et l'analyse des données, l'étude du comportement d'objets et la publication des résultats. Configurez les éléments suivants pour la connexion aux serveurs de réponse : • **Délai d'attente (s.)**. Délai maximal de réponse du serveur. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur. • **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur. Vous pouvez obtenir un certificat TLS sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto sur la plateforme Open Single Management Platform (voir les instructions dans l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises)). Après avoir configuré les paramètres du serveur, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un conteneur crypto protégé par mot de passe.
Adresse et **Port** (serveurs de réponse)	Paramètres de connexion aux serveurs de réponse. Vous pouvez saisir une adresse IP (IPv4 ou IPv6). Vous pouvez ajouter plusieurs adresses de serveur de collecte de données télémétriques. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

Paramètres de Endpoint Detection and Response (KATA)

Paramètre	Description
Envoyer une demande de synchronisation au serveur toutes les (min.)	Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.
Connexion aux serveurs KATA	Configurez les éléments suivants pour la connexion au serveur Central Node : • **Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node. • **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). • **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe. Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.
Adresse et **Port** (serveurs KATA)	Paramètres de connexion aux serveurs Kaspersky Anti Targeted Attack Platform. Saisissez l'adresse IP (IPv4 ou IPv6) et le port du serveur Central Node auquel se connecter. Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

Paramètre	Description
Envoyer la télémétrie à KATA	Cette fonctionnalité permet de désactiver complètement l'envoi de télémétrie au serveur KATA. Par exemple, si vous utilisez Kaspersky Anti Targeted Attack Platform avec une autre solution qui utilise également la télémétrie, vous pouvez désactiver l'envoi de la télémétrie pour KATA (EDR). Cela vous permet d'optimiser la charge du serveur pour ces solutions. Si vous avez déployé la solution Managed Detection and Response et KATA (EDR), vous pouvez utiliser la télémétrie MDR et créer des tâches Threat Response dans KATA (EDR). Configurez les paramètres de la télémétrie : • **Délai maximal de transmission des événements (s.)**. L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes. • **Nombre maximal de paquets d'événements**. L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements. Le paramètre par défaut est de 1024 événements.
Activer la limitation des demandes	Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements. Configurez les paramètres de la télémétrie : • **Nombre maximal d'événements par heure**. L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure. • **Pourcentage de la limite d'événement excédentaire**. L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows fonctionne avec le module Kaspersky Network Detection and Response dans le cadre de la solution Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *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 trois unités fonctionnelles :

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Vous pouvez acheter l'ensemble des unités fonctionnelles ou des unités fonctionnelles individuelles séparément. Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security est installé sur chaque ordinateur de l'infrastructure informatique de l'entreprise et surveille en permanence les processus, les connexions réseau ouvertes ainsi que les fichiers en cours de modification. Les informations relatives aux événements survenus sur l'ordinateur (données de télémétrie) sont envoyées au serveur Kaspersky Anti Targeted Attack Platform. Dans ce cas, Kaspersky Endpoint Security envoie également au serveur Kaspersky Anti Targeted Attack Platform des informations relatives aux menaces découvertes par l'application ainsi que des informations relatives aux résultats du traitement de ces menaces.

L'intégration de EDR (KATA) et NDR (KATA) est configurée dans la console de Kaspersky Security Center. L'agent intégré est ensuite géré à l'aide de la console Kaspersky Anti Targeted Attack Platform, y compris l'exécution des tâches, la gestion des objets mis en quarantaine, l'affichage des rapports et d'autres actions.

Paramètre	Description
Paramètres de connexion au serveur	**Délai d'attente (s.)**. Délai maximal de réponse du serveur Central Node. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur Central Node. **Certificat TLS du serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur Central Node. Vous pouvez obtenir un certificat TLS dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur Central Node. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur Central Node, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Vous pouvez obtenir un conteneur crypto dans la console Kaspersky Anti Targeted Attack Platform (voir les instructions dans l'aide de Kaspersky Anti Targeted Attack Platform). Après avoir configuré les paramètres du Central Node, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un crypto-conteneur protégé par mot de passe. Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.
Adresse et **Port**	Paramètres de connexion aux serveurs Kaspersky Anti Targeted Attack Platform. Saisissez l'adresse IP (IPv4 ou IPv6) et le port du serveur Central Node auquel se connecter. Vous pouvez ajouter plusieurs adresses de serveur de nœud central. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.
Envoyer une demande de synchronisation au serveur NDR toutes les (min.)	Fréquence des requêtes de synchronisation envoyées au serveur. Lors de la synchronisation, Kaspersky Endpoint Security envoie des informations sur les paramètres et les tâches modifiés de l'application.
Délai maximal de transmission des événements (s.)	L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
Activer la limitation des demandes	Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application restreint la transmission des événements. Si le nombre d'événements dépasse les limites configurées, Kaspersky Endpoint Security arrête d'envoyer des événements.
Nombre maximal d'événements par heure	L'application analyse le flux de données de télémétrie et limite l'envoi d'événements si le flux d'événements dépasse la limite configurée du nombre d'événements par heure. Kaspersky Endpoint Security reprend l'envoi des événements après une heure. Le paramètre par défaut est de 3 000 événements par heure. Si l'application est installée sur un serveur, le flux de données de télémétrie est plus élevé. Pour les serveurs, il est recommandé d'augmenter la valeur à 60 000 événements par heure.
Pourcentage de la limite d'événement excédentaire	L'application trie les événements par type (par exemple, les événements "modifications du registre") et limite la transmission des événements si le rapport des événements du même type au nombre total d'événements dépasse la limite configurée en pourcentage. Kaspersky Endpoint Security reprend l'envoi d'événements lorsque le rapport entre les autres événements et le nombre total d'événements redevient suffisant. Le paramètre par défaut est de 15 %.

Intégration de KUMA

Kaspersky Endpoint Security for Windows prend en charge la solution Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* est une solution de gestion de la sécurité des informations et des événements (SIEM) pour l'infrastructure informatique des organisations. KUMA permet de détecter, d'analyser et d'atténuer les menaces à la sécurité avant qu'elles ne causent des dommages.

Paramètre	Description
Durée d'attente maximale pour l'envoi des événements (sec)	L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation. Le paramètre par défaut est de 30 secondes.
Connexion aux serveurs KUMA	**Délai d'attente (s.)**. Délai maximal d'attente d'une réponse du serveur KUMA (la valeur par défaut est de 5 secondes). À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur KUMA. **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur KUMA. Vous pouvez obtenir un certificat TLS dans la console de Kaspersky Unified Monitoring and Analysis Platform (consultez les instructions dans l'aide de Kaspersky Unified Monitoring and Analysis Platform). Pour établir une connexion de confiance, dans la console KUMA, dans les paramètres du connecteur tcp, vous devez sélectionner le **With verification** mode TLS (cf. aide de Kaspersky Unified Monitoring and Analysis Platform). **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre KES et KUMA. Pour utiliser l'authentification bidirectionnelle, vous devez sélectionner le mode TLS **Custom PFX with client authentication** dans les paramètres du connecteur de la console KUMA (consultez les paramètres du connecteur dans l'aide de Kaspersky Unified Monitoring and Analysis Platform). Ensuite, vous devez télécharger un certificat de serveur et définir un mot de passe pour protéger le conteneur crypto. Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.
Serveurs KUMA	Paramètres de connexion aux serveurs de Kaspersky Unified Monitoring and Analysis Platform. Vous pouvez saisir une adresse IP (IPv4 ou IPv6). Vous pouvez ajouter plusieurs adresses de serveur KUMA. Kaspersky Endpoint Security se connecte au serveur en utilisant la première adresse IP. Si une connexion ne peut être établie, Kaspersky Endpoint Security tente de se connecter en utilisant la deuxième adresse IP de la liste et ainsi de suite.

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

Kaspersky Disk Encryption n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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 *Administrer 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 Single Sign-On (SSO) 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 l'infrastructure Kaspersky Next. BitLocker chiffre le volume logique. BitLocker ne permet de pas de chiffrer les disques amovibles. Pour en savoir plus sur le fonctionnement de BitLocker, consultez la documentation de Microsoft.

> Lors du chiffrement du disque, BitLocker place le programme de démarrage et les autres fichiers auxiliaires dans la system partition. Cette partition n'est pas chiffrée. Lors de l'installation de Windows, le système d'exploitation crée la partition système automatiquement. Si le disque est entièrement partitionné avant l'installation de Windows, le système d'exploitation ne peut pas créer de partition système. Dans ce cas, lorsque vous démarrez le chiffrement de disque BitLocker, le système d'exploitation vous invite à repartitionner le disque et à créer une partition système. Une fois que vous aurez créé une partition système, le système d'exploitation lancera le chiffrement BitLocker.

BitLocker fournit un stockage sécurisé des clés d'accès à l'aide d'un module de plateforme sécurisée. *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 dur du système, l'utilisateur doit passer par l'authentification BitLocker pour lancer le système d'exploitation. Après l'authentification, BitLocker autorise l'utilisateur à se connecter. BitLocker n'est pas compatible avec la technologie d'authentification unique (SSO).

Après avoir chiffré le disque, BitLocker crée une clé de récupération. Kaspersky Endpoint Security envoie la clé de réserve 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 la clé de récupération et les informations sur le chiffrement du disque à Kaspersky Security Center.

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	**Chiffrer tous les disques durs**. Si vous choisissez cette option, l'application chiffre tous les disques durs lors de l'application de la stratégie. 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. **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. **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.
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.
Paramètres de création de comptes utilisateur de l'Agent d'authentification	**Tous les comptes de l'ordinateur**. Tous les comptes de l'ordinateur qui ont été actifs à un moment donné. **Tous les comptes de domaine de l'ordinateur**. Tous les comptes de l'ordinateur qui appartiennent à un domaine et qui ont été actifs à un moment donné. **Tous les comptes locaux de l'ordinateur**. Tous les comptes locaux de l'ordinateur qui ont été actifs à un moment donné. **Compte de service avec un mot de passe à usage unique**. Le compte de service est nécessaire pour accéder à l'ordinateur, par exemple lorsque l'utilisateur a oublié son mot de passe. Vous pouvez également utiliser le compte de service comme un compte de réserve. Vous devez saisir le nom du compte (par défaut, `ServiceAccount`). Kaspersky Endpoint Security crée automatiquement un mot de passe. Vous pouvez trouver le mot de passe dans Kaspersky Security Center Console. **Administrateur local**. Kaspersky Endpoint Security crée un compte utilisateur de l'Agent d'authentification pour l'administrateur local de l'ordinateur. **Gestionnaire de l'ordinateur**. Kaspersky Endpoint Security crée un compte utilisateur de l'Agent d'authentification pour le compte du gestionnaire de l'ordinateur. Vous pouvez déterminer quel compte présente le rôle de gestionnaire de l'ordinateur dans les propriétés de l'ordinateur dans Active Directory. Par défaut, le rôle de gestionnaire de l'ordinateur n'est pas défini, c'est-à-dire qu'il ne correspond à aucun compte. **Compte actif**. Kaspersky Endpoint Security crée automatiquement un compte d'Agent d'authentification pour le compte qui est actif au moment du chiffrement du disque.
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 *Administrer les comptes de l'Agent d'authentification* pour les ordinateurs avec des disques déjà chiffrés.
Enregistrer le nom d'utilisateur saisi dans l'Agent d'authentification	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.

Paramètre	Description
Chiffrer uniquement l'espace occupé (réduit la durée du chiffrement)	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. 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. Par défaut, la case est décochée.
Utiliser le Legacy USB Support (déconseillé)	La case active ou désactive la fonctionnalité 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'incidence 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 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.
Utiliser 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.
Emballer les fournisseurs de certification tiers	Kaspersky Endpoint Security prend en charge le fournisseur d'informations d'identification tiers ADSelfService Plus. Dans le cadre du recours à des fournisseurs d'informations d'identification tiers, l'Agent d'authentification intercepte le mot de passe avant le chargement du système d'exploitation. Cela signifie qu'un utilisateur doit saisir un mot de passe une seule fois lorsqu'il se connecte à Windows. Après s'être connecté à Windows, l'utilisateur peut utiliser les fonctionnalités offertes par un fournisseur d'informations d'identification tiers pour s'authentifier auprès de services d'entreprise, par exemple. Les fournisseurs d'informations d'identification tiers permettent également aux utilisateurs de réinitialiser leur propre mot de passe de façon indépendante. Dans ce cas, Kaspersky Endpoint Security mettra automatiquement à jour le mot de passe de l'Agent d'authentification. Si vous utilisez un fournisseur d'informations d'identification tiers qui n'est pas pris en charge par l'application, il se peut que vous rencontriez certaines limitations dans le fonctionnement de la technologie d'authentification unique.
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.

Paramètre	Description
Mode de chiffrement	**Chiffrer tous les disques durs**. Si vous choisissez cette option, l'application chiffre tous les disques durs lors de l'application de la stratégie. 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. **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. **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.
Autoriser l'utilisation de l'authentification BitLocker qui requiert une saisie au clavier avant le démarrage sur les tablettes	L'utilisation d'une 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). 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. 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. Si cette case est décochée, le chiffrement de disque BitLocker n'est pas possible sur les tablettes.
Utiliser le chiffrement au niveau matériel (Windows 8 et versions ultérieures)	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.
Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures)	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. 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. Par défaut, la case est décochée.

Paramètre	Description
Méthode d'authentification	**Mot de passe uniquement (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. **Trusted Platform Module (TPM)** Si vous avez choisi cette option, BitLocker utilise le Trusted Platform Module (TPM). *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 un 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. • **Trusted Platform Module (TPM) ou mot de passe si le TPM n'est pas disponible**. Si cette option est sélectionnée, 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. La méthode d'authentification sélectionnée doit être configurée en précisant les exigences en matière de mot de passe ou de code PIN : • **Longueur minimale du code PIN (caractères)** (la valeur par défaut est 6). • **Longueur minimale du mot de passe (caractères)** (la valeur par défaut est 8). • **Nombre maximal de mots de passe/codes PIN enregistrés** (la valeur par défaut est 5). • **Limiter la durée de validité du mot de passe/code PIN pour le TPM (jours)** (désactivé par défaut). • **Utiliser un code PIN amélioré (lettres et chiffres)**. Le *code PIN renforcé* permet l'utilisation d'autres caractères en plus des caractères numériques : lettres latines majuscules et minuscules, caractères spéciaux et espaces. Désactivé par défaut.
Recréer automatiquement la clé de récupération (jours)	Mettez automatiquement à jour le mot de passe pour restaurer l'accès à un disque protégé par BitLocker. Si la case est cochée, précisez la période de validité du mot de passe de la clé de récupération. Cette mesure permet d'éviter la réutilisation du mot de passe de la clé de récupération.

Chiffrement des fichiers

Le chiffrement des fichiers n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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.

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.

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
Mode de 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. **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. **Tout déchiffrer**. Si vous choisissez cette option, Kaspersky Endpoint Security déchiffre tous les fichiers et les dossiers chiffrés.

Paramètre	Description
Chiffrement	Cet onglet affiche les règles de chiffrement des fichiers enregistrés sur les disques locaux. Vous pouvez ajouter des fichiers comme suit : • **Dossiers standards**. Kaspersky Endpoint Security permet d'ajouter les zones suivantes : **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). • **Dossier personnalisé**. 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 : 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. 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 *Archives*. Vous pouvez également ajouter l'extension de fichier manuellement.
Déchiffrement	Cet onglet affiche les règles de déchiffrement des fichiers enregistrés sur les disques locaux.
Règles pour les applications	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.
Archives chiffrées	Paramètres de complexité des mots de passe lors de la création d'archives chiffrées.

Chiffrement des disques amovibles

Le chiffrement des disques amovibles n'est pas pris en charge sur les ordinateurs basés sur l'architecture ARM.

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 :

- Full Disk Encryption (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).

- File Level Encryption (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
Mode de chiffrement	**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. **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. **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. **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. **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.
Mode portable	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. 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. Le mode portable est disponible pour les modes **Chiffrer tous les fichiers** ou **Chiffrer uniquement les nouveaux fichiers**.

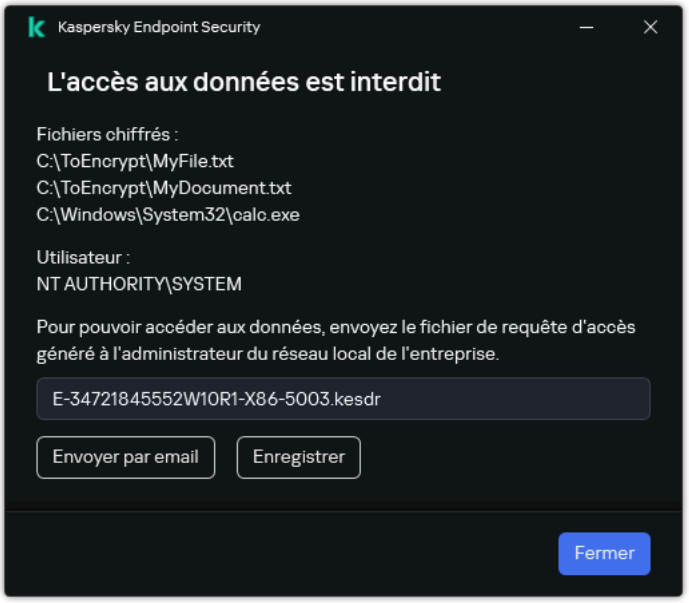
Paramètre	Description
Chiffrer uniquement l'espace occupé	La case active ou désactive le mode de chiffrement selon lequel seuls les secteurs occupés du disque sont chiffrés. Ce mode est recommandé pour les nouveaux disques dont les données n'ont pas été modifiées ou supprimées. Si la case est cochée, 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. Si la case est décochée, tout le disque est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant. La fonction de chiffrement réservé à l'espace utilisé est disponible uniquement pour le mode **Chiffrer tout le disque amovible**. 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.

Règles personnalisées	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 :
	
	• Ajoutez un disque amovible à partir de la liste des appareils de confiance du Contrôle des appareils.
	
	• Ajoutez un disque amovible manuellement :
	
	  • selon l'identificateur d'appareil (en anglais, Hardware ID - HWID) ;
	
	  • selon le modèle d'appareil : Vendor ID (VID) et Product ID (PID)

Autoriser le chiffrement des disques amovibles en mode hors ligne	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 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 des mots de passe de chiffrement/Gestionnaire de fichiers 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 tags pour filtrer les messages.
- **Message de l'utilisateur**. 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, en tenant compte des propriétés des objets gérés et des 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.

À partir de Kaspersky Endpoint Security 12.5 for Windows, vous pouvez ajouter la télémétrie EDR à la zone de confiance. Cette option permet d'optimiser les données que l'application envoie au serveur de collecte de données télémétriques pour la solution Kaspersky Anti Targeted Attack Platform (EDR).

À partir de Kaspersky Endpoint Security 12.6 for Windows, des exclusions de l'analyse et des applications de confiance sont ajoutées à la zone de confiance. Les exclusions de l'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Endpoint Security sur les serveurs SQL, les serveurs Microsoft Exchange et System Center Configuration Manager. Cela signifie que vous n'avez pas besoin de configurer manuellement une zone de confiance pour l'application sur les serveurs.

À partir de Kaspersky Endpoint Security 12.8 for Windows, vous pouvez installer l'application en mode Light Agent pour protéger les environnements virtuels. Les exclusions d'analyse et les applications de confiance prédéfinies peuvent vous aider à configurer rapidement Kaspersky Endpoint Security dans les environnements virtuels Citrix et VMware.

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 un ordinateur et aux données de l'utilisateur. De telles applications n'ont pas nécessairement de finalité malveillante, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que des individus malintentionnés peuvent utiliser pour compromettre l'ordinateur ou les données de l'utilisateur, consultez le site de l'Encyclopédie 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.
- Tâche *Analyse des logiciels malveillants*

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 surveille 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. Après l'ajout d'une application à la liste des applications de confiance, Kaspersky Endpoint Security cesse de surveiller l'activité de l'application.

La différence entre les exclusions d'analyse et les applications de confiance est que pour les exclusions, Kaspersky Endpoint Security n'analyse pas les fichiers, tandis que pour les applications de confiance, il ne contrôle pas les processus lancés. Si une application de confiance crée un fichier malveillant dans un dossier qui n'est pas inclus dans les exclusions d'analyse, Kaspersky Endpoint Security détectera le fichier et éliminera la menace. Si le dossier est ajouté aux exclusions, Kaspersky Endpoint Security ignorera ce fichier.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance afin que les objets utilisés par cette application ne soient pas surveillés. Cela augmentera les performances de l'ordinateur, ce qui est particulièrement important lors de l'utilisation d'applications serveur.

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.

Les applications de confiance permettent d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, le problème de la double analyse du trafic réseau d'un ordinateur tiers par Kaspersky Endpoint Security et par une autre application antivirus).

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre 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	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.

- **Virus et vers**

  Sous-catégorie : virus et vers (Viruses_and_Worms)

  Niveau de danger : 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 *Overwriting* remplacent le code du fichier infecté par leur propre code, effaçant ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *Parasitic* modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les virus *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-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	Name	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.
IM-Worm	Vers de client 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-Worm	Vers de chats	Ils se diffusent via les canaux Internet Relay Chats, des systèmes qui permettent de discuter en temps réel avec d'autres personnes. 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.
Net-Worm	Vers de réseau (vers de réseaux informatiques)	Ils se diffusent via les réseaux informatiques. 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.
P2P-Worm	Vers de réseau d'échange de fichiers	Ils se propagent via les réseaux d'échange de fichiers pair à pair. 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. 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.
Ver	Autres vers	Parmi ces autres vers, citons : • 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 (y compris les ransomwares)**

  Sous-catégories : chevaux de Troie (Trojan_programs)

Niveau de danger : 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	Name	Description
Trojan-ArcBomb	Chevaux de Troie (bombes dans les archives)	Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur. 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.
Backdoor	Chevaux de Troie pour l'administration à distance	Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs. 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.
Trojan	Chevaux de Troie	Cette catégorie reprend les programmes malveillants suivants : • **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	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 : • 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-PSW	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 « attaquant » 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	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	Name	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". 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. Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploites de type Nuker sont des paquets réseau qui mettent l'ordinateur hors service.
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.
Spoofer	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.
IM-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.

- **Logiciel publicitaire**

  Sous-catégorie : Logiciels publicitaires (Adware)

  Niveau de danger : Moyen

  Les logiciels 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	Name	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.
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.

- **Programme légitime qui peut être utilisé par des intrus 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	Name	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.
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.

- **Objets compactés pouvant dissimuler un programme malveillant**

  Sous-catégorie : fichiers compressés susceptibles de causer des dommages.

  Niveau de danger : Moyen.

  Le fichier est compressé à l'aide d'un outil de compression spécial utilisé pour contenir des programmes malveillants : virus, vers, chevaux de Troie. Kaspersky Endpoint Security analyse le module de décompression dans les archives autoextractibles SFX.

  Pour dissimuler les programmes malveillants afin qu'ils ne soient pas détectés par un antivirus, les pirates informatiques les compressent à l'aide d'empaqueteurs spéciaux. Les experts de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

- **Objets compactés à plusieurs reprises**

  Sous-catégorie : fichiers compressés susceptibles de causer des dommages.

  Niveau de danger : Moyen.

  Le fichier est compressé à l'aide d'un outil de compression spécial utilisé pour contenir des programmes malveillants : virus, vers, chevaux de Troie. Kaspersky Endpoint Security analyse le module de décompression dans les archives autoextractibles SFX.

  Pour dissimuler les programmes malveillants afin qu'ils ne soient pas détectés par un antivirus, les pirates informatiques les compressent à l'aide d'empaqueteurs spéciaux. Les experts de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

Exclusions	Tableau contenant les informations relatives aux exclusions de l'analyse.
	
	Nous recommandons d'utiliser des chemins relatifs plutôt que des chemins absolus. Cela permet d'exclure non seulement les objets du système de fichiers, mais aussi les objets sans fichier. Par exemple, `*\Program Files (x86)\Folder\Subfolder`.
	
	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:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` 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:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
	
	  Vous pouvez utiliser des masques n'importe où dans un chemin de fichier ou de dossier. Par exemple, si vous souhaitez que la zone d'analyse inclue le dossier Téléchargements pour tous les comptes sur l'ordinateur, saisissez le masque `C:\Users\*\Downloads\`.
	
	  Kaspersky Endpoint Security prend en charge les variables d'environnement
	
	  Kaspersky Endpoint Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'exclusions à l'aide de 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.
	
	• Saisissez le nom du type d'objet en fonction de 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, l'application exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.
	
	Kaspersky Endpoint Security masque la liste des exclusions d'analyse dans l'interface utilisateur de l'application si la configuration des exclusions d'analyse est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les exclusions d'analyse locales sont interdites (la case **Autoriser l'utilisation des exclusions locales** est décochée).

Applications de confiance	Tableau des applications de confiance dont l'activité n'est pas analysée par Kaspersky Endpoint Security. 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 dans 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. 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. Kaspersky Endpoint Security masque la liste consolidée des applications de confiance dans l'interface utilisateur de l'application si la configuration des applications de confiance est bloquée par l'administrateur dans la console (symbole « cadenas fermé ») et si les applications de confiance locales sont interdites (la case **Autoriser l'utilisation des applications de confiance** est décochée).
Regrouper les valeurs après l'héritage *(disponible uniquement dans Kaspersky Security Center Console)*	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. 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. 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. 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. 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. Cette fonctionnalité permet également de fusionner des listes dans des profils de stratégie. Pour fusionner des listes, activez l'héritage des paramètres d'un profil de priorité inférieure dans le profil de priorité la plus élevée. Pour en savoir plus sur les priorités du profil de stratégie, consultez l'aide de Kaspersky Security Center.
Autoriser l'utilisation des exclusions locales/Autoriser l'utilisation des applications de confiance *(disponible uniquement dans Kaspersky Security Center Console)*	*Exclusions locales et applications locales de confiance (zone locale de confiance)* : 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 proposée par une stratégie. 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. 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.
Télémétrie EDR (KATA) / NDR (KATA) *(disponible uniquement dans Kaspersky Security Center Console)*	Tableau contenant les informations relatives aux exclusions de la télémétrie EDR.
Télémétrie KUMA *(disponible uniquement dans Kaspersky Security Center Console)*	Liste des événements à envoyer à Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security fonctionne dans les modes suivants : • **Envoyer tous les événements**. Dans ce mode, l'application envoie tous les événements du journal Windows à l'exception des événements ajoutés aux règles d'exclusion. • **Envoyer uniquement les événements sélectionnés**. Dans ce mode, l'application envoie uniquement les événements ajoutés dans les règles d'inclusion.
Boutique des certificats système de confiance	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 **De confiance**. 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 l'application au démarrage de l'ordinateur (recommandé)	Si cette option est sélectionnée, 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. Lorsque cette option est désélectionnée, 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.
Utiliser la technologie de la désinfection avancée (requiert des ressources informatiques considérables)	En règle générale, Kaspersky Endpoint Security élimine les programmes malveillants détectés avant que l'ordinateur ne soit infecté. La technologie de désinfection avancée protège l'ordinateur des programmes malveillants déjà actifs (infection active), minimisant ainsi le risque de perte de données et de propagation de la menace. Si cette technologie est activée, lorsqu'une activité malveillante est détectée, Kaspersky Endpoint Security affiche une fenêtre contextuelle de notification. Dans sa notification, Kaspersky Endpoint Security propose à l'utilisateur d'effectuer une réparation de l'infection active. Si l'utilisateur confirme l'exécution de la procédure, Kaspersky Endpoint Security neutralise la menace, puis redémarre l'ordinateur. La technologie de désinfection avancée utilise des ressources informatiques considérables, ce qui peut ralentir d'autres applications. Quand l'application recherche la présence éventuelle d'une infection active, certaines fonctions du système d'exploitation peuvent être indisponibles. La disponibilité du système d'exploitation est rétablie lorsque la Désinfection de l'infection active est terminée et après le redémarrage de l'ordinateur. Si Kaspersky Endpoint Security est installé sur un ordinateur fonctionnant sous Windows for Servers, Kaspersky Endpoint Security n'affiche pas la notification. Par conséquent, vous ne pouvez pas sélectionner une action pour désinfecter une menace active. Pour désinfecter une menace, vous devez appliquer la technologie de désinfection avancée dans les paramètres de l'application et activer la désinfection immédiate de l'infection active dans les paramètres de la tâche *Analyse des logiciels malveillants*. Ensuite, vous devez démarrer la tâche *Analyse des logiciels malveillants*.
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation *(disponible uniquement dans Kaspersky Security Center Console)*	Si la case est cochée, l'application utilise le Serveur d'administration de Kaspersky Security Center comme serveur proxy pour la connexion aux serveurs d'activation. Cette procédure est nécessaire si vous utilisez un code d'activation pour activer l'application dans un segment isolé du réseau sans accès à Internet. Si vous activez l'application à l'aide d'un fichier clé, vous ne devez pas disposer d'un accès à Internet.
Activer l'Autodéfense	Si cette fonctionnalité est activée, 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.

Paramètre	Description
Bloquer la gestion externe des services de l'application	Si cette fonctionnalité est activée, Kaspersky Endpoint Security n'autorise pas l'administration des services de l'application à l'aide d'applications tierces (comme CMD). Lorsqu'une tentative est faite pour gérer les services d'application à l'aide des applications tierces, 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). Vous pouvez autoriser l'administration externe des services de l'application sur les ordinateurs qui ne prennent pas en charge la technologie AM-PPL ou sur les ordinateurs sur lesquels la technologie désactivée.
Reporter les tâches planifiées lors de l'exécution sur batterie	Si la case est cochée, le mode d'économie d'énergie est activé lorsque l'ordinateur fonctionne sur batterie. Kaspersky Endpoint Security reporte les tâches planifiées. Vous pouvez démarrer manuellement une analyse ou les tâches de mise à jour, si nécessaire. Quand le mode d'économie d'énergie est activé, les tâches suivantes ne sont pas exécutées quand un ordinateur est alimenté par la batterie, mais si elles sont programmées : • *Analyse complète*. • *Analyse des zones critiques*. • *Analyse personnalisée*. • *Vérification de l'intégrité de l'application*. • *Analyse IOC*. • *Mise à jour des bases et des modules d'application* (correctifs uniquement) L'application ne suspend les mises à jour programmées de la base de données que lorsque l'ordinateur portable fonctionne sur batterie et que le niveau de charge de celle-ci est inférieur à 30 % (valeur par défaut). Vous pouvez modifier le niveau de charge minimal de la batterie à partir duquel l'application commence à suspendre les mises à jour programmées des bases antivirus en modifiant le Registre. Dans tous les autres cas, Kaspersky Endpoint Security met à jour ses bases de données selon la planification, que l'ordinateur portable soit branché sur secteur ou fonctionne sur batterie, ou que l'application soit en mode économie d'énergie.
Céder les ressources aux autres applications	La consommation des ressources de l'ordinateur par Kaspersky Endpoint Security lors de l'analyse d'un ordinateur peut augmenter la charge des sous-systèmes du processeur et du disque dur. Ce processus peut ralentir d'autres applications. Pour optimiser les performances, Kaspersky Endpoint Security propose un *mode de transfert des ressources vers d'autres applications*. Dans ce mode, le système d'exploitation peut réduire la priorité des tâches d'analyse de Kaspersky Endpoint Security lorsque la charge du processeur est élevée. Cette fonction permet de redistribuer les ressources du système d'exploitation à d'autres applications. Le processeur consacrera donc moins de ressources aux tâches d'analyse. Par conséquent, Kaspersky Endpoint Security mettra plus de temps à analyser l'ordinateur. Par défaut, l'application est configurée pour céder des ressources aux autres applications.
Limiter l'utilisation du processeur pour les tâches d'analyse	Pour optimiser les performances de Kaspersky Endpoint Security, vous pouvez limiter l'utilisation du processeur par la tâche *Analyse des logiciels malveillants*. Si la case est cochée, la charge moyenne de tous les cœurs du processeur de la tâche *Analyse des logiciels malveillants* se rapproche de la valeur indiquée. Par défaut, la case est décochée.
Activer l'enregistrement des fichiers de vidage	Si la case est cochée, Kaspersky Endpoint Security écrit des vidages en cas de panne. 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.
Activer la protection des fichiers de vidage et des fichiers de traçage	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. Si la case est décochée, tout utilisateur peut accéder aux fichiers de vidage et aux fichiers de traçage.
État de l'ordinateur à l'application des paramètres *(disponible uniquement dans Kaspersky Security Center Console)*	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 suivants sont disponibles : *OK*, *Avertissement* et *Critique*.

Paramètre	Description
Installer les mises à jour sans redémarrer l'ordinateur	Le fait de mettre à jour l'application sans redémarrer l'ordinateur permet d'assurer un fonctionnement ininterrompu des serveurs. Vous pouvez mettre à jour l'application sans redémarrage à partir de la version 11.10.0. Pour mettre à jour une version antérieure de l'application, vous devez redémarrer l'ordinateur. À partir de la version 11.11.0, vous pouvez effectuer les actions suivantes sans redémarrer l'ordinateur : • installer des correctifs • changer l'ensemble des modules d'application • installer Kaspersky Endpoint Security sur Kaspersky Security for Windows Server La valeur par défaut du paramètre varie en fonction du type de système d'exploitation. Si l'application est installée sur un poste de travail, l'option de mise à jour de l'application sans redémarrage est désactivée. Si l'application est installée sur un serveur, l'option de mise à jour de l'application sans redémarrage est activée.
Compatibilité avec les logiciels d'administration à distance *(disponible uniquement dans Kaspersky Security Center Console)*	Si l'utilisation de Kaspersky Endpoint Security avec les outils d'administration à distance (RAT) pose des problèmes, vous pouvez activer le mode de compatibilité. Les problèmes peuvent être liés à l'incompatibilité des RAT avec la fonctionnalité Secure Desktop de l'application. Le but de cette fonctionnalité est de confirmer les actions susceptibles de réduire le niveau de sécurité de l'ordinateur. Cette fonctionnalité permet à une application d'afficher une boîte de dialogue de confirmation isolée des autres processus. Cette fonctionnalité utilise des droits élevés pour sécuriser la demande. De cette façon, seul l'utilisateur peut confirmer l'action et non le programme malveillant. Si cette option est sélectionnée, le mode de compatibilité RAT est activé. L'application affiche une boîte de dialogue de confirmation sans cette fonctionnalité. Le niveau de sécurité de l'ordinateur peut s'en trouver réduit. Nous vous déconseillons d'activer le mode de compatibilité si Kaspersky Endpoint Security ne pose pas de problèmes avec votre RAT. Si cette option est désélectionnée, le mode de compatibilité RAT est désactivé. Par défaut, la case est décochée. Exemple : lors de l'utilisation du navigateur en mode RemoteApp, Kaspersky Endpoint Security peut ne pas afficher de fenêtre de confirmation lors de la visite d'un site Web avec un certificat non fiable, car RemoteApp ne prend pas en charge la fonctionnalité Bureau sécurisé de l'application. Le navigateur peut alors ne plus répondre. Pour que le navigateur fonctionne correctement en mode RemoteApp, vous devez activer le mode de compatibilité. Vous pouvez également essayer d'activer le mode de compatibilité si vous rencontrez des problèmes avec la fonctionnalité Bureau sécurisé lors de l'utilisation d'un autre logiciel tiers.

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.14.2\Report`.

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.14.2\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.

Quarantaine

La *Quarantaine* est un stockage local spécial sur l'ordinateur. L'utilisateur peut mettre en quarantaine les fichiers qu'il considère comme dangereux pour l'ordinateur. Les fichiers mis en quarantaine sont stockés dans un état chiffré et ne menacent pas la sécurité de l'appareil. Kaspersky Endpoint Security utilise la Quarantaine uniquement lorsqu'elle est intégrée aux solutions de détection et de réponse de Kaspersky. Dans d'autres cas, Kaspersky Endpoint Security place le fichier correspondant dans la Sauvegarde. Pour en savoir plus sur la gestion de la Quarantaine dans le cadre des solutions, veuillez consulter l'aide de Kaspersky Sandbox, l'aide de Kaspersky Endpoint Detection and Response Optimum, l'aide de Kaspersky Endpoint Detection and Response Expert, l'aide de Kaspersky Anti Targeted Attack Platform et l'aide de Kaspersky Endpoint Detection and Response Expert (on-premises).

La quarantaine peut être configurée uniquement à l'aide de Web Console. Vous pouvez également utiliser Web Console pour gérer les objets mis en quarantaine (restauration, suppression, ajout, etc.). Vous pouvez restaurer les objets localement sur l'ordinateur en utilisant la ligne de commande.

Kaspersky Endpoint Security utilise le compte système (SYSTEM) pour mettre les fichiers en quarantaine.

Paramètres des rapports et du stockage

Paramètre	Description
Supprimer les rapports après (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 des rapports à (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 (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 (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 1 024 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.
Limiter la taille de la Quarantaine	Si la case est cochée, la taille maximale de la Quarantaine est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 1 024 Mo. Lorsque la Quarantaine atteint sa taille maximale, Kaspersky Endpoint Security envoie l'événement *Espace insuffisant dans le Stockage en ligne* à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application arrête de mettre en quarantaine les nouveaux objets. Vous devez vider la Quarantaine manuellement.
Avertir lorsque le stockage de la Quarantaine atteint (%)	Valeur seuil de la Quarantaine. Par exemple, vous pouvez fixer le seuil de la Quarantaine à 50 %. Lorsque la Quarantaine atteint le seuil, Kaspersky Endpoint Security envoie l'événement correspondant à Kaspersky Security Center et publie l'événement dans le journal d'événements Windows. Pendant ce temps, l'application continue de mettre en quarantaine les nouveaux objets.

Paramètre	Description
Transfert des données au Serveur d'administration *(disponible uniquement dans Kaspersky Security Center)*	Les catégories des événements survenus sur les ordinateurs client dont les données doivent être transmises au Serveur d'administration. Vous pouvez désactiver le transfert de certaines données pour optimiser l'espace sur le disque du Serveur d'administration. L'application envoie les événements des catégories suivantes : • **À propos des fichiers de la Quarantaine**. Vous pouvez consulter la liste des fichiers mis en quarantaine dans la console de Kaspersky Security Center, dans le dossier **Avancé** → **Stockages** → **Quarantaine**. Kaspersky Endpoint Security utilise la Quarantaine uniquement lorsqu'elle est intégrée aux solutions de détection et de réponse de Kaspersky. • **À propos des fichiers de la Sauvegarde**. Vous pouvez consulter la liste des fichiers de la Sauvegarde dans la console de Kaspersky Security Center, dans le dossier **Avancé** → **Stockages** → **Sauvegarde**. • **À propos des fichiers non traités**. Vous pouvez consulter la liste des fichiers non traités dans la console de Kaspersky Security Center, dans le dossier **Avancé** → **Stockages** → **Menaces actives**. • **À propos des appareils installés**. Vous pouvez consulter la liste des appareils connectés dans la console de Kaspersky Security Center dans le dossier **Avancé** → **Stockages** → **Matériel**. La liste des appareils est également disponible dans les propriétés de l'ordinateur et dans la stratégie Kaspersky Endpoint Security for Windows (section **Contrôle des appareils**). • **À propos des applications exécutables**. Vous pouvez consulter la liste des fichiers exécutables dans la console de Kaspersky Security Center, dans le dossier **Avancé** → **Gestion des applications** → **Fichiers exécutables**. La liste des fichiers exécutables est également disponible dans les propriétés de l'ordinateur. • **À propos des erreurs de chiffrement des fichiers**. Vous pouvez consulter la liste des erreurs de chiffrement des fichiers dans la console de Kaspersky Security Center, dans le dossier **Avancé** → **Chiffrement et protection des données** → **Événements du chiffrement**. La liste des erreurs est également disponible dans les propriétés de l'ordinateur. • **Rapport sur l'état des règles du Contrôle évolutif des anomalies**. Vous pouvez consulter le rapport dans la console de Kaspersky Security Center dans le nœud **Serveur d'administration** sous l'onglet **Rapports**. Ce rapport est également disponible dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows (section **Contrôle évolutif des anomalies**). • **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**. Vous pouvez consulter le rapport dans la console de Kaspersky Security Center dans le nœud **Serveur d'administration** sous l'onglet **Rapports**. Ce rapport est également disponible dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows (section **Contrôle évolutif des anomalies**). • **À propos d'une chaîne de développement de menaces**. Vous pouvez consulter les détails de la détection dans Kaspersky Security Center Web Console dans la section **Surveillance** → **Alerte**. Les informations relatives à la chaîne de développement de la menace sont utilisées par les solutions Kaspersky Endpoint Detection and Response.

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
Restreindre le trafic sur les connexions limitées	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. Le Contrôle du trafic Internet fonctionne sur les ordinateurs exécutant Windows 8 ou une version ultérieure.
Implanter un script dans le trafic Internet pour interagir avec les pages Internet	Si la case est cochée, Kaspersky Endpoint Security implante 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. 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.
Paramètres du serveur proxy	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. 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, l'application utilise l'adresse du serveur proxy spécifiée dans les paramètres du navigateur Microsoft Internet Explorer.

Paramètre	Description
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.
Paramètres d'authentification du serveur proxy	Pour authentifier l'application sur le serveur proxy d'accès à Internet, vous devez saisir les identifiants de l'utilisateur. Kaspersky Endpoint Security prend en charge l'authentification automatique sur le serveur proxy. Si l'authentification automatique échoue, l'application vous invite à saisir les identifiants. **Ne pas utiliser l'authentification**. **Authentification NTLM**. Authentification NTLM avec le compte utilisateur actuel (par défaut). **Authentification NTLM avec nom d'utilisateur et mot de passe**. Authentification NTLM avec des identifiants spécifiés manuellement. **Nom d'utilisateur et mot de passe**. Authentification avec des identifiants spécifiés manuellement. **Authentification automatique**. **Authentification Kerberos**. Authentification Kerberos avec le compte utilisateur actuel. Pour garantir le bon fonctionnement de l'authentification Kerberos lorsque vous utilisez des enregistrements CNAME pour l'adresse du serveur proxy, vous devez enregistrer un Service Principal Name (SPN) pour chaque enregistrement CNAME. **Authentification Kerberos avec nom d'utilisateur et mot de passe**. Authentification Kerberos avec des identifiants spécifiés manuellement. Si l'authentification Kerberos est sélectionnée, Kaspersky Endpoint Security peut, en fonction de la configuration du serveur proxy, procéder à l'authentification selon le protocole Kerberos ou NTLM.
Ports contrôlés	**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 et Protection contre les menaces par emails) contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur. **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. **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. **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.
Analyse des connexions chiffrées	Kaspersky Endpoint Security analyse le trafic réseau chiffré transmis via les protocoles suivants : • SSL 3.0 ; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security prend en charge les modes d'analyse des connexions chiffrées suivants : • **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 menaces Internet, 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.

Paramètre	Description
Certificats racine de confiance	Liste des certificats racine de confiance. Kaspersky Endpoint Security vous permet d'installer des certificats racine de confiance sur les ordinateurs des utilisateurs si, par exemple, vous devez déployer un nouveau centre de certification. L'application vous permet d'ajouter un certificat à une liste de certificats spéciale de Kaspersky Endpoint Security. Dans ce cas, le certificat est considéré comme étant fiable uniquement pour l'application Kaspersky Endpoint Security. Autrement dit, l'utilisateur peut accéder à un site Internet avec le nouveau certificat dans le navigateur. Si une autre application tente d'accéder au site Internet, vous pouvez obtenir une erreur de connexion en raison d'un problème de certificat. Pour ajouter des éléments à la liste de certificats du système, vous pouvez utiliser les stratégies de groupe Active Directory.
Accès à un domaine doté d'un certificat douteux	• **Autoriser**. Kaspersky Endpoint Security autorise l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. 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. Si une application ou un service tiers établit une connexion avec un domaine présentant un certificat douteux, Kaspersky Endpoint Security crée son propre certificat pour analyser le trafic. Le nouveau certificat porte l'état *Douteuse*. Cette mesure est nécessaire pour avertir l'application tierce de la connexion douteuse, car la page HTML ne peut pas être affichée dans ce cas, et la connexion peut être établie en arrière-plan. • **Bloquer**. Kaspersky Endpoint Security bloque l'établissement d'une connexion réseau lors de l'accès à un domaine avec un certificat douteux. 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.
Accès à un domaine présentant une erreur d'analyse des connexions chiffrées	• **Bloquer**. Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée. • **Autoriser et ajouter le domaine aux exclusions**. 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**. Kaspersky Endpoint Security génère également un événement pour signaler l'erreur d'analyse de la connexion chiffrée.
Bloquer les connexions SSL 2.0	Si cette case est cochée, l'application surveille et bloque les connexions réseau établies via le protocole SSL 2.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole SSL 2.0. Cependant, l'application ne contrôle pas le trafic réseau via ce protocole.
Bloquer les connexions SSL 3.0	Si cette case est cochée, l'application bloque les connexions réseau établies via le protocole SSL 3.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole SSL 3.0. L'application surveille le trafic réseau via ce protocole. Tous les modules de l'application fonctionnent sans restrictions.
Bloquer les connexions TLS 1.0	Si cette case est cochée, l'application bloque les connexions réseau établies via le protocole TLS 1.0. Si cette case est décochée, l'application ne bloque pas les connexions réseau établies via le protocole TLS 1.0. L'application surveille le trafic réseau via ce protocole. Tous les modules de l'application fonctionnent sans restrictions.
Déchiffrer les connexions chiffrées avec un site qui utilise le certificat EV	Les certificats EV (Extended Validation Certificate) 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. Si cette case est cochée, l'application déchiffre et surveille les connexions chiffrées avec les sites qui utilisent un certificat EV. Si la case est décochée, l'application 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, `https://bing.com`. 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.

Paramètre	Description
Configurer les adresses de confiance	Ce mode utilise une liste d'adresses Internet pour lesquels Kaspersky Endpoint Security n'analyse pas les connexions réseau. Dans ce cas, Kaspersky Endpoint Security n'analyse pas le trafic HTTPS des URL de confiance lorsque les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet fonctionnent. Vous pouvez saisir un nom de domaine ou une adresse IP. Kaspersky Endpoint Security prend en charge le caractère `*` pour saisir un masque dans le nom de domaine. Kaspersky Endpoint Security ne prend pas en charge le symbole `*` pour les adresses IP. Vous pouvez sélectionner une plage d'adresses IP à l'aide d'un masque de sous-réseau (par exemple, 198.51.100.0/24). Exemples : • `domain.com` : l'enregistrement comprend les adresses suivantes : `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. L'enregistrement ne comprend pas les sous-domaines (par exemple, `subdomain.domain.com`). • `subdomain.domain.com` : l'enregistrement comprend les adresses suivantes : `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`. • `*.domain.com` : l'enregistrement comprend les adresses suivantes : `https://movies.domain.com`, `https://images.domain.com/page123`. L'enregistrement ne comprend pas le domaine `domain.com`.
Configurer les applications de confiance	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 `*` et `?` lors de la saisie d'un masque.
Pour analyser les connexions chiffrées dans les applications disposant de leur propre liste de certificats, utilisez *(disponible uniquement dans l'interface de Kaspersky Endpoint Security)*	Si cette case est cochée, l'application 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. 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, l'application n'analyse pas le trafic dans le navigateur Mozilla Firefox et le client de messagerie Thunderbird. L'application 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. • **Liste de certificats Windows (recommandé)**. Le certificat racine de Kaspersky est ajouté à cette boutique lors de l'installation de Kaspersky Endpoint Security. • **Propre liste de certificats**. 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.

Paramètre	Description
Interaction avec l'utilisateur *(disponible uniquement dans Kaspersky Security Center Console)*	**Afficher l'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 uniquement les notifications nécessitant une action de l'utilisateur au-dessus de l'icône de l'application. **Afficher l'interface utilisateur**. 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. **Masquer la section Surveillance des applications**. Sur l'ordinateur client, dans la fenêtre principale de Kaspersky Endpoint Security, le bouton **Surveillance des applications** n'est pas disponible. 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. **Ne pas afficher l'interface utilisateur**. 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.
Accéder aux tâches locales	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, 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. Si cette case est décochée, les tâches locales sont masquées dans l'interface de l'application. 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. L'utilisateur peut toujours lancer la recherche 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.
Afficher les tâches de groupe	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. Si cette case n'est pas cochée, Kaspersky Endpoint Security affiche une liste de tâches vide.
Gérer les tâches de groupe	Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans la console de 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. Si cette case n'est pas cochée, Kaspersky Endpoint Security lance automatiquement les tâches selon la planification ou l'administrateur les lance manuellement dans la console de Kaspersky Security Center.
Configurer les notifications	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.
Configurer les notifications par email	Paramètres du serveur SMTP pour l'envoi de notifications relatives aux événements enregistrés pendant le fonctionnement de l'application. Par défaut, Kaspersky Endpoint Security utilise les paramètres de notification par email de Kaspersky Security Center. Pour en savoir plus sur les paramètres de notification par email, consultez l'aide de Kaspersky Security Center. Si vous devez configurer une notification par email individuelle, vous pouvez modifier les paramètres suivants : • **Adresse de l'expéditeur**. Adresse email de l'expéditeur. Il n'est pas recommandé d'utiliser une adresse non existante. • **Serveur SMTP**. Au moins une adresse de serveurs de messagerie de votre organisation (par exemple, `mail.company.com`). Vous pouvez saisir une adresse IP (IPv4 ou IPv6). Pour authentifier l'utilisateur sur le serveur SMTP, saisissez les identifiants de l'expéditeur dans les champs correspondants. Pour tester les notifications par email, vous pouvez envoyer un message de test. • **Adresse du destinataire**. Adresses email des destinataires auxquels l'application enverra les notifications. • **Mode de diffusion**. Mode d'envoi des notifications par email. Kaspersky Endpoint Security peut envoyer des messages immédiatement lorsqu'un événement se produit. Alternativement, il peut suivre un calendrier préconfiguré.
Afficher l'état de l'application dans la zone de notifications	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).
Notifications sur l'état des bases anti-malware locales	Paramètres de notification sur le caractère dépassé des bases antivirus que l'application utilise.

Paramètre	Description
Protection par mot de passe	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. Une fois la Protection par mot de passe activée, Kaspersky Endpoint Security propose de définir un mot de passe pour le compte KLAdmin.
Assistance aux utilisateurs/Liens vers des ressources Internet *(disponible uniquement dans Kaspersky Security Center Console)*	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 **Support technique** de l'interface locale de Kaspersky Endpoint Security aux côtés des liens standard.
Assistance aux utilisateurs/Description *(disponible uniquement dans Kaspersky Security Center Console)*	Message qui apparaît dans la fenêtre **Support technique** de l'interface locale de Kaspersky Endpoint Security.

Administration 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 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 de fonctionnement de l'application recommandés par Kaspersky. Lorsque les paramètres sont restaurés, le niveau de protection **Recommandé** sera sélectionné pour tous les modules de la protection.

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 fonctionnalités des mise à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) peuvent ne pas être disponibles dans le logiciel aux États-Unis.

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.

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.

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 concernant l'état actuel des bases de données de Kaspersky Endpoint Security sont affichées dans la fenêtre principale de l'application ou dans l'infobulle que vous voyez lorsque vous passez le curseur sur l'icône de l'application dans la zone de notification.

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.

Si l'application fonctionne en mode Light Agent, la mise à jour des bases et des modules de l'application doit faire l'objet de considérations particulières.

Paramètres de mise à jour des modules d'application et des bases de données

Paramètre	Description
Calendrier de mise à jour des bases de données	**Automatiquement**. Le mode d'exécution de la tâche de mise à jour où l'application 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. **Manuellement**. Ce mode d'exécution de la tâche de mise à jour permet de lancer la tâche de mise à jour manuellement. **Selon la planification**. 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.
Lancer les tâches non exécutées	Si la case est cochée, Kaspersky Endpoint Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Endpoint Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Sources 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. En cas d'indisponibilité des serveurs de mise à jour de Kaspersky, Kaspersky Endpoint Security peut utiliser d'autres domaines pour mettre à jour ses bases de données et ses modules logiciels. Pour en savoir plus, consultez la Base des connaissances du Support Technique. 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. Par défaut, Kaspersky Endpoint Security utilise le serveur Kaspersky Security Center comme première source de mise à jour. Il est ainsi possible de réduire le trafic lors des mises à jour. Si une stratégie n'est pas appliquée à l'ordinateur, les serveurs Kaspersky sont sélectionnés comme première source de mise à jour dans les paramètres de la tâche locale *Mise à jour des bases et des modules d'application* parce que l'application n'a peut-être pas accès au serveur de Kaspersky Security Center. Si l'application s'exécute en mode Light Agent, un dossier sur la SVM est sélectionné comme source des mises à jour.
Lancer les mises à jour des bases avec les privilèges suivants	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 l'application et lancer la tâche de mise à jour de Kaspersky Endpoint Security au nom de cet utilisateur.

Paramètre	Description
Télécharger les mises à jour des modules de l'application	Téléchargement des mises à jour des modules d'application avec les mises à jour de la base de données des applications. 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 : • **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. 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. 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. Cette case est cochée par défaut.
Copier les mises à jour dans le dossier	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.14.2\Update distribution\`.
Serveur proxy pour les mises à jour *(disponible uniquement dans l'interface de Kaspersky Endpoint Security)*	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. 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.
Ne pas utiliser de serveur proxy pour les adresses locales *(disponible uniquement dans l'interface de Kaspersky Endpoint Security)*	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.

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 l'application 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 l'application dans le groupe *Restrictions faibles*.

  Il existe des restrictions minimes 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 l'application 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 l'application dans le groupe *Douteuses*.

  Pour de telles 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 ;

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, xltm : 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, xlsm : 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 ;

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, xltm : 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, xlsm : 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 du réseau pour l'interaction avec les 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 les paramètres réseau suivants pour interagir avec les services externes.

Paramètres du réseau

Adresse	Description
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocole : `HTTPS` Port : `443`	Activation de l'application.

Adresse	Description

`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`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocole : `HTTPS`
Port : `443`
	Mise à jour des bases de données et des modules de l'application.

`downloads.upd.kaspersky.com` Protocole : `HTTPS` Port : `443`	• Mise à jour des bases de données et des modules de l'application. • Vérification de l'accès aux serveurs de Kaspersky. Si l'accès aux serveurs à l'aide du DNS 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). 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.
`touch.kaspersky.com` Protocole : `HTTP`	• Réception du temps de confiance pour vérifier la période de validité du certificat (connexion TLS). • Avertissement concernant l'accès refusé à une ressource Internet dans le navigateur lorsque la Protection contre les menaces Internet est en cours d'exécution.

Adresse	Description

`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`
`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`
Protocole : `HTTP`
Port : `80`
	Mise à jour des bases de données et des modules de l'application.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocole : `HTTPS`
Port : `443`
	Utilisation de Kaspersky Security Network.

`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`
Protocole : `KSN`
Port : `443`, `1443`
	Utilisation de Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protocole : `HTTPS`
Port : `443`
	Suivez les liens de l'interface.

Paramètres utilisés pour le chiffrement

Adresse	Description

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocole : `HTTP`
Port : `80`
	Infrastructure à clés publiques (ICP).

Annexe 6. Événements relatifs aux applications

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'achèvement de chaque tâche de recherche de logiciels malveillants, 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 de Kaspersky Security Center et dans le journal des événements Windows.

Kaspersky Endpoint Security génère des événements des types suivants : événements généraux et événements particuliers. Les événements particuliers sont créés uniquement par Kaspersky Endpoint Security for Windows. Les événements particuliers ont un identifiant simple, tel que `000000cb`. Les événements particuliers contiennent les paramètres requis suivants :

- `GNRL_EA_DESCRIPTION` est le contenu de l'événement.
- `GNRL_EA_ID` est l'identifiant de service de l'événement.
- `GNRL_EA_SEVERITY` est l'état de l'événement. `1` – *Information*, `2` – *Avertissement*, `3` – *Erreur de fonctionnement*, `4` – *Critique*.
- `EVENT_TYPE_DISPLAY_NAME` est le titre de l'événement.
- `TASK_DISPLAY_NAME` est le nom du module de l'application qui a déclenché l'événement.

Les événements généraux peuvent être créés par Kaspersky Endpoint Security for Windows ainsi que par d'autres applications Kaspersky (par exemple, Kaspersky Security for Windows Server). Les événements généraux ont un identifiant plus complexe, tel que `GNRL_EV_VIRUS_FOUND`. En plus des paramètres obligatoires, les événements généraux contiennent des paramètres avancés.

Durée de conservation des événements sur le serveur

Critique

La licence a expiré

État	!
Module	Audit système
Identifiant de l'événement Windows	`201`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La durée de validité de la licence expire bientôt

État	!
Module	Audit système
Identifiant de l'événement Windows	`203`

Identifiant de l'événement de Kaspersky Security Center	`000000cb`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les bases sont endommagées ou manquantes

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`206`
Identifiant de l'événement de Kaspersky Security Center	`000000ce`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Les bases sont fortement dépassées

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`207`
Identifiant de l'événement de Kaspersky Security Center	`000000cf`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le lancement automatique de l'application est désactivé

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`209`
Identifiant de l'événement de Kaspersky Security Center	`000000d1`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'activation

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`229`
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une menace active a été détectée. Il faut lancer la procédure de désinfection avancée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`231`
Identifiant de l'événement de Kaspersky Security Center	`000000e7`

Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Serveurs de KSN indisponibles

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2023
Identifiant de l'événement de Kaspersky Security Center	000007e7
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Espace insuffisant dans le Stockage en ligne

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	343
Identifiant de l'événement de Kaspersky Security Center	00000157
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet non restauré de la Quarantaine

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	346
Identifiant de l'événement de Kaspersky Security Center	0000015a
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet non supprimé de la Quarantaine

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	348
Identifiant de l'événement de Kaspersky Security Center	0000015c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application a établi une connexion à un site avec un certificat non approuvé

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	57
Identifiant de l'événement de Kaspersky Security Center	00000039

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Échec de la vérification d'une connexion chiffrée. Le domaine est ajouté à la liste d'exclusions

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	`60`
Identifiant de l'événement de Kaspersky Security Center	`0000003c`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet malveillant a été détecté (bases locales)

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Détection comportementale Protection contre le chiffrement Protection contre les Exploits Analyse des logiciels malveillants
Identifiant de l'événement Windows	`302`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. Lorsque le chiffrement externe de dossiers partagés est détecté, l'application indique le chemin d'accès au fichier cible. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet malveillant a été détecté (KSN)

État	!
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Détection comportementale Protection contre le chiffrement Protection contre les Exploits Analyse des logiciels malveillants
Identifiant de l'événement Windows	`302`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Désinfection impossible

État	!
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Prévention des intrusions Détection comportementale Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	`312`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Suppression impossible

État	!
Module	Protection contre les fichiers malicieux Prévention des intrusions Détection comportementale Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	313
Identifiant de l'événement de Kaspersky Security Center	00000139
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de traitement

État	!
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Prévention des intrusions Protection AMSI Analyse des logiciels malveillants
Identifiant de l'événement Windows	317
Identifiant de l'événement de Kaspersky Security Center	0000013d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le processus est terminé

État	!
Module	Protection contre les fichiers malicieux Prévention des intrusions Détection comportementale Analyse des logiciels malveillants
Identifiant de l'événement Windows	452
Identifiant de l'événement de Kaspersky Security Center	000001c4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible d'arrêter le processus

État	!
Module	Protection contre les fichiers malicieux Prévention des intrusions Détection comportementale Analyse des logiciels malveillants
Identifiant de l'événement Windows	453
Identifiant de l'événement de Kaspersky Security Center	000001c5
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Un lien dangereux a été bloqué

État	!
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	362
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Paramètres de l'événement	• GNRL_EA_PARAM_2 est le chemin d'accès à l'objet. • GNRL_EA_PARAM_5 est le nom de l'objet selon la classification Kaspersky. • GNRL_EA_PARAM_7 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_8 est le type de menace (type). • GNRL_EA_PARAM_9 est une information supplémentaire à propos de l'objet détecté : Module d'application (engine). Technologie de détection des menaces (method). Menace détectée par le KSN privé (blacklist) : true ou false.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un lien dangereux a été ouvert

État	!
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	363
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Paramètres de l'événement	• GNRL_EA_PARAM_2 est le chemin d'accès à l'objet. • GNRL_EA_PARAM_5 est le nom de l'objet selon la classification Kaspersky. • GNRL_EA_PARAM_7 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_8 est le type de menace (type). • GNRL_EA_PARAM_9 est une information supplémentaire à propos de l'objet détecté : Module d'application (engine). Technologie de détection des menaces (method). Menace détectée par le KSN privé (blacklist) : true ou false.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un lien dangereux ouvert précédemment a été détecté

État	!
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	1201
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Paramètres de l'événement	• GNRL_EA_PARAM_2 est le chemin d'accès à l'objet. • GNRL_EA_PARAM_5 est le nom de l'objet selon la classification Kaspersky. • GNRL_EA_PARAM_7 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_8 est le type de menace (type). • GNRL_EA_PARAM_9 est une information supplémentaire à propos de l'objet détecté : Module d'application (engine). Technologie de détection des menaces (method). Menace détectée par le KSN privé (blacklist) : true ou false.

Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Action du processus bloquée

État	!
Module	Contrôle évolutif des anomalies
Identifiant de l'événement Windows	`2200`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le nom de la règle du Contrôle évolutif des anomalies. • `GNRL_EA_PARAM_2` est l'identifiant de la règle heuristique. • `GNRL_EA_PARAM_3` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_4` est le processus source. • `GNRL_EA_PARAM_5` est l'objet source. • `GNRL_EA_PARAM_6` est le processus cible. • `GNRL_EA_PARAM_7` est l'objet cible. • `GNRL_EA_PARAM_8` est une information supplémentaire à propos de l'objet détecté : Sommes de contrôle du processus / objet source et du processus / objet cible. Processus bloqué (`verdict_type`) : `true` ou `false`. Identifiant de sécurité de l'utilisateur (SID).
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le clavier n'a pas été autorisé

État	!
Module	Protection BadUSB
Identifiant de l'événement Windows	`2051`
Identifiant de l'événement de Kaspersky Security Center	`00000803`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une requête AMSI a été bloquée

État	!
Module	Protection AMSI
Identifiant de l'événement Windows	`2200`
Identifiant de l'événement de Kaspersky Security Center	`00000898`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'activité réseau est interdite

État	!
Module	Pare-feu
Identifiant de l'événement Windows	`602`
Identifiant de l'événement de Kaspersky Security Center	`00000329`

Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une attaque réseau a été détectée

État	!
Module	Protection contre les menaces réseau
Identifiant de l'événement Windows	`651`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_ATTACK_DETECTED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le nom de l'attaque. • `GNRL_EA_PARAM_2` est le protocole. • `GNRL_EA_PARAM_3` est l'adresse IP de l'ordinateur agissant comme source de l'attaque réseau. L'adresse IP est indiquée dans l'ordre des octets de l'hôte. Par exemple, `2886729929` pour `172.16.0.201`. • `GNRL_EA_PARAM_4` est le numéro de port. • `GNRL_EA_PARAM_5` est une adresse IPv6, par exemple, `12B012B012B012B012B012B012B012B0`. • `GNRL_EA_PARAM_6` est l'adresse IP de l'ordinateur visé par l'attaque réseau. L'adresse IP est indiquée dans l'ordre des octets de l'hôte. Par exemple, `2886729929` pour `172.16.0.201`.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le lancement de l'application est interdit

État	!
Module	Contrôle des applications
Identifiant de l'événement Windows	`702`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Paramètres de l'événement	• `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_3` est l'identifiant de catégorie créé manuellement. • `GNRL_EA_PARAM_4` est l'identifiant de la catégorie d'application. • `GNRL_EA_PARAM_5` est une information sur la signature numérique de l'application. • `GNRL_EA_PARAM_6` est le nom du fichier exécutable de l'application (par exemple, chrome.exe). • `GNRL_EA_PARAM_7` est le chemin d'accès au fichier exécutable. • `GNRL_EA_PARAM_8` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_9` est la version de l'application que l'utilisateur essaie d'exécuter.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le processus interdit a été lancé avant le démarrage de Kaspersky Endpoint Security

État	!
Module	Contrôle des applications
Identifiant de l'événement Windows	`710`
Identifiant de l'événement de Kaspersky Security Center	`000002c6`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès interdit (bases locales)

État	!
Module	Contrôle Internet
Identifiant de l'événement Windows	752
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Paramètres de l'événement	• GNRL_EA_PARAM_1 est l'URL. • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_3 est le nom de la règle du Contrôle Internet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès interdit (KSN)

État	!
Module	Contrôle Internet
Identifiant de l'événement Windows	752
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Paramètres de l'événement	• GNRL_EA_PARAM_1 est l'URL. • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_3 est le nom de la règle du Contrôle Internet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'opération avec l'appareil est interdite

État	!
Module	Contrôle des appareils
Identifiant de l'événement Windows	802
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Paramètres de l'événement	• GNRL_EA_PARAM_1 est l'identifiant du matériel (HWID). • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réseau bloquée

État	!
Module	Contrôle des appareils
Identifiant de l'événement Windows	809
Identifiant de l'événement de Kaspersky Security Center	00000329
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'utilisation de l'appareil est interdite tant que Kaspersky Endpoint Security n'a pas été lancé

État	!
Module	Contrôle des appareils
Identifiant de l'événement Windows	816
Identifiant de l'événement de Kaspersky Security Center	00000330
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La connexion de l'appareil est interdite tant que Kaspersky Endpoint Security n'a pas été lancé

État	!
Module	Contrôle des appareils
Identifiant de l'événement Windows	817
Identifiant de l'événement de Kaspersky Security Center	00000331
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de mise à jour du module

État	!
Module	Mise à jour
Identifiant de l'événement Windows	1011
Identifiant de l'événement de Kaspersky Security Center	000003f3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de copie des mises à jour du module

État	!
Module	Mise à jour
Identifiant de l'événement Windows	1012
Identifiant de l'événement de Kaspersky Security Center	000003f4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Erreur locale de mise à jour

État	!
Module	Mise à jour
Identifiant de l'événement Windows	1014
Identifiant de l'événement de Kaspersky Security Center	000003f6
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Erreur réseau de mise à jour

État	⊙
Module	Mise à jour
Identifiant de l'événement Windows	1015
Identifiant de l'événement de Kaspersky Security Center	000003f7
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Impossible de lancer deux tâches simultanément

État	⊙
Module	Mise à jour
Identifiant de l'événement Windows	1017
Identifiant de l'événement de Kaspersky Security Center	000003f9
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'analyse des bases et des modules de l'application

État	⊙
Module	Mise à jour
Identifiant de l'événement Windows	1018
Identifiant de l'événement de Kaspersky Security Center	000003fa
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'interaction avec Kaspersky Security Center

État	⊙
Module	Mise à jour
Identifiant de l'événement Windows	1019
Identifiant de l'événement de Kaspersky Security Center	000003fb
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certains modules n'ont pas été mis à jour

État	⊙
Module	Mise à jour
Identifiant de l'événement Windows	1021
Identifiant de l'événement de Kaspersky Security Center	000003fd
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La mise à jour a réussi tandis que la copie des mises à jour s'est soldée par un échec

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1023
Identifiant de l'événement de Kaspersky Security Center	000003ff
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Erreur interne de la tâche

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	101
Identifiant de l'événement de Kaspersky Security Center	00000065
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Erreur d'installation du correctif

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2153
Identifiant de l'événement de Kaspersky Security Center	00000869
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'annulation du correctif

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2156
Identifiant de l'événement de Kaspersky Security Center	0000086c
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'application des règles de chiffrement/déchiffrement des fichiers

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	904
Identifiant de l'événement de Kaspersky Security Center	00000388
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur du chiffrement/déchiffrement du fichier

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	912
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Paramètres de l'événement	• GNRL_EA_PARAM_1 est le chemin d'accès au fichier. • GNRL_EA_PARAM_2 est la cause de l'erreur. • GNRL_EA_PARAM_3 est le type d'appareil.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'accès au fichier est bloqué

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	940
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Paramètres de l'événement	• GNRL_EA_PARAM_1 est l'objet cible. • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_3 est le nom du fichier exécutable de l'application (par exemple, chrome.exe), qui essaie d'accéder au fichier.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Erreur d'activation du mode portable

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	951
Identifiant de l'événement de Kaspersky Security Center	000003b7
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de désactivation du mode portable

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	953
Identifiant de l'événement de Kaspersky Security Center	000003b9
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de création de l'archive chiffrée

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	931
Identifiant de l'événement de Kaspersky Security Center	000003a3
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de chiffrement/déchiffrement de l'appareil

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	1305
Identifiant de l'événement de Kaspersky Security Center	00000519
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de charger le module de chiffrement

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	1311
Identifiant de l'événement de Kaspersky Security Center	0000051f
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La tâche de gestion des comptes utilisateur de l'Agent d'authentification a échoué

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	1340
Identifiant de l'événement de Kaspersky Security Center	0000053c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La stratégie ne peut pas être appliquée

État	!
Module	Audit système
Identifiant de l'événement Windows	1312
Identifiant de l'événement de Kaspersky Security Center	00000520
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La mise à jour de la fonction de chiffrement s'est soldée par une erreur

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	1342
Identifiant de l'événement de Kaspersky Security Center	0000053e
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le retour à l'état antérieur à la mise à jour de la fonction de chiffrement s'est soldé par une erreur (pour en savoir plus, consultez l'aide en ligne de Kaspersky Endpoint Security for Windows)

État	!
Module	Chiffrement des données
Identifiant de l'événement Windows	1344
Identifiant de l'événement de Kaspersky Security Center	00000540
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Serveur Kaspersky Anti Targeted Attack Platform inaccessible

État	!
Module	Endpoint Sensor
Identifiant de l'événement Windows	2100
Identifiant de l'événement de Kaspersky Security Center	00000834
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de suppression de l'objet

État	!
Module	Sandbox
Identifiant de l'événement Windows	2252
Identifiant de l'événement de Kaspersky Security Center	000008cc
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet non mis en quarantaine (Sandbox)

État	!
Module	Sandbox
Identifiant de l'événement Windows	2603
Identifiant de l'événement de Kaspersky Security Center	00000a2b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une erreur interne s'est produite

État	!
Module	Sandbox
Identifiant de l'événement Windows	2607
Identifiant de l'événement de Kaspersky Security Center	00000a2f
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat du serveur Sandbox non valide

État	!
Module	Sandbox
Identifiant de l'événement Windows	2613
Identifiant de l'événement de Kaspersky Security Center	00000a35
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le nœud Sandbox est indisponible

État	!
Module	Sandbox
Identifiant de l'événement Windows	2614
Identifiant de l'événement de Kaspersky Security Center	00000a36
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de traiter un objet dans Sandbox

État	!
Module	Sandbox
Identifiant de l'événement Windows	2617
Identifiant de l'événement de Kaspersky Security Center	00000a39
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La charge maximale de Sandbox est dépassée

État	!
Module	Sandbox
Identifiant de l'événement Windows	2618
Identifiant de l'événement de Kaspersky Security Center	00000a3a
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

IOC trouvé

État	!
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2651
Identifiant de l'événement de Kaspersky Security Center	00000a5b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de la vérification de la licence Sandbox

État	!
Module	Sandbox
Identifiant de l'événement Windows	2620
Identifiant de l'événement de Kaspersky Security Center	00000a3c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible d'envoyer la tâche d'analyse à Sandbox par un utilisateur

État	!
Module	Sandbox
Identifiant de l'événement Windows	2623
Identifiant de l'événement de Kaspersky Security Center	00000a3e
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de création de la tâche Sandbox

État	!
Module	Sandbox
Identifiant de l'événement Windows	2621
Identifiant de l'événement de Kaspersky Security Center	00000a3d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le démarrage de l'objet est bloqué

État	!
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2553
Identifiant de l'événement de Kaspersky Security Center	000009f9
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le démarrage du processus est bloqué

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2551
Identifiant de l'événement de Kaspersky Security Center	000009f7
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Exécution du script bloquée

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2559
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet non mis en quarantaine (Endpoint Detection and Response)

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2556
Identifiant de l'événement de Kaspersky Security Center	000009fc
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le démarrage du processus n'est pas bloqué

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2561
Identifiant de l'événement de Kaspersky Security Center	00000a01
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet n'est pas bloqué

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2562
Identifiant de l'événement de Kaspersky Security Center	00000a02
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'exécution du script n'est pas bloquée

État	!
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2563
Identifiant de l'événement de Kaspersky Security Center	00000a03
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de modification de la sélection de modules de l'application

État	!
Module	Audit système
Identifiant de l'événement Windows	1401
Identifiant de l'événement de Kaspersky Security Center	00000579
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certains comportements indiquent une possible attaque par force brute dans le système

État	!
Module	Inspection des journaux
Identifiant de l'événement Windows	2800
Identifiant de l'événement de Kaspersky Security Center	00000af0
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certains comportements indiquent une possible violation du journal des événements Windows

État	!
Module	Inspection des journaux
Identifiant de l'événement Windows	2801
Identifiant de l'événement de Kaspersky Security Center	00000af1
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Des actions inhabituelles ont été détectées au nom d'un nouveau service installé

État	!
Module	Inspection des journaux
Identifiant de l'événement Windows	2802
Identifiant de l'événement de Kaspersky Security Center	00000af2
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion inhabituelle utilisant des identifiants explicites

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2803
Identifiant de l'événement de Kaspersky Security Center	00000af3
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2804
Identifiant de l'événement de Kaspersky Security Center	00000af4
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2805
Identifiant de l'événement de Kaspersky Security Center	00000af5
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une activité inhabituelle a été détectée lors d'une session de connexion au réseau

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2806
Identifiant de l'événement de Kaspersky Security Center	00000af6
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La règle d'inspection des journaux a été déclenchée

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2807
Identifiant de l'événement de Kaspersky Security Center	00000af7
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un événement inhabituel se produit trop souvent. L'agrégation des événements a commencé

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2808
Identifiant de l'événement de Kaspersky Security Center	00000af8
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Rapport sur un événement inhabituel pour la période d'agrégation

État	ⓘ
Module	Inspection des journaux
Identifiant de l'événement Windows	2809
Identifiant de l'événement de Kaspersky Security Center	00000af9
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises)
Identifiant de l'événement Windows	2850
Identifiant de l'événement de Kaspersky Security Center	00000b22
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises)
Identifiant de l'événement Windows	2851
Identifiant de l'événement de Kaspersky Security Center	00000b23
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises)
Identifiant de l'événement Windows	2852
Identifiant de l'événement de Kaspersky Security Center	00000b24
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur de réponse EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	2858
Identifiant de l'événement de Kaspersky Security Center	00000b22
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur de réponse EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	2859
Identifiant de l'événement de Kaspersky Security Center	00000b23
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur de réponse EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	2860
Identifiant de l'événement de Kaspersky Security Center	00000b24
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur de collecte de télémétrie EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	2854
Identifiant de l'événement de Kaspersky Security Center	00000b22
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur de collecte de télémétrie EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	2855
Identifiant de l'événement de Kaspersky Security Center	00000b23

Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur de collecte de télémétrie EDR Expert

État	!
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	`2856`
Identifiant de l'événement de Kaspersky Security Center	`00000b24`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur NDR

État	!
Module	Network Detection and Response (KATA)
Identifiant de l'événement Windows	`3080`
Identifiant de l'événement de Kaspersky Security Center	`00000c08`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur NDR

État	!
Module	Network Detection and Response (KATA)
Identifiant de l'événement Windows	`3081`
Identifiant de l'événement de Kaspersky Security Center	`00000c09`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur NDR

État	!
Module	Network Detection and Response (KATA)
Identifiant de l'événement Windows	`3082`
Identifiant de l'événement de Kaspersky Security Center	`00000c0a`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Votre appareil est connecté à un Serveur d'administration non fiable. Veuillez contacter l'administrateur

État	!
Module	Protection de la connexion au Serveur d'administration
Identifiant de l'événement Windows	`3301`
Identifiant de l'événement de Kaspersky Security Center	`00000ce5`

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un changement du fichier ou du dossier a été détecté

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2950`
Identifiant de l'événement de Kaspersky Security Center	`00000b86`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

L'objet est trop souvent modifié. L'agrégation des événements a commencé

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2955`
Identifiant de l'événement de Kaspersky Security Center	`00000b8b`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Rapport sur la modification d'un objet pour la période d'agrégation

État	ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2953`
Identifiant de l'événement de Kaspersky Security Center	`00000b89`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2956`
Identifiant de l'événement de Kaspersky Security Center	`00000b8c`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Un changement du registre a été détecté

État	/ /
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2951
Identifiant de l'événement de Kaspersky Security Center	00000b87
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Connexion/Déconnexion de l'appareil détectée

État	/ /
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2952
Identifiant de l'événement de Kaspersky Security Center	00000b88
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

La zone de surveillance inclut des objets incorrects

État	/ /
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2903
Identifiant de l'événement de Kaspersky Security Center	00000b89
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Les tentatives d'exécution des opérations restreintes avec l'objet sont trop nombreuses. L'agrégation d'événements a commencé

État	
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2963

Identifiant de l'événement de Kaspersky Security Center	00000b93
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une opération sur les fichiers de la zone de surveillance a été bloquée

État	!
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2959
Identifiant de l'événement de Kaspersky Security Center	00000b8f
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Modification du registre interdite

État	!
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2960
Identifiant de l'événement de Kaspersky Security Center	00000b90
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Erreur de traitement

État	!
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2954
Identifiant de l'événement de Kaspersky Security Center	00000b8a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Contrôle de l'intégrité du système : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2964

Identifiant de l'événement de Kaspersky Security Center	00000b94
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Contrôle des applications : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Contrôle des applications
Identifiant de l'événement Windows	711
Identifiant de l'événement de Kaspersky Security Center	000002c7
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Contrôle des appareils : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Contrôle des appareils
Identifiant de l'événement Windows	810
Identifiant de l'événement de Kaspersky Security Center	0000032a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Contrôle Internet : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Contrôle Internet
Identifiant de l'événement Windows	757
Identifiant de l'événement de Kaspersky Security Center	000002f5
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Contrôle évolutif des anomalies : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Contrôle évolutif des anomalies
Identifiant de l'événement Windows	504
Identifiant de l'événement de Kaspersky Security Center	000001f8
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Inspection des journaux : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant

État	!
Module	Inspection des journaux
Identifiant de l'événement Windows	2810
Identifiant de l'événement de Kaspersky Security Center	00000afa
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

SVM non disponible

État	!
Module	Light Agent
Identifiant de l'événement Windows	3151
Identifiant de l'événement de Kaspersky Security Center	00000c4f
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet malveillant détecté. La désinfection avancée doit être lancée sur un modèle de machine virtuelle

État	!
Module	Light Agent
Identifiant de l'événement Windows	3182
Identifiant de l'événement de Kaspersky Security Center	00000c6e
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La connexion réseau établie via le protocole obsolète a été bloquée

État	!
Module	Protection
Identifiant de l'événement Windows	75
Identifiant de l'événement de Kaspersky Security Center	0000004b
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur KUMA

État	!
Module	Intégration KUMA
Identifiant de l'événement Windows	2854
Identifiant de l'événement de Kaspersky Security Center	00000b26
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur KUMA

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	2855
Identifiant de l'événement de Kaspersky Security Center	00000b27
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur KUMA

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	2856
Identifiant de l'événement de Kaspersky Security Center	00000b28
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de connexion au serveur SIEM

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	3250
Identifiant de l'événement de Kaspersky Security Center	00000cb2
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide du serveur SIEM

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	3251
Identifiant de l'événement de Kaspersky Security Center	00000cb3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certificat non valide de l'agent sur le serveur SIEM

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	3252
Identifiant de l'événement de Kaspersky Security Center	00000cb4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur de fonctionnement

Impossible d'exécuter la tâche

État	⊘
Module	Audit système
Identifiant de l'événement Windows	212
Identifiant de l'événement de Kaspersky Security Center	000000d4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur dans les paramètres de la tâche. Les paramètres ne sont pas appliqués

État	⊘
Module	Audit système
Identifiant de l'événement Windows	707
Identifiant de l'événement de Kaspersky Security Center	000002c3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Avertissement

Une panne de la session antérieure de l'application a été détectée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	237
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

La licence expire bientôt

État	⚠
Module	Audit système
Identifiant de l'événement Windows	204
Identifiant de l'événement de Kaspersky Security Center	000000cc
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les bases sont dépassées

État	⚠
Module	Audit système
Identifiant de l'événement Windows	208
Identifiant de l'événement de Kaspersky Security Center	000000d0
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La mise à jour automatique est désactivée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	210
Identifiant de l'événement de Kaspersky Security Center	000000d2
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'Autodéfense de l'application est désactivée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	211
Identifiant de l'événement de Kaspersky Security Center	000000d3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les modules de la protection sont désactivés

État	⚠
Module	Audit système
Identifiant de l'événement Windows	214
Identifiant de l'événement de Kaspersky Security Center	000000d6
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'ordinateur fonctionne en mode sans échec

État	⚠
Module	Audit système
Identifiant de l'événement Windows	215
Identifiant de l'événement de Kaspersky Security Center	000000d7
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Il y a des fichiers non traités

État	⚠
Module	Audit système
Identifiant de l'événement Windows	216
Identifiant de l'événement de Kaspersky Security Center	000000d8
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une stratégie de groupe a été appliquée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	219
Identifiant de l'événement de Kaspersky Security Center	000000db
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La tâche est interrompue

État	⚠
Module	Audit système
Identifiant de l'événement Windows	222
Identifiant de l'événement de Kaspersky Security Center	000000de
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Quittez l'application et lancez-la à nouveau pour terminer la mise à jour

État	⚠
Module	Audit système
Identifiant de l'événement Windows	224
Identifiant de l'événement de Kaspersky Security Center	0000057b
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Redémarrage de l'ordinateur requis

État	⚠
Module	Audit système
Identifiant de l'événement Windows	225
Identifiant de l'événement de Kaspersky Security Center	000000e1
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Certains des modules de l'application autorisés par la licence ne sont pas installés

État	⚠
Module	Audit système
Identifiant de l'événement Windows	226
Identifiant de l'événement de Kaspersky Security Center	000000e2
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La procédure de désinfection avancée a été lancée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	232
Identifiant de l'événement de Kaspersky Security Center	000000e8
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La procédure de désinfection avancée est terminée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	233
Identifiant de l'événement de Kaspersky Security Center	000000e9
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La clé de réserve est incorrecte

État	⚠
Module	Audit système
Identifiant de l'événement Windows	230
Identifiant de l'événement de Kaspersky Security Center	000000e6
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'abonnement expire bientôt

État	⚠
Module	Audit système
Identifiant de l'événement Windows	240
Identifiant de l'événement de Kaspersky Security Center	000000f0
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Bloqué

État	⚠
Module	Détection comportementale Protection contre le chiffrement Protection contre les Exploits Protection contre les menaces Internet
Identifiant de l'événement Windows	`331`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. Lorsque le chiffrement externe de dossiers partagés est détecté, l'application indique le chemin d'accès au fichier cible. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Les paramètres du système d'exploitation ne permettent pas de contrôler l'accès aux réseaux Wi-Fi

État	⚠
Module	Contrôle des appareils
Identifiant de l'événement Windows	`249`
Identifiant de l'événement de Kaspersky Security Center	`000000f9`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Objet non restauré depuis la Sauvegarde

État	⚠
Module	Audit système
Identifiant de l'événement Windows	`336`
Identifiant de l'événement de Kaspersky Security Center	`00000150`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Une activité réseau suspecte a été détectée

État	⚠
Module	Audit système

Identifiant de l'événement Windows	2001
Identifiant de l'événement de Kaspersky Security Center	000007d1
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une connexion chiffrée a été interrompue

État	⚠
Module	Audit système
Identifiant de l'événement Windows	250
Identifiant de l'événement de Kaspersky Security Center	000007d3
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La participation à KSN est désactivée

État	⚠
Module	Audit système
Identifiant de l'événement Windows	2021
Identifiant de l'événement de Kaspersky Security Center	000007e5
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Désactivation du traitement par l'application de certaines fonctions du système d'exploitation

État	⚠
Module	Audit système
Identifiant de l'événement Windows	245
Identifiant de l'événement de Kaspersky Security Center	000000f5
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'espace de la Quarantaine est presque insuffisant

État	⚠
Module	Audit système
Identifiant de l'événement Windows	344
Identifiant de l'événement de Kaspersky Security Center	00000158
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réseau bloquée

État	⚠
Module	Audit système

Identifiant de l'événement Windows	809
Identifiant de l'événement de Kaspersky Security Center	00000abe
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de créer une copie de sauvegarde de l'objet

État	⚠
Module	Protection contre les fichiers malicieux Détection comportementale Protection contre le chiffrement Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	310
Identifiant de l'événement de Kaspersky Security Center	00000136
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet n'a pas été traité

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Prévention des intrusions Protection AMSI Analyse des logiciels malveillants
Identifiant de l'événement Windows	314
Identifiant de l'événement de Kaspersky Security Center	0000013a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet est chiffré

État	⚠
Module	Prévention des intrusions
Identifiant de l'événement Windows	320
Identifiant de l'événement de Kaspersky Security Center	00000140
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

L'objet est endommagé

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	321
Identifiant de l'événement de Kaspersky Security Center	00000141

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Un programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles a été détecté (bases locales)

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Prévention des intrusions Protection AMSI Détection comportementale Protection contre le chiffrement Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	`303`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles a été détecté (KSN)

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Prévention des intrusions Protection AMSI Détection comportementale Protection contre le chiffrement Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	`303`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été supprimé

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Prévention des intrusions Protection contre les Exploits Détection comportementale Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	`307`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_DELETED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été désinfecté

État	⚠
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	`306`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_CURED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet sera désinfecté au redémarrage

État	⚠
Module	Prévention des intrusions Protection contre les fichiers malicieux Analyse des logiciels malveillants
Identifiant de l'événement Windows	324
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'objet sera supprimé au redémarrage

État	⚠
Module	Détection comportementale Protection contre le chiffrement Protection contre les Exploits Prévention des intrusions Protection contre les fichiers malicieux Analyse des logiciels malveillants
Identifiant de l'événement Windows	323
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Objet supprimé selon les paramètres

État	⚠
Module	Protection contre les menaces par emails
Identifiant de l'événement Windows	342
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le retour à l'état antérieur a été exécuté

État	⚠
Module	Protection contre les fichiers malicieux Détection comportementale Protection contre le chiffrement Protection contre les Exploits Analyse des logiciels malveillants
Identifiant de l'événement Windows	455
Identifiant de l'événement de Kaspersky Security Center	000001c7
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur lors de la suppression de la version précédente de l'application

État	⚠
Module	Audit système
Identifiant de l'événement Windows	`246`
Identifiant de l'événement de Kaspersky Security Center	`000000f6`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le téléchargement de l'objet a été bloqué

État	⚠
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	`341`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Erreur d'autorisation de clavier

État	⚠
Module	Protection BadUSB
Identifiant de l'événement Windows	`2052`
Identifiant de l'événement de Kaspersky Security Center	`00000804`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le résultat de l'analyse de l'objet a été transmis à une application tierce

État	⚠
Module	Protection AMSI
Identifiant de l'événement Windows	`1512`

Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_OBJECT_REPORTED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_2` est le nom de l'objet. • `GNRL_EA_PARAM_5` est le nom de la menace selon la classification Kaspersky, par exemple, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_8` est le type de menace (`type`). • `GNRL_EA_PARAM_9` est une information supplémentaire à propos de l'objet détecté : Module d'application (`engine`). Technologie de détection des menaces (`method`). Menace détectée par Kaspersky Private Security Network (`blacklist`) : `true` ou `false`. Version EDR. Identifiant de la menace dans EDR. Hash MD5 de l'objet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Application réussie des paramètres de la tâche

État	⚠
Module	Contrôle des applications
Identifiant de l'événement Windows	`708`
Identifiant de l'événement de Kaspersky Security Center	`000002c4`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Avertissement de contenu indésirable (bases locales)

État	⚠
Module	Contrôle Internet
Identifiant de l'événement Windows	`708`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_WEB_URL_WARNING`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est l'URL. • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_3` est le nom de la règle du Contrôle Internet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Avertissement de contenu indésirable (KSN)

État	⚠
Module	Contrôle Internet
Identifiant de l'événement Windows	`708`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_WEB_URL_WARNING`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est l'URL. • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_3` est le nom de la règle du Contrôle Internet.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le contenu indésirable a été consulté après un avertissement

État	⚠
Module	Contrôle Internet
Identifiant de l'événement Windows	754
Identifiant de l'événement de Kaspersky Security Center	000002f2
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Accès temporaire à l'appareil activé

État	⚠
Module	Contrôle des appareils
Identifiant de l'événement Windows	803
Identifiant de l'événement de Kaspersky Security Center	000002f2
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'opération a été annulée par l'utilisateur

État	⚠
Module	Mise à jour
Identifiant de l'événement Windows	1016
Identifiant de l'événement de Kaspersky Security Center	000003f8
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'utilisateur a refusé la stratégie de chiffrement

État	⚠
Module	Chiffrement des données
Identifiant de l'événement Windows	1306
Identifiant de l'événement de Kaspersky Security Center	0000051a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application des règles de chiffrement/déchiffrement des fichiers est interrompue

État	⚠
Module	Chiffrement des données
Identifiant de l'événement Windows	903
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Interruption du chiffrement/déchiffrement du fichier

État	⚠
Module	Chiffrement des données
Identifiant de l'événement Windows	914
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Interruption du chiffrement/déchiffrement de l'appareil

État	⚠
Module	Chiffrement des données
Identifiant de l'événement Windows	1303
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Échec de l'installation ou de la mise à jour des pilotes de Kaspersky Disk Encryption dans l'image WinRE

État	⚠
Module	Chiffrement des données
Identifiant de l'événement Windows	1345
Identifiant de l'événement de Kaspersky Security Center	00000541
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Échec de la vérification de la signature du module

État	⚠
Module	Vérification de l'intégrité du système
Identifiant de l'événement Windows	2002
Identifiant de l'événement de Kaspersky Security Center	000007d2
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Lancement de l'application bloqué

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2105
Identifiant de l'événement de Kaspersky Security Center	00000839
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Ouverture du document bloquée

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2106
Identifiant de l'événement de Kaspersky Security Center	0000083a
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le processus a été interrompu par l'administrateur du serveur Kaspersky Anti Targeted Attack Platform

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2112
Identifiant de l'événement de Kaspersky Security Center	00000840
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le fonctionnement de l'application a été interrompu par l'administrateur du serveur Kaspersky Anti Targeted Attack Platform

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2113
Identifiant de l'événement de Kaspersky Security Center	00000841
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un fichier ou un flux a été supprimé par l'administrateur du serveur de Kaspersky Anti Targeted Attack Platform

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2111
Identifiant de l'événement de Kaspersky Security Center	0000083f
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un fichier a été restauré depuis la Quarantaine du serveur Kaspersky Anti Targeted Attack Platform par l'administrateur

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2110
Identifiant de l'événement de Kaspersky Security Center	0000083e
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un fichier a été mis en quarantaine sur le serveur de Kaspersky Anti Targeted Attack Platform par l'administrateur

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2109
Identifiant de l'événement de Kaspersky Security Center	0000083d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'activité réseau de toutes les applications tierces est bloquée

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2107
Identifiant de l'événement de Kaspersky Security Center	0000083b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'activité réseau de toutes les applications tierces est débloquée

État	⚠
Module	Endpoint Sensor
Identifiant de l'événement Windows	2108
Identifiant de l'événement de Kaspersky Security Center	0000083c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet sera supprimé après le redémarrage (Sandbox)

État	⚠
Module	Sandbox
Identifiant de l'événement Windows	2605
Identifiant de l'événement de Kaspersky Security Center	00000a2d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La taille totale des tâches d'analyse a dépassé la limite

État	⚠
Module	Sandbox
Identifiant de l'événement Windows	2612
Identifiant de l'événement de Kaspersky Security Center	00000a34
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le démarrage de l'objet est autorisé, l'événement est enregistré

État	⚠
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2553
Identifiant de l'événement de Kaspersky Security Center	000009fa
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le démarrage du processus est autorisé, l'événement est enregistré

État	⚠
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2554
Identifiant de l'événement de Kaspersky Security Center	000009f8
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet sera supprimé au redémarrage (Endpoint Detection and Response)

État	⚠
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2558
Identifiant de l'événement de Kaspersky Security Center	000009fe
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Isolement du réseau

État	⚠
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2700
Identifiant de l'événement de Kaspersky Security Center	00000a8c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Interruption de l'isolement du réseau

État	⚠
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2701
Identifiant de l'événement de Kaspersky Security Center	00000a8d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Il faut redémarrer l'ordinateur pour terminer la tâche

État	⚠
Module	Audit système
Identifiant de l'événement Windows	225
Identifiant de l'événement de Kaspersky Security Center	0000057b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La connexion à un site avec un certificat non approuvé est établie par décision de l'utilisateur

État	⚠
Module	Network Detection and Response (KATA)
Identifiant de l'événement Windows	70
Identifiant de l'événement de Kaspersky Security Center	00000046
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Message envoyé à l'administrateur sur l'interdiction du lancement de l'application

État	⚠
Module	Contrôle des applications
Identifiant de l'événement Windows	503
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Paramètres de l'événement	• GNRL_EA_DESCRIPTION est le message adressé à l'utilisateur. • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_6 est le nom du fichier exécutable de l'application (par exemple, chrome.exe). • GNRL_EA_PARAM_7 est le chemin d'accès au fichier exécutable. • GNRL_EA_PARAM_8 est le hachage de l'objet (SHA256). • GNRL_EA_PARAM_9 est la version de l'application que l'utilisateur essaie d'exécuter.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Message envoyé à l'administrateur sur l'interdiction de l'accès à l'appareil

État	⚠
Module	Contrôle des appareils
Identifiant de l'événement Windows	804
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Paramètres de l'événement	• c_er_descr est le message adressé à l'utilisateur. • GNRL_EA_PARAM_1 est l'identifiant du matériel (HWID). • GNRL_EA_PARAM_2 est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet

État	⚠
Module	Contrôle Internet
Identifiant de l'événement Windows	`755`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_WC_USER_REQUEST`
Paramètres de l'événement	• `GNRL_EA_DESCRIPTION` est le message adressé à l'utilisateur. • `GNRL_EA_PARAM_1` est l'URL. • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Interdiction de connexion de l'appareil

État	⚠
Module	Contrôle des appareils
Identifiant de l'événement Windows	`807`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est l'identifiant du matériel (HWID). • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Message envoyé à l'administrateur sur l'interdiction de l'action de l'application

État	⚠
Module	Contrôle évolutif des anomalies
Identifiant de l'événement Windows	`503`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Paramètres de l'événement	• `GNRL_EA_DESCRIPTION` est le message adressé à l'utilisateur. • `GNRL_EA_PARAM_1` est le nom de la règle du Contrôle évolutif des anomalies. • `GNRL_EA_PARAM_2` est l'identifiant de la règle heuristique. • `GNRL_EA_PARAM_3` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_4` est le processus source. • `GNRL_EA_PARAM_5` est l'objet source. • `GNRL_EA_PARAM_6` est le processus cible. • `GNRL_EA_PARAM_7` est l'objet cible. • `GNRL_EA_PARAM_8` est une information supplémentaire à propos de l'objet détecté : Hachage du processus/objet source et du processus/objet cible. Processus bloqué (`verdict_type`) : `true` ou `false`. Identifiant de sécurité de l'utilisateur (SID).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Lancement de l'application client de service cloud interdit

État	⚠
Module	Cloud Discovery
Identifiant de l'événement Windows	`2212`

Identifiant de l'événement de Kaspersky Security Center	000008a4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès au service cloud interdit

État	⚠
Module	Cloud Discovery
Identifiant de l'événement Windows	2213
Identifiant de l'événement de Kaspersky Security Center	000008a5
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un changement du fichier ou du dossier a été détecté

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2950
Identifiant de l'événement de Kaspersky Security Center	00000b86
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

L'objet est trop souvent modifié. L'agrégation des événements a commencé

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2955
Identifiant de l'événement de Kaspersky Security Center	00000b8b
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Rapport sur la modification d'un objet pour la période d'agrégation

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2956
Identifiant de l'événement de Kaspersky Security Center	00000b8c
Journal des événements Windows (par défaut)	–

Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Un changement du registre a été détecté

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2951`
Identifiant de l'événement de Kaspersky Security Center	`00000b87`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Connexion/Déconnexion de l'appareil détectée

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2952`
Identifiant de l'événement de Kaspersky Security Center	`00000b88`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

La zone de surveillance inclut des objets incorrects

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	`2903`
Identifiant de l'événement de Kaspersky Security Center	`00000b89`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

L'opération interdite a été autorisée en mode test

État	⚠
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2961
Identifiant de l'événement de Kaspersky Security Center	00000b91
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de se connecter au Serveur d'intégration pendant plus de 30 minutes. Vérifiez l'état du Serveur d'intégration et les paramètres du réseau

État	⚠
Module	Light Agent
Identifiant de l'événement Windows	3102
Identifiant de l'événement de Kaspersky Security Center	00000c1e
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de se connecter au Serveur d'intégration pendant plus de 6 heures. Vérifiez l'état du Serveur d'intégration et les paramètres du réseau

État	⚠
Module	Light Agent
Identifiant de l'événement Windows	3103
Identifiant de l'événement de Kaspersky Security Center	00000c1f
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Impossible de se connecter au Serveur d'intégration. Vérifiez l'état du Serveur d'intégration et les paramètres du réseau

État	⚠
Module	Light Agent
Identifiant de l'événement Windows	3101
Identifiant de l'événement de Kaspersky Security Center	00000c1d
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le modèle de machine virtuelle doit être mis à jour

État	⚠
Module	Light Agent
Identifiant de l'événement Windows	3181
Identifiant de l'événement de Kaspersky Security Center	00000c6d
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La licence Standard a expiré. L'application fonctionne sous la licence Enterprise

État	⚠
Module	Light Agent
Identifiant de l'événement Windows	3171
Identifiant de l'événement de Kaspersky Security Center	00000c64
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

État	⚠
Module	Contrôle de l'intégrité des fichiers
Identifiant de l'événement Windows	2901
Identifiant de l'événement de Kaspersky Security Center	00000b55
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

État	⚠
Module	Contrôle de l'intégrité des fichiers
Identifiant de l'événement Windows	2900
Identifiant de l'événement de Kaspersky Security Center	00000b54
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Messages d'information

L'application a été lancée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	235
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'application a été arrêtée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	236
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'Autodéfense a restreint l'accès à la ressource protégée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	213
Identifiant de l'événement de Kaspersky Security Center	000000d5
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le rapport a été purgé

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	217
Identifiant de l'événement de Kaspersky Security Center	000000d9
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Stratégie de groupe désactivée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	220
Identifiant de l'événement de Kaspersky Security Center	000000dc
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Les paramètres de l'application ont été modifiés

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	218
Identifiant de l'événement de Kaspersky Security Center	000000da
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

La tâche est lancée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	221
Identifiant de l'événement de Kaspersky Security Center	000000dd
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La tâche est terminée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	223
Identifiant de l'événement de Kaspersky Security Center	000000df
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Tous les modules de l'application, admis par la licence, sont installés et fonctionnent en mode normal

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	227
Identifiant de l'événement de Kaspersky Security Center	000000e3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Les paramètres de l'abonnement ont été modifiés

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	238
Identifiant de l'événement de Kaspersky Security Center	000000ee
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'abonnement a été renouvelé

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	239
Identifiant de l'événement de Kaspersky Security Center	000000ef
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet restauré depuis la Sauvegarde

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	335
Identifiant de l'événement de Kaspersky Security Center	0000014f
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Saisie du nom d'utilisateur et du mot de passe

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2000
Identifiant de l'événement de Kaspersky Security Center	000007d0
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

La participation à KSN est activée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2020
Identifiant de l'événement de Kaspersky Security Center	000007e4
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les serveurs de KSN sont disponibles

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2022
Identifiant de l'événement de Kaspersky Security Center	000007e6
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application fonctionne conformément à la législation locale et utilise l'infrastructure locale

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2024
Identifiant de l'événement de Kaspersky Security Center	000007e8
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet restauré depuis la Quarantaine

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	345
Identifiant de l'événement de Kaspersky Security Center	00000159
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet supprimé de la Quarantaine

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	347
Identifiant de l'événement de Kaspersky Security Center	0000015b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une copie de sauvegarde de l'objet a été créée

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces par emails Détection comportementale Protection contre le chiffrement Prévention des intrusions Sandbox Analyse des logiciels malveillants
Identifiant de l'événement Windows	308
Identifiant de l'événement de Kaspersky Security Center	00000134
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été écrasé par une copie désinfectée auparavant

État	ⓘ
Module	Protection contre les fichiers malicieux Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	327
Identifiant de l'événement de Kaspersky Security Center	00000147
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Une archive protégée par mot de passe a été détectée

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	322
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Paramètres de l'événement	• GNRL_EA_PARAM_2 est le nom de l'objet. • GNRL_EA_PARAM_3 est la date de création de l'objet (facultatif). • GNRL_EA_PARAM_7 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_9 est une information supplémentaire à propos de l'objet détecté : Module d'application (engine). Technologie de détection des menaces (method). Menace détectée par le KSN privé (liste de refus) : true or false.

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Informations relatives à l'objet détecté

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	`332`
Identifiant de l'événement de Kaspersky Security Center	`0000014c`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet se trouve dans une liste d'autorisation de Kaspersky Private Security Network

État	ⓘ
Module	Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Prévention des intrusions Analyse des logiciels malveillants
Identifiant de l'événement Windows	`340`
Identifiant de l'événement de Kaspersky Security Center	`00000154`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'objet a été renommé

État	ⓘ
Module	Protection contre les menaces par emails Protection contre les Exploits Détection comportementale Protection contre le chiffrement Analyse des logiciels malveillants
Identifiant de l'événement Windows	`329`
Identifiant de l'événement de Kaspersky Security Center	`00000149`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été traité

État	ⓘ
Module	Prévention des intrusions Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Analyse des logiciels malveillants
Identifiant de l'événement Windows	`301`

Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Un objet a été ignoré

État	ⓘ
Module	Prévention des intrusions Protection contre les fichiers malicieux Protection AMSI Analyse des logiciels malveillants
Identifiant de l'événement Windows	315
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Une archive a été détectée

État	ⓘ
Module	Prévention des intrusions Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Analyse des logiciels malveillants
Identifiant de l'événement Windows	318
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Un objet compressé a été détecté

État	ⓘ
Module	Prévention des intrusions Protection contre les fichiers malicieux Protection contre les menaces Internet Protection contre les menaces par emails Protection AMSI Analyse des logiciels malveillants
Identifiant de l'événement Windows	319
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le lien a été traité

État	ⓘ
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	361
Identifiant de l'événement de Kaspersky Security Center	–

Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le lancement de l'application est autorisé

État	ⓘ
Module	Contrôle des applications
Identifiant de l'événement Windows	701
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

La source des mises à jour a été sélectionnée

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1001
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le serveur proxy a été sélectionné

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1002
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le lien se trouve dans une liste d'autorisation de Kaspersky Private Security Network

État	ⓘ
Module	Protection contre les menaces Internet
Identifiant de l'événement Windows	370
Identifiant de l'événement de Kaspersky Security Center	00000172
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application est placée dans le groupe des applications de confiance

État	ⓘ
Module	Prévention des intrusions
Identifiant de l'événement Windows	401
Identifiant de l'événement de Kaspersky Security Center	00000191

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application a été placée dans un groupe à privilèges restreints

État	ⓘ
Module	Prévention des intrusions
Identifiant de l'événement Windows	`402`
Identifiant de l'événement de Kaspersky Security Center	`00000192`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Déclenchement du module Prévention des intrusions

État	ⓘ
Module	Prévention des intrusions
Identifiant de l'événement Windows	`403`
Identifiant de l'événement de Kaspersky Security Center	`00000193`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le fichier a été restauré

État	ⓘ
Module	Détection comportementale Protection contre le chiffrement Protection contre les Exploits Prévention des intrusions
Identifiant de l'événement Windows	`457`
Identifiant de l'événement de Kaspersky Security Center	`000001c9`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La valeur du registre a été restaurée

État	ⓘ
Module	Détection comportementale Protection contre les Exploits
Identifiant de l'événement Windows	`458`
Identifiant de l'événement de Kaspersky Security Center	`000001ca`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

La valeur du registre a été supprimée

État	ⓘ
Module	Détection comportementale Protection contre les Exploits

Identifiant de l'événement Windows	459
Identifiant de l'événement de Kaspersky Security Center	000001cb
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Action du processus ignorée

État	ⓘ
Module	Contrôle évolutif des anomalies
Identifiant de l'événement Windows	2201
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Paramètres de l'événement	• GNRL_EA_PARAM_1 est le nom de la règle du Contrôle évolutif des anomalies. • GNRL_EA_PARAM_2 est l'identifiant de la règle heuristique. • GNRL_EA_PARAM_3 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_4 est le processus source. • GNRL_EA_PARAM_5 est l'objet source. • GNRL_EA_PARAM_6 est le processus cible. • GNRL_EA_PARAM_7 est l'objet cible. • GNRL_EA_PARAM_8 est une information supplémentaire à propos de l'objet détecté : Hachage du processus/objet source et du processus/objet cible. Processus bloqué (verdict_type) : true ou false. Identifiant de sécurité de l'utilisateur (SID).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le clavier a été autorisé

État	ⓘ
Module	Protection BadUSB
Identifiant de l'événement Windows	2050
Identifiant de l'événement de Kaspersky Security Center	00000802
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'activité réseau est autorisée

État	ⓘ
Module	Pare-feu
Identifiant de l'événement Windows	601
Identifiant de l'événement de Kaspersky Security Center	00000259
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Le lancement de l'application est interdit en mode test

État	ⓘ
Module	Contrôle des applications
Identifiant de l'événement Windows	703

Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_DENIED`
Paramètres de l'événement	• `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_3` est l'identifiant de catégorie créé manuellement. • `GNRL_EA_PARAM_4` est l'identifiant de sécurité du compte (SID). • `GNRL_EA_PARAM_5` est une information sur la signature numérique de l'application. • `GNRL_EA_PARAM_6` est le nom du fichier exécutable de l'application (par exemple, chrome.exe). • `GNRL_EA_PARAM_7` est le chemin d'accès au fichier exécutable. • `GNRL_EA_PARAM_8` est le hachage de l'objet (SHA256). • `GNRL_EA_PARAM_9` est la version de l'application que l'utilisateur essaie d'exécuter.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le lancement de l'application est autorisé en mode test

État	ⓘ
Module	Contrôle des applications
Identifiant de l'événement Windows	`704`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_ALLOW`
Paramètres de l'événement	• `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session. • `GNRL_EA_PARAM_3` est l'identifiant de catégorie créé manuellement. • `GNRL_EA_PARAM_4` est l'identifiant de sécurité du compte (SID). • `GNRL_EA_PARAM_5` est une information sur la signature numérique de l'application.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Page autorisée ouverte

État	ⓘ
Module	Contrôle Internet
Identifiant de l'événement Windows	`751`
Identifiant de l'événement de Kaspersky Security Center	`000002f4`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

L'opération avec l'appareil est autorisée

État	ⓘ
Module	Contrôle des appareils
Identifiant de l'événement Windows	`801`
Identifiant de l'événement de Kaspersky Security Center	`00000321`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Une opération a été exécutée sur un fichier

État	ⓘ
Module	Contrôle des appareils

Identifiant de l'événement Windows	808
Identifiant de l'événement de Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Paramètres de l'événement	• GNRL_EA_PARAM_1 est l'opération sur le fichier (écriture ou suppression). • GNRL_EA_PARAM_2 est le chemin d'accès au fichier. • GNRL_EA_PARAM_3 est le nom de l'appareil. • GNRL_EA_PARAM_4 est le nom de l'utilisateur de la session. • GNRL_EA_PARAM_5 est l'identifiant du matériel (HWID).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Il n'y a pas de mises à jour disponibles

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1020
Identifiant de l'événement de Kaspersky Security Center	000003fc
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

La copie des mises à jour a réussi

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1022
Identifiant de l'événement de Kaspersky Security Center	000003fe
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Téléchargement de fichiers...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1003
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le fichier a été téléchargé

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1004
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le fichier a été installé

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1005
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le fichier a été mis à jour

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1006
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le fichier a été restauré en raison d'une erreur de mise à jour

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1007
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Mise à jour des fichiers...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1008
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Copie des mises à jour...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1009
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Remise à l'état antérieur des fichiers...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1010
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Composition de la liste des fichiers à télécharger...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	1013
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Téléchargement des correctifs...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2150
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Installation du correctif...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2151
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Un correctif a été installé

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2152
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Annulation du correctif...

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2154
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Annulation du correctif terminée

État	ⓘ
Module	Mise à jour
Identifiant de l'événement Windows	2155
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'application des règles de chiffrement/déchiffrement des fichiers est en cours

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	901
Identifiant de l'événement de Kaspersky Security Center	00000385
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'application des règles de chiffrement/déchiffrement des fichiers est terminée

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	902
Identifiant de l'événement de Kaspersky Security Center	00000386
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Reprise d'application des règles de chiffrement/déchiffrement des fichiers

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	905
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Lancement du chiffrement/déchiffrement du fichier

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	910
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Fin du chiffrement/déchiffrement du fichier

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	911
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le fichier n'a pas été chiffré car il s'agit d'une exclusion

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	913
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le mode portable est activé

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	950
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le mode portable est désactivé

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	952
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Lancement du chiffrement/déchiffrement de l'appareil

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1301
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Fin du chiffrement/déchiffrement de l'appareil

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1302
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Reprise du chiffrement/déchiffrement de l'appareil

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1304
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

L'appareil n'est pas chiffré

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1307
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le processus de chiffrement/déchiffrement de l'appareil est passé en mode actif

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1308
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le processus de chiffrement/déchiffrement de l'appareil est passé en mode passif

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1309
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le module de chiffrement a été chargé

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1310
Identifiant de l'événement de Kaspersky Security Center	0000051e
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Création d'un compte utilisateur de l'Agent d'authentification

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1330
Identifiant de l'événement de Kaspersky Security Center	00000532
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Un compte utilisateur de l'Agent d'authentification a été supprimé

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1331
Identifiant de l'événement de Kaspersky Security Center	00000533
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Le mot de passe du compte utilisateur de l'Agent d'authentification a été modifié

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1332
Identifiant de l'événement de Kaspersky Security Center	00000534
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

L'authentification dans l'Agent d'authentification a réussi

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1333
Identifiant de l'événement de Kaspersky Security Center	00000535
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

L'authentification dans l'Agent d'authentification s'est soldée par une erreur

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1334
Identifiant de l'événement de Kaspersky Security Center	00000536
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

L'accès au disque dur a été obtenu à l'aide de la procédure de demande d'accès aux appareils chiffrés

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1335
Identifiant de l'événement de Kaspersky Security Center	00000537
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

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

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1336
Identifiant de l'événement de Kaspersky Security Center	00000538
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Le compte n'a pas été ajouté. Ce compte existe déjà

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1337
Identifiant de l'événement de Kaspersky Security Center	00000539
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Le compte n'a pas été modifié. Ce compte n'existe pas

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1338
Identifiant de l'événement de Kaspersky Security Center	0000053a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Le compte n'a pas été supprimé. Ce compte n'existe pas

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1339
Identifiant de l'événement de Kaspersky Security Center	0000053b
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

La mise à jour de la fonction de chiffrement a réussi

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1341
Identifiant de l'événement de Kaspersky Security Center	0000053d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La restauration de la mise à jour de la fonction de chiffrement a réussi

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1343
Identifiant de l'événement de Kaspersky Security Center	0000053f
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Échec de la désinstallation des pilotes de Kaspersky Disk Encryption dans l'image WinRE

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1346
Identifiant de l'événement de Kaspersky Security Center	00000542
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La clé de récupération BitLocker a été modifiée

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1370
Identifiant de l'événement de Kaspersky Security Center	0000055a
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le mot de passe/code PIN de BitLocker a été modifié

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1371
Identifiant de l'événement de Kaspersky Security Center	0000055b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La clé de récupération BitLocker a été enregistrée sur un disque amovible

État	ⓘ
Module	Chiffrement des données
Identifiant de l'événement Windows	1372
Identifiant de l'événement de Kaspersky Security Center	0000055c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les tâches du serveur Kaspersky Anti Targeted Attack Platform ne sont pas traitées

État	ⓘ
Module	Endpoint Sensor
Identifiant de l'événement Windows	2103
Identifiant de l'événement de Kaspersky Security Center	00000837
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Endpoint Sensor connecté au serveur

État	ⓘ
Module	Endpoint Sensor
Identifiant de l'événement Windows	2101
Identifiant de l'événement de Kaspersky Security Center	00000835
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion au serveur Kaspersky Anti Targeted Attack Platform rétablie

État	ⓘ
Module	Endpoint Sensor
Identifiant de l'événement Windows	2102
Identifiant de l'événement de Kaspersky Security Center	00000836
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Les tâches du serveur Kaspersky Anti Targeted Attack Platform sont en cours de traitement

État	ⓘ
Module	Endpoint Sensor
Identifiant de l'événement Windows	2104
Identifiant de l'événement de Kaspersky Security Center	00000838
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été supprimé

État	ⓘ
Module	Suppression des données
Identifiant de l'événement Windows	2251
Identifiant de l'événement de Kaspersky Security Center	000008cb
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	–

Statistiques de la tâche de suppression

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises)
Identifiant de l'événement Windows	2853
Identifiant de l'événement de Kaspersky Security Center	00000b25
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

État	ⓘ
Module	Suppression des données
Identifiant de l'événement Windows	2253
Identifiant de l'événement de Kaspersky Security Center	000008cd
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet mis en quarantaine (Sandbox)

État	ⓘ
Module	Sandbox

Identifiant de l'événement Windows	2602
Identifiant de l'événement de Kaspersky Security Center	00000a2a
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet supprimé (Sandbox)

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	2604
Identifiant de l'événement de Kaspersky Security Center	00000a2c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Analyse IOC démarrée

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2652
Identifiant de l'événement de Kaspersky Security Center	00000a5c
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Analyse IOC terminée

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2653
Identifiant de l'événement de Kaspersky Security Center	00000a5d
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Objet mis en quarantaine (Endpoint Detection and Response)

État	ⓘ
Module	Endpoint Detection and Response
Identifiant de l'événement Windows	2555
Identifiant de l'événement de Kaspersky Security Center	000009fb
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un objet a été supprimé (Endpoint Detection and Response)

État	ⓘ
Module	Endpoint Detection and Response

Identifiant de l'événement Windows	2557
Identifiant de l'événement de Kaspersky Security Center	000009fd
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

La sélection de modules de l'application a été modifiée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	1402
Identifiant de l'événement de Kaspersky Security Center	0000057a
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	2606
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	2609
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	2610
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	2616
Identifiant de l'événement de Kaspersky Security Center	–
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	–

Le Serveur d'administration auquel votre appareil est connecté est défini comme étant fiable

État	ⓘ
Module	Protection de la connexion au Serveur d'administration
Identifiant de l'événement Windows	`3300`
Identifiant de l'événement de Kaspersky Security Center	`00000ce4`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Votre appareil est connecté à un nouveau Serveur d'administration fiable

État	ⓘ
Module	Protection de la connexion au Serveur d'administration
Identifiant de l'événement Windows	`3302`
Identifiant de l'événement de Kaspersky Security Center	`00000ce6`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Le Serveur d'administration auquel votre appareil est connecté n'est plus considéré comme étant fiable

État	ⓘ
Module	Protection de la connexion au Serveur d'administration
Identifiant de l'événement Windows	`3303`
Identifiant de l'événement de Kaspersky Security Center	`00000ce7`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Détection asynchrone de Sandbox

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	`2619`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_APP_INCIDENT_OCCURED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` sont les paramètres des modules Sandbox. • `GNRL_EA_PARAM_2` est le chemin d'accès à l'objet. • `GNRL_EA_PARAM_3` est l'identifiant de l'incident. • `GNRL_EA_PARAM_4` est le hachage de l'objet (SHA256).
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

La tâche d'analyse a été envoyée avec succès à Sandbox par l'utilisateur

État	ⓘ
Module	Sandbox
Identifiant de l'événement Windows	`2622`
Identifiant de l'événement de Kaspersky Security Center	`00000a3e`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'appareil est connecté

État	ⓘ
Module	Contrôle des appareils
Identifiant de l'événement Windows	`805`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est l'identifiant du matériel (HWID). • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

L'appareil est déconnecté

État	ⓘ
Module	Contrôle des appareils
Identifiant de l'événement Windows	`806`
Identifiant de l'événement de Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Paramètres de l'événement	• `GNRL_EA_PARAM_1` est l'identifiant du matériel (HWID). • `GNRL_EA_PARAM_2` est le nom de l'utilisateur de la session.
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réussie au serveur EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises)
Identifiant de l'événement Windows	`2853`
Identifiant de l'événement de Kaspersky Security Center	`00000b25`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réussie au serveur de réponse EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identifiant de l'événement Windows	`2853`
Identifiant de l'événement de Kaspersky Security Center	`00000b25`
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réussie au serveur de collecte de télémétrie EDR Expert

État	ⓘ
Module	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)

Identifiant de l'événement Windows	2857
Identifiant de l'événement de Kaspersky Security Center	00000b26
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réussie au serveur NDR

État	ⓘ
Module	Network Detection and Response (KATA)
Identifiant de l'événement Windows	3083
Identifiant de l'événement de Kaspersky Security Center	00000c0b
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Lancement de l'application client de service cloud autorisé

État	ⓘ
Module	Cloud Discovery
Identifiant de l'événement Windows	2210
Identifiant de l'événement de Kaspersky Security Center	000008a2
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès au service cloud autorisé

État	ⓘ
Module	Cloud Discovery
Identifiant de l'événement Windows	2211
Identifiant de l'événement de Kaspersky Security Center	000008a3
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Accès à la zone protégée

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	2004
Identifiant de l'événement de Kaspersky Security Center	000007d4
Journal des événements Windows (par défaut)	✓
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un changement du fichier ou du dossier a été détecté

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système

Identifiant de l'événement Windows	2950
Identifiant de l'événement de Kaspersky Security Center	00000b86
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

L'objet est trop souvent modifié. L'agrégation des événements a commencé

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2955
Identifiant de l'événement de Kaspersky Security Center	00000b8b
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Rapport sur la modification d'un objet pour la période d'agrégation

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2956
Identifiant de l'événement de Kaspersky Security Center	00000b8c
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Un changement du registre a été détecté

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2951
Identifiant de l'événement de Kaspersky Security Center	00000b87
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Connexion/Déconnexion de l'appareil détectée

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2952
Identifiant de l'événement de Kaspersky Security Center	00000b88
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

La zone de surveillance inclut des objets incorrects

État	ⓘ / ⚠ / ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2903
Identifiant de l'événement de Kaspersky Security Center	00000b89
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Référence créée

État	ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2957
Identifiant de l'événement de Kaspersky Security Center	00000b8d
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Référence mise à jour

État	ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2958
Identifiant de l'événement de Kaspersky Security Center	00000b8e
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Une opération est effectuée par l'utilisateur de confiance

État	ⓘ
Module	Contrôle de l'intégrité du système
Identifiant de l'événement Windows	2962
Identifiant de l'événement de Kaspersky Security Center	00000b92
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Pour configurer la durée de conservation de cet événement, accédez à la page **Configuration de l'événement** de la stratégie et définissez la période de conservation pour l'événement général Contrôle de l'intégrité du système – *Un changement du fichier ou du dossier a été détecté*.

Connecté à la SVM

État	ⓘ
Module	Light Agent
Identifiant de l'événement Windows	3152
Identifiant de l'événement de Kaspersky Security Center	00000c50
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Un mot de passe temporaire a été créé

État	ⓘ
Module	Audit système
Identifiant de l'événement Windows	265
Identifiant de l'événement de Kaspersky Security Center	00000109
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connecté au Serveur d'intégration

État	ⓘ
Module	Light Agent
Identifiant de l'événement Windows	3105
Identifiant de l'événement de Kaspersky Security Center	00000c21
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Restauration de la connexion au Serveur d'intégration...

État	ⓘ
Module	Light Agent
Identifiant de l'événement Windows	3104
Identifiant de l'événement de Kaspersky Security Center	00000c20

Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Connexion réussie au serveur KUMA

État	ⓘ
Module	Intégration KUMA
Identifiant de l'événement Windows	`2857`
Identifiant de l'événement de Kaspersky Security Center	`00000b29`
Journal des événements Windows (par défaut)	–
Journal des événements de Kaspersky Security Center (par défaut)	✓

Annexe 7. Extensions de fichier prises en charge pour Prévention de l'exécution

Kaspersky Endpoint Security prend en charge la prévention de l'ouverture de fichiers au format office dans certaines applications. Le tableau suivant reprend les informations relatives aux extensions de fichier et aux applications prises en charge.

Extensions de fichier prises en charge pour Prévention de l'exécution

Nom de l'application	Fichier exécutable	Extension de fichier
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw

Nom de l'application	Fichier exécutable	Extension de fichier
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Navigateur Yandex Navigateur Tor	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Annexe 8. Interpréteurs de script pris en charge pour la prévention de l'exécution

Prévention de l'exécution prend en charge les interpréteurs de script suivants :

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe

- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Prévention de l'exécution est compatible avec les applications Java dans l'environnement d'exécution Java (processus java.exe et javaw.exe).

Annexe 9. Zone de l'analyse IOC dans le registre (RegistryItem)

Lorsque vous ajoutez le type de données **Registre Windows - RegistryItem** à la zone de l'analyse IOC, Kaspersky Endpoint Security analyse les clés de registre suivantes :

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile
```

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Annexe 10. Exigences relatives aux fichiers IOC

Lorsque vous créez des tâches d'analyse IOC, tenez compte des exigences et des limites suivantes relatives aux fichiers IOC :

- L'application prend en charge les fichiers IOC avec les extensions XML du standard ouvert OpenIOC versions 1.0 et 1.1 pour la description des indicateurs de compromission.

- Après avoir téléchargé les fichiers IOC, vous pouvez modifier les fichiers manuellement dans l'éditeur intégré directement dans les propriétés de la tâche. Kaspersky Endpoint Security prend en charge l'édition des fichiers IOC conformes à la norme OpenIOC 1.1. Il n'est pas possible de modifier le contenu des fichiers IOC conformes à OpenIOC version 1.0.

- Si, lors de la création d'une tâche d'*Analyse IOC* à partir de la ligne de commande, vous chargez des fichiers IOC, dont certains ne sont pas pris en charge lorsque la tâche est exécutée, l'application utilise uniquement les fichiers IOC pris en charge. Si, lors de la création d'une tâche d'*Analyse IOC* à partir de la ligne de commande, tous les fichiers IOC que vous chargez ne sont pas pris en charge, la tâche peut quand même être exécutée, mais elle ne détectera aucun indicateur de compromission. Il n'est pas possible de téléverser des fichiers IOC non pris en charge à l'aide de Web Console ou de Cloud Console.

- Les erreurs sémantiques et les termes IOC et les tags non pris en charge dans les fichiers IOC ne font pas échouer l'exécution de la tâche. Dans ces sections des fichiers IOC, l'application ne détecte aucune correspondance.

- Les identifiants de tous les fichiers IOC utilisés dans une même tâche d'analyse IOC Scan doivent être uniques. S'il y a des fichiers IOC avec le même identifiant, cela peut affecter les résultats de l'exécution de la tâche.

- Un seul fichier IOC ne doit pas dépasser 2 Mo. L'utilisation de fichiers plus volumineux entraînera la fin des tâches d'analyse IOC avec une erreur. La taille totale de tous les fichiers ajoutés à la collection IOC ne doit pas dépasser 10 Mo. Si la taille totale de tous les fichiers dépasse 10 Mo, vous devez scinder la collection IOC et créer plusieurs tâches *Analyse IOC*.

- Il est recommandé de créer un fichier IOC par menace. Cela facilite l'analyse des résultats de la tâche *Analyse IOC*.

Le fichier que vous pouvez télécharger via le lien ci-dessous contient une table reprenant la liste complète des termes IOC de la norme OpenIOC.

DOWNLOAD THE IOC_TERMS.XLSX FILE

Les fonctionnalités et les limites de la prise en charge de l'application pour le standard OpenIOC sont présentées dans le tableau suivant.

Conditions prises en charge	OpenIOC 1.0 :
	
	`is`
	`isnot` (comme exception à l'ensemble)
	`contains`
	`containsnot` (comme exception à l'ensemble)
	OpenIOC 1.1 :
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Pour les termes Email/*, seules les conditions `contains` et `is` sont prises en charge. Pour que l'analyse IOC rétrospective fonctionne correctement, lors de l'utilisation de la condition `is`, les adresses email dans les fichiers IOC doivent être au format suivant : `"name@example.org" <SMTP:name@example.org>`. Lors de l'exécution de la tâche *Analyse IOC* normalement, il suffit d'indiquer l'adresse email au format suivant : `name@example.org`.

Attributs de condition pris en charge	OpenIOC 1.1 :
	
	`preserve-case`
	`negate`

Opérateurs pris en charge	`AND` `OR`
Types de données pris en charge	`"date"` : date (conditions applicables : `is`, `greater-than`, `less-than`) `"int"` : entier (conditions applicables : `is`, `greater-than`, `less-than`) `"string"` : chaîne (conditions applicables : `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"` : durée en secondes (conditions applicables : `is`, `greater-than`, `less-than`)

Caractéristiques de l'interprétation des types de données	Les types de données `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` et `"base64Binary"` sont interprétés comme des chaînes.
	
	L'application prend en charge l'interprétation du paramètre `Content` pour les types de données `int` et `date` lorsqu'il est défini sous forme d'intervalles :
	
	OpenIOC 1.0 :
	Utilisation de l'opérateur `TO` dans le champ `Content` :
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1 :
	Utilisation des conditions `greater-than` et `less-than`
	Utilisation de l'opérateur `TO` dans le champ `Content`
	L'application prend en charge l'interprétation des types de données `date` et `duration` si les indicateurs sont définis au format `ISO 8601, Zulu time zone, UTC`.

Annexe 11. API pour la réponse aux menaces EDR

Kaspersky Endpoint Security 12.9 for Windows prend désormais en charge les actions de réponse aux menaces EDR (EDR responses) à l'aide de Kaspersky Security Center OpenAPI. Autrement dit, vous pouvez appeler des méthodes OpenAPI pour automatiser la réponse aux menaces EDR à l'aide de Python. Vous pouvez appeler ces méthodes lorsqu'elles sont intégrées à des solutions SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, la solution de Kaspersky SIEM, prend en charge la réponse aux menaces EDR OpenAPI à partir de la version 3.4.1. Vous trouverez des exemples de scripts dans la documentation de KUMA.

Pour exécuter les actions de réponse aux menaces EDR, vous devez créer une demande et l'envoyer à l'aide de KSC Open API (`AddIncident`). Une fois que la demande est traitée, la tâche spéciale est créée dans la console de Kaspersky Security Center.

> Pour créer des tâches en réponse aux menaces EDR, vous devez établir une connexion en arrière-plan entre le Serveur d'administration et Kaspersky Security Center Web Console. Le service de connexion en arrière-plan est disponible dans Kaspersky Security Center Windows 14.2 ou toute version ultérieure et dans Kaspersky Security Center Linux 15.2 ou toute version ultérieure. Les autres consoles, y compris les consoles des solutions Kaspersky Detection and Response, ne sont pas prises en charge.

Pour la réponse aux menaces EDR, vous devez préciser des paramètres de requête de base, par exemple, au format JSON :

- `task` est le type de la tâche (voir ci-dessous).
- `targetHost` est l'identifiant de l'ordinateur sur lequel le script doit être exécuté. Argument requis. Le script obtient cet argument à partir de l'événement.
- `responseEventIncidentArea` est le nom de l'application qui a exécuté le script (par exemple, `KUMA`). Ce paramètre s'ajoute au nom de la tâche créée.

Pour configurer la réponse aux menaces EDR, vous devez préciser les paramètres de la tâche au format JSON dans le paramètre `"KLINCDT_BODY": json.dumps(data)`. Par conséquent, l'application crée le `[Response] [KUMA] <task type> - <Date> <Time> - <ID>` dans la console de Kaspersky Security Center.

Connexion à Kaspersky Security Center OpenAPI

Dans le cadre de la réponse aux menaces EDR, l'application crée des tâches spéciales dans la console de Kaspersky Security Center. La création de ces tâches requiert l'établissement d'une connexion entre l'ordinateur et Kaspersky Security Center. Pour ce faire, les paramètres de connexion à Kaspersky Security Center doivent être précisés dans la requête.

> Dans Kaspersky XDR version 2.1, le mode d'autorisation des requêtes a changé. Kaspersky XDR utilise des jetons PAT à la place de l'authentification par nom d'utilisateur et mot de passe. Par conséquent, il n'est pas possible d'exécuter des scripts dans Kaspersky XDR. Pour en savoir plus sur l'autorisation des demandes, veuillez consulter l'aide de Kaspersky XDR.

Paramètres de connexion à Kaspersky Security Center

Paramètre	Type	Description
`kscHost`	`string`	Adresse du Serveur d'administration de Kaspersky Security Center. Paramètre obligatoire.
`kscPort`	`int`	Port de connexion au Serveur d'administration. Paramètre obligatoire.
`kscCert`	`string`	Chemin d'accès au fichier de certificat de connexion au Serveur d'administration de Kaspersky Security Center. Par défaut, le paramètre est défini sur `False`.
`kscUser`	`string`	Nom du compte utilisateur. Paramètre obligatoire.
`kscPassword`	`string`	Mot de passe du compte utilisateur. Paramètre obligatoire.

Exemple

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Les données du compte utilisateur ne sont pas protégées, vous devez donc dédier un utilisateur distinct qui sera utilisé pour effectuer uniquement ces actions.

Obtention du fichier – getFile

Paramètres de la tâche Obtention du fichier

Paramètre	Type	Description
md5hash	string	Hachage MD5 du fichier que vous souhaitez obtenir.
sha256hash	string	Hachage SHA256 du fichier que vous souhaitez obtenir.
path	string	Chemin d'accès au fichier que vous souhaitez obtenir.

Exemple

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Supprimer le fichier – deleteFile

Paramètres de la tâche Supprimer le fichier

Paramètre	Type	Description
`md5hash`	`string`	Hachage MD5 du fichier que vous souhaitez supprimer.
`sha256hash`	`string`	Hachage SHA256 du fichier que vous souhaitez supprimer.
`path`	`string`	Chemin d'accès au fichier que vous souhaitez supprimer.
`searchInSubfolders?`	`boolean`	Recherchez le fichier que vous souhaitez supprimer dans les sous-dossiers.

Exemple

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Placer le fichier en Quarantaine – quarantineFile

Paramètres de la tâche Placer le fichier en Quarantaine

Paramètre	Type	Description
`md5hash`	`string`	Hachage MD5 du fichier que vous souhaitez mettre en quarantaine.
`sha256hash`	`string`	Hachage SHA256 du fichier que vous souhaitez mettre en quarantaine.
`path`	`string`	Chemin d'accès au fichier que vous souhaitez mettre en quarantaine.

Exemple

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Analyse IOC – iocScan

Paramètres de la tâche Analyse IOC

Paramètre	Type	Description
`ioc`	`string`	Chemin d'accès à l'archive ZIP contenant le fichier IOC que vous souhaitez utiliser pour effectuer l'analyse.
`isolateHost`	`boolean`	Isolez l'ordinateur du réseau lorsqu'un indicateur de compromission est détecté pour empêcher la menace de se propager.
`scanCriticalAreas`	`boolean`	Exécutez la tâche *Analyse des zones critiques* lorsqu'un indicateur de compromission est détecté.
`quarantineObject`	`boolean`	Supprimez l'objet malveillant dès que l'indicateur de compromission est détecté. Avant de supprimer l'objet, Kaspersky Endpoint Security crée une copie de sauvegarde au cas où l'objet devrait être restauré ultérieurement. Kaspersky Endpoint Security déplace la copie de sauvegarde dans la Quarantaine.

Exemple

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Démarrez le processus – startProcess

Paramètres de la tâche Démarrez le processus

Paramètre	Type	Description
`executablePath`	`string`	Chemin d'accès au fichier exécutable utilisé pour lancer le processus.
`arguments?`	`string`	Arguments de ligne de commande supplémentaires pour le lancement du processus.
`workingFolder?`	`string`	Chemin d'accès au dossier de travail du processus.

Exemple

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Fin du processus – terminateProcess

Paramètres de la tâche Fin du processus

Paramètre	Type	Description
`md5hash`	`string`	Hachage MD5 du fichier dont vous souhaitez arrêter le processus.
`sha256hash`	`string`	Hachage SHA256 du fichier dont vous souhaitez arrêter le processus.
`path`	`string`	Chemin d'accès au fichier que vous souhaitez supprimer.
`caseSensitive`	`boolean`	Le respect de la casse lors de la recherche du fichier.

Exemple

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Isolement du réseau pour l'ordinateur – isolateHost

Paramètres d'isolement du réseau pour l'ordinateur

Paramètre	Type	Description
`action`	`string`	Mode de fonctionnement de l'isolement du réseau.

Exemple

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prévention de l'exécution – preventExecution

Paramètres de Prévention de l'exécution

Paramètre	Type	Description
hash	string	Hachage MD5 du fichier dont vous souhaitez empêcher l'exécution.
path	string	Chemin d'accès au fichier dont vous souhaitez empêcher l'exécution.
caseSensitive	boolean	Le respect de la casse lors de la recherche du fichier.

Exemple

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Analyse des logiciels malveillants – onDemandScan

Paramètres de la tâche Analyse des logiciels malveillants

Paramètre	Type	Description
path	string	Liste de fichiers et de dossiers séparés par des espaces pour l'analyse personnalisée.
recursive	boolean	Mode d'analyse récursif.
type	number	Zone d'analyse.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Exemple

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
```

```
  responseEventIncidentArea: string;
};
```

Annexe 12. Comptes utilisateurs dans les règles des modules d'application

Pour configurer certains modules de l'application, vous devez ajouter des règles spéciales. Par exemple, pour le Contrôle Internet, vous devez ajouter une règle avec une liste d'adresses Internet que l'application doit bloquer. Dans les règles des modules d'application, vous pouvez également configurer une planification pour le module ou sélectionner les utilisateurs auxquels l'application doit appliquer la règle.

Pour la configuration des modules d'application suivants, il est nécessaire d'ajouter des règles :

- Contrôle des applications.
- Contrôle Internet.
- Contrôle des appareils.
- Inspection des journaux.
- Contrôle évolutif des anomalies.
- Contrôle de l'intégrité du système.

À partir de Kaspersky Endpoint Security for Windows 12.5, vous pouvez sélectionner des utilisateurs non seulement dans Active Directory, mais également dans la liste des utilisateurs de Kaspersky Security Center. Vous pouvez également saisir les données du compte utilisateur local manuellement. Cela signifie que vous pouvez ajouter des utilisateurs comme suit :

- Active Directory (recommandé)
- Liste des utilisateurs dans Kaspersky Security Center
- Compte utilisateur local

> Afin d'utiliser correctement toutes les méthodes de sélection des utilisateurs, vous devez mettre à jour l'application Kaspersky Endpoint Security ainsi que le plug-in de gestion vers la version 12.5 ou vers une version ultérieure.

Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Pour en savoir plus sur les risques de sécurité liés à l'utilisation de comptes locaux, consultez la Base de connaissances Microsoft. Vous assumez l'entière responsabilité de la sécurité de l'ordinateur en cas d'utilisation de comptes utilisateurs locaux. En particulier, cela inclut la responsabilité de contrôler et de limiter l'accès aux paramètres de Kaspersky Endpoint Security.

L'application utilise le SID (Security Identifier) de l'utilisateur pour identifier les utilisateurs. Lors de l'utilisation de comptes utilisateurs depuis Active Directory ou depuis la liste des utilisateurs de Kaspersky Security Center, l'application détermine le SID sur le Serveur d'administration. Cela signifie que l'application n'impose pas de charge supplémentaire à l'ordinateur pour identifier l'utilisateur. Si vous avez ajouté plus de 1 000 comptes utilisateurs locaux à une règle d'application, l'application contacte le contrôleur de domaine pour identifier l'utilisateur. Cela signifie que la charge de l'ordinateur est augmentée. Pour optimiser l'impact sur les performances de l'ordinateur, nous vous recommandons d'utiliser des comptes utilisateurs d'Active Directory ou de la liste des utilisateurs de Kaspersky Security Center.

L'application utilise les noms NetBIOS pour identifier les comptes utilisateurs ajoutés manuellement aux formats `<username>` et `<hostname>\<username>`. Le nom NetBIOS peut comporter jusqu'à 16 octets (15 caractères). Si le nom de l'ordinateur comporte plus de 15 caractères, l'application ne peut pas identifier l'utilisateur. Ensuite, l'application désactive la règle et génère une erreur, par exemple, *Contrôle Internet : le déclenchement des règles est désactivé pour les comptes utilisateurs sans identifiant de sécurité (SID) correspondant*. Pour que la règle fonctionne, vous devez raccourcir le nom de l'ordinateur manuellement. Vous pouvez ajouter des comptes utilisateurs à partir d'Active Directory ou de Kaspersky Security Center. Dans ce cas, l'application raccourcit automatiquement le nom de l'ordinateur.

Kaspersky Endpoint Security prend également en charge les utilisateurs et les groupes intégrés (comme le groupe « Tous ») dans les règles. En raison du mode de détermination du SID de l'utilisateur, l'application permet d'utiliser uniquement les comptes utilisateurs intégrés ajoutés à partir d'Active Directory ou de la liste des utilisateurs de Kaspersky Security Center. Les règles dans lesquelles un compte utilisateur intégré est ajouté localement ne fonctionnent pas.

Informations légales

À propos des données

Cette section contient des informations sur les données que l'application Kaspersky Endpoint Security peut stocker sur l'appareil et transmettre automatiquement à Kaspersky pendant son fonctionnement.

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.

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 ;
- identifiant unique de la demande aux services du Détenteur des droits ;
- identifiants des modules 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 actuelle ;
  - clé active ;
  - durée de validité de la licence de Kaspersky Endpoint Security ;
  - état actuel de la licence ;
  - type de licence actuelle ;
  - 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 de 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 de 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, liste des actions réalisées par l'application malveillante et la décision prise par le logiciel et l'utilisateur en réponse à celles-ci, 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 Détenteur 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, somme de contrôle (MD5) du profil récolté pour l'objet, 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 ;

- DNS 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 (UEFL 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, chemine 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 d'ETW, fournisseurs d'événements EventTrace / EventMetadata de Microsoft : informations sur la séquence des événements système (type, heure, date, fuseau horaire), métadonnées sur le fichier avec résultats de traçage (nom, structure, paramètres de traçage, répartition du nombre d'opérations de trace par type), informations sur le système d'exploitation (nom, type, version, build, date de sortie, heure de début) ;

- 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.

Collecte des données lors de l'utilisation de solutions Detection and Response

Les données préparées pour l'envoi automatique vers les serveurs de Kaspersky Endpoint Detection and Response, de Kaspersky Sandbox et de Kaspersky Anti Targeted Attack Platform sont stockées sur les ordinateurs sur lesquels Kaspersky Endpoint Security est installé. Les fichiers sont stockés sur les ordinateurs sous une forme simple et non chiffrée.

L'ensemble spécifique de données dépend de la solution dans laquelle Kaspersky Endpoint Security est utilisé.

Kaspersky Endpoint Detection and Response

Toutes les données que l'application stocke localement sur l'ordinateur sont supprimées de l'ordinateur lors de la désinstallation de Kaspersky Endpoint Security.

Données reçues à la suite de l'exécution de la tâche Analyse IOC (tâche standard)

Kaspersky Endpoint Security soumet automatiquement les données sur les résultats de l'exécution de la tâche *Analyse IOC* à Kaspersky Security Center.

Les données des résultats d'exécution de la tâche *Analyse IOC* peuvent contenir les informations suivantes :

- Adresse IP de la table ARP
- Adresse physique de la table ARP
- Type et nom d'enregistrement DNS
- Adresse IP de l'ordinateur protégé
- Adresse physique (adresse MAC) de l'ordinateur protégé
- Identifiant dans l'entrée du journal des événements
- Nom de la source de données dans le journal
- Nom du journal
- Heure de l'événement
- Hachages MD5 et SHA256 du fichier
- Nom complet du fichier (y compris le chemin)
- Taille du fichier
- Adresse IP et port distants auxquels la connexion a été établie pendant l'analyse
- Adresse IP de l'adaptateur local
- Port ouvert sur l'adaptateur local
- Protocole sous forme de numéro (conformément à la norme IANA)
- Nom du processus
- Arguments du processus

- Chemin d'accès au fichier du processus
- Identifiant Windows (PID) du processus
- Identifiant Windows (PID) du processus parent
- Compte utilisateur qui a lancé le processus
- Date et heure de démarrage du processus
- Nom du service
- Description du service
- Chemin et nom du service DLL (pour svchost)
- Chemin et nom du fichier exécutable du service
- Identifiant Windows (PID) du service
- Type de service (par exemple, un pilote ou un adaptateur de noyau)
- État du service
- Mode de lancement du service
- Nom du compte utilisateur.
- Nom du volume
- Lettre du volume
- Type de volume
- Valeur du registre Windows
- Valeur de la section du registre
- Chemin d'accès à la clé de registre (sans nom de section ni de valeur)
- Paramètre de registre
- Système (environnement)
- Nom et version du système d'exploitation installé sur l'ordinateur
- Nom du réseau de l'ordinateur protégé
- Domaine ou groupe auquel appartient l'ordinateur protégé
- Nom du navigateur
- Version du navigateur
- Heure à laquelle la ressource Web a été consultée pour la dernière fois

- URL de la demande HTTP
- Nom du compte utilisé pour la demande HTTP
- Nom de fichier du processus qui a effectué la demande HTTP
- Chemin d'accès complet au fichier du processus qui a effectué la demande HTTP
- Identifiant Windows (PID) du processus qui a effectué la demande HTTP
- Référent HTTP (URL source de la demande HTTP)
- URI de la ressource demandée via HTTP
- Informations sur l'agent utilisateur HTTP (l'application qui a effectué la demande HTTP)
- Temps d'exécution de la demande HTTP
- Identifiant unique du processus qui a effectué la requête HTTP

Données permettant de créer une chaîne de développement de menaces

Les données permettant de créer une chaîne de développement de menaces sont stockées pendant sept jours par défaut. Les données sont automatiquement envoyées à Kaspersky Security Center.

Les données permettant de créer une chaîne de développement de menaces peuvent contenir les informations suivantes :

- Date et heure de l'incident
- Nom de la détection
- Mode d'analyse
- État de la dernière action liée à la détection
- Raison pour laquelle le traitement de la détection a échoué
- Type d'objet détecté
- Nom de l'objet détecté
- État de la menace après le traitement de l'objet
- Raison pour laquelle l'exécution des actions sur l'objet a échoué
- Actions effectuées pour annuler les actions malveillantes
- Informations concernant l'objet traité :
  - Identifiant unique du processus
  - Identifiant unique du processus parent

- Identifiant unique du fichier de processus
- Identifiant du processus Windows (PID)
- Ligne de commande du processus
- Compte utilisateur qui a lancé le processus
- Code de la session de connexion dans laquelle le processus s'exécute
- Type de session dans laquelle le processus s'exécute
- Niveau d'intégrité du processus en cours de traitement
- Appartenance du compte utilisateur qui a démarré le processus dans les groupes locaux et de domaine privilégiés
- Identifiant de l'objet traité
- Nom complet de l'objet traité
- Identifiant de l'appareil protégé
- Nom complet de l'objet (nom du fichier local ou adresse Web du fichier téléchargé)
- Hachage MD5 ou SHA256 de l'objet traité
- Type d'objet traité
- Date de création de l'objet traité
- Date à laquelle l'objet traité a été modifié pour la dernière fois
- Taille de l'objet traité
- Attributs de l'objet traité
- Organisation qui a signé l'objet traité
- Résultat de la vérification du certificat numérique de l'objet traité
- Identifiant de sécurité (SID) de l'objet traité
- Identifiant de fuseau horaire de l'objet traité
- Adresse Web du téléchargement de l'objet traité (uniquement pour les fichiers sur disque)
- Nom de l'application qui a téléchargé le fichier
- Hachages MD5 et SHA256 de l'application qui a téléchargé le fichier
- Nom de l'application qui a modifié le fichier pour la dernière fois
- Hachages MD5 et SHA256 de l'application qui a modifié le fichier pour la dernière fois

- Nombre de démarrages d'objets traités
- Date et heure auxquelles l'objet traité a été lancé pour la première fois
- Identifiants uniques du fichier
- Nom complet du fichier (nom du fichier local ou adresse Web du fichier téléchargé)
- Chemin d'accès à la variable de registre Windows traitée
- Nom de la variable de registre Windows traitée
- Valeur de la variable de registre Windows traitée
- Type de la variable de registre Windows traitée
- Indicateur de l'appartenance de la clé de registre traitée au point d'exécution automatique
- Adresse Web de la demande Web traitée
- Source du lien de la demande Web traitée
- Agent utilisateur de la demande Web traitée
- Type de la demande Web traitée (`GET` ou `POST`)
- Port IP local de la demande Web traitée
- Port IP distant de la demande Web traitée
- Sens de connexion (entrant ou sortant) de la demande Web traitée
- Identifiant du processus dans lequel le code malveillant a été intégré

Kaspersky Sandbox

Toutes les données que l'application stocke localement sur l'ordinateur sont supprimées de l'ordinateur lors de la désinstallation de Kaspersky Endpoint Security.

Données d'entretien

Kaspersky Endpoint Security stocke les données suivantes traitées lors de la réponse automatique :

- Fichiers traités et données saisies par l'utilisateur lors de la configuration de l'agent intégré de Kaspersky Endpoint Security :
  - Fichiers en quarantaine
  - Clé publique du certificat utilisé pour l'intégration avec Kaspersky Sandbox

- Cache de l'agent intégré de Kaspersky Endpoint Security :
  - Heure à laquelle les résultats de l'analyse ont été écrits dans le cache
  - Hachage MD5 de la tâche d'analyse
  - Identifiant de la tâche d'analyse
  - Résultat de l'analyse de l'objet
- File d'attente des demandes d'analyse d'objets :
  - Identifiant de l'objet dans la file d'attente
  - Heure à laquelle l'objet a été placé dans la file d'attente
  - État de traitement de l'objet dans la file d'attente
  - Identifiant de la session utilisateur dans le système d'exploitation où la tâche d'analyse d'objet a été créée
  - Identifiant système (SID) de l'utilisateur du système d'exploitation dont le compte a été utilisé pour créer la tâche
  - Hachage MD5 de la tâche d'analyse de l'objet
- Informations sur les tâches pour lesquelles l'agent intégré de Kaspersky Endpoint Security attend les résultats de l'analyse de Kaspersky Sandbox :
  - Heure à laquelle la tâche d'analyse d'objet a été reçue
  - État de traitement de l'objet
  - Identifiant de la session utilisateur dans le système d'exploitation où la tâche d'analyse d'objet a été créée
  - Identifiant de la tâche d'analyse de l'objet
  - Hachage MD5 de la tâche d'analyse de l'objet
  - Identifiant système (SID) de l'utilisateur du système d'exploitation dont le compte a été utilisé pour créer la tâche
  - Schéma XML de l'IOC créé automatiquement
  - Hachage MD5 ou SHA256 de l'objet analysé
  - Erreurs de traitement
  - Noms des objets pour lesquels la tâche a été créée
  - Résultat de l'analyse de l'objet

Données dans les demandes à Kaspersky Sandbox

Les données suivantes des requêtes de l'agent intégré de Kaspersky Endpoint Security à Kaspersky Sandbox sont stockées localement sur l'ordinateur :

- Hachage MD5 de la tâche d'analyse
- Identifiant de la tâche d'analyse
- Objet analysé et tous les fichiers associés

Données reçues à la suite de l'exécution de la tâche Analyse IOC (tâche autonome)

Kaspersky Endpoint Security soumet automatiquement les données sur les résultats de l'exécution de la tâche *Analyse IOC* à Kaspersky Security Center.

Les données des résultats d'exécution de la tâche *Analyse IOC* peuvent contenir les informations suivantes :

- Adresse IP de la table ARP
- Adresse physique de la table ARP
- Type et nom d'enregistrement DNS
- Adresse IP de l'ordinateur protégé
- Adresse physique (adresse MAC) de l'ordinateur protégé
- Identifiant dans l'entrée du journal des événements
- Nom de la source de données dans le journal
- Nom du journal
- Heure de l'événement
- Hachages MD5 et SHA256 du fichier
- Nom complet du fichier (y compris le chemin)
- Taille du fichier
- Adresse IP et port distants auxquels la connexion a été établie pendant l'analyse
- Adresse IP de l'adaptateur local
- Port ouvert sur l'adaptateur local
- Protocole sous forme de numéro (conformément à la norme IANA)

- Nom du processus
- Arguments du processus
- Chemin d'accès au fichier du processus
- Identifiant Windows (PID) du processus
- Identifiant Windows (PID) du processus parent
- Compte utilisateur qui a lancé le processus
- Date et heure de démarrage du processus
- Nom du service
- Description du service
- Chemin et nom du service DLL (pour svchost)
- Chemin et nom du fichier exécutable du service
- Identifiant Windows (PID) du service
- Type de service (par exemple, un pilote ou un adaptateur de noyau)
- État du service
- Mode de lancement du service
- Nom du compte utilisateur.
- Nom du volume
- Lettre du volume
- Type de volume
- Valeur du registre Windows
- Valeur de la section du registre
- Chemin d'accès à la clé de registre (sans nom de section ni de valeur)
- Paramètre de registre
- Système (environnement)
- Nom et version du système d'exploitation installé sur l'ordinateur
- Nom du réseau de l'ordinateur protégé
- Domaine ou groupe auquel appartient l'ordinateur protégé
- Nom du navigateur

- Version du navigateur
- Heure à laquelle la ressource Web a été consultée pour la dernière fois
- URL de la demande HTTP
- Nom du compte utilisé pour la demande HTTP
- Nom de fichier du processus qui a effectué la demande HTTP
- Chemin d'accès complet au fichier du processus qui a effectué la demande HTTP
- Identifiant Windows (PID) du processus qui a effectué la demande HTTP
- Référent HTTP (URL source de la demande HTTP)
- URI de la ressource demandée via HTTP
- Informations sur l'agent utilisateur HTTP (l'application qui a effectué la demande HTTP)
- Temps d'exécution de la demande HTTP
- Identifiant unique du processus qui a effectué la requête HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Toutes les données que l'application stocke localement sur l'ordinateur sont supprimées de l'ordinateur lors de la désinstallation de Kaspersky Endpoint Security.

Données d'entretien

L'agent intégré de Kaspersky Endpoint Security stocke localement les données suivantes :

- Données requises pour l'intégration au module EDR Expert (on-premises) :
  - Adresse et port pour la connexion au serveur KATA Central Node
  - Adresse et port pour la connexion au serveur de transmission de données télémétriques
  - Adresse et port pour la connexion au serveur de réponse
  - Informations sur les certificats utilisés pour l'intégration à KATA Central Node
  - Informations sur les certificats pour l'intégration au serveur de transmission de données télémétriques
  - Informations sur les certificats utilisés pour l'intégration au serveur de réponse
- Fichiers en quarantaine

Données des événements de télémétrie transmis

- **Données télémétriques**
  - Données sur les fichiers :
    - Identifiants uniques du fichier
    - Type de fichiers
    - Chemin d'accès complet
    - Taille du fichier
    - Attributs du fichier
    - Identifiant de zone
    - Date et heure de création du fichier
    - Date et heure de la dernière modification du fichier
    - Nom du fichier d'origine
    - Nom de l'application
    - Version de l'application.
    - Fournisseur de l'application
    - Description du fichier
    - Version du fichier.
    - Hachages MD5 et SHA256 de l'objet
    - Résultat de la vérification de la signature du fichier
    - Nom de l'émetteur du certificat
    - Nom du titulaire du certificat
    - Numéro de série du certificat
  - Données relatives à l'analyse AMSI :
    - Identifiant unique du processus qui a établi l'activité
    - Type de contenu de l'objet transmis à AMSI
    - Contenu de l'objet transmis à AMSI

    - Nom de l'objet
    - Hachages MD5 et SHA256 de l'objet
- Données relatives au blocage des applications :
    - Identifiant unique du processus à l'origine du blocage de l'application
    - Identifiant unique du processus parent
    - Identifiant système unique du processus
    - Commande permettant de lancer un processus
    - Identifiant de la session de connexion
    - Niveau d'intégrité du processus
    - État du processus
    - Identifiant unique du fichier de processus
    - Ligne de commande du processus
    - Liste des identifiants uniques des fichiers interprétés
- Données relatives aux ouvertures de fichiers bloquées :
    - Identifiant unique du processus à l'origine de l'ouverture du fichier
    - Identifiants uniques du fichier
- Données relatives au chargement du pilote :
    - Identifiant unique du pilote chargé
- Données relatives aux événements :
    - Identifiant unique de l'événement
    - Date et heure de l'événement
- Données relatives à la modification du fichier :
    - Identifiant unique du processus à l'origine de la modification du fichier
    - Identifiants uniques du fichier
    - Type d'opération de modification
    - Indicateur précisant que le fichier sera supprimé après le redémarrage de l'ordinateur
    - Identifiant unique du fichier modifié
    - Identifiant unique du fichier avant modification

    - Ensemble d'indicateurs qui déterminent la manière dont le fichier a été ouvert
    - Données relatives aux opérations sur la liste de contrôle d'accès
    - Données relatives aux modifications de la propriété ou du groupe parent du fichier
- Données relatives à la session de connexion :
    - Identifiant de la session de connexion
    - Nom d'utilisateur de la personne connectée
    - Type de compte utilisateur
    - Type de session
- Données relatives aux connexions réseau :
    - Identifiant unique du processus qui a établi la connexion
    - Adresse IP locale utilisée pour établir la connexion
    - Adresse IP distante du terminal de la connexion
    - Sens de connexion
    - Protocole de transfert de données
    - Méthode HTTP
    - Chemin d'accès sans nom d'hôte
    - Nom d'hôte
    - État dynamique du processus au moment de la connexion
    - Indicateur précisant que la connexion est ouverte au niveau du socket brut
    - Version TLS utilisée lors de la session de connexion
    - Nom du serveur TLS
    - Hachages MD5 et SHA1 du certificat de serveur TLS
    - Liste des noms alternatifs du sujet (SAN) du certificat
    - Nom de l'émetteur du certificat TLS
    - Numéro de série du certificat
    - Algorithme de chiffrement utilisé
    - Dates de début et de fin du certificat

    - Empreinte digitale JA3 du client TLS
    - Empreinte digitale JA3S du serveur
- Données capturées lors de l'écoute sur un port réseau :
    - Identifiant unique du processus qui a établi la connexion
- Données saisies via la ligne de commande :
    - Identifiant unique du processus à l'origine de l'entrée dans la console
    - Type d'entrée dans la console
    - Texte saisi par un utilisateur ou un processus
- Données relatives à la création du processus :
    - Identifiant unique du processus
    - Identifiant unique du processus parent
    - Identifiant système unique du processus
    - Commande permettant de lancer un processus
    - Identifiant de la session de connexion
    - Niveau d'intégrité du processus
    - Identifiant unique du fichier de processus
    - Liste des identifiants uniques des fichiers interprétés
    - Type de processus
- Données relatives au module chargé par le processus :
    - Identifiant unique du processus qui a lancé le téléchargement
    - Chemin d'accès complet au fichier qui a été chargé dans le processus
    - Identifiant unique du fichier du module
    - Nom qualifié complet de l'assembly .NET, si le fichier chargé est un module .NET
    - Indicateurs de l'assembly .NET défini dans son fichier manifeste
- Données relatives à l'arrêt du processus :
    - Identifiant unique du processus arrêté

- Données relatives à la modification du registre :
  - Identifiant unique du processus à l'origine de la modification du registre
  - Type d'opération de registre
  - Chemin d'accès complet à la clé de registre
  - Nom de la valeur au sein d'une clé de registre
  - Type de données stockées dans la valeur de la clé de registre
  - Données spécifiées dans la valeur de la clé de registre
  - Nom de la clé avant le changement de nom
  - Informations concernant un changement de propriétaire de la clé ou du groupe de clés principales
  - Liste des modifications apportées à la liste de contrôle d'accès (ACL) de la clé
- Données relatives à la menace détectée et à son traitement :
  - Indicateur signalant que la détection des menaces s'est exécutée en arrière-plan
  - Verdict de menace
  - Nom du verdict
  - Identifiant unique de l'enregistrement de la base de données
  - Heure d'enregistrement de la menace dans la base de données
  - Mode de traitement des menaces
  - Type d'objet infecté
  - Nom de l'objet infecté
  - Hachages MD5 et SHA256 de l'objet
  - Identifiant unique de l'objet infecté
  - Identifiant unique du processus qui a téléchargé l'objet infecté depuis Internet
  - URL à partir de laquelle l'objet infecté a été téléchargé
  - Adresse d'email de l'expéditeur qui a envoyé l'objet infecté
  - Protocole réseau par lequel provient l'objet infecté
  - Adresse locale d'où provient l'objet infecté
  - Adresse externe d'où provient l'objet infecté

    - Type de contenu de l'objet
    - Contenu de l'objet
- Données relatives à l'accès aux processus :
    - Identifiant unique du processus qui a tenté l'accès
    - Identifiant unique du processus cible auquel on a accédé
    - Ensemble de privilèges demandé au processus cible
    - Type d'opération
    - Ensemble des appels au moment de l'accès au processus
    - Descripteur du processus source
    - Descripteur du processus cible
- Données relatives au DNS :
    - Identifiant unique du processus qui a effectué la requête DNS
    - Adresse IP du serveur DNS
    - Indicateurs permettant de contrôler le comportement d'une requête DNS
    - Vérifier l'état d'avancement de la demande
    - Nom de domaine complet spécifié dans la requête DNS
    - Type de données dans la requête DNS
    - Réponses du serveur DNS
- Données relatives à l'injection de code :
    - Identifiant unique du processus qui a tenté d'injecter du code
    - Mode d'accès utilisé
    - Ensemble des appels au moment où le code injecté a été détecté
    - Identifiant unique du processus cible vers lequel le code a été chargé
    - Données relatives aux modifications de la séquence de commandes du processus cible
    - Adresse du processus cible
    - Nom de la bibliothèque DLL qui a été chargée dans le processus cible
    - Chemin d'accès complet au fichier DDL

- Données relatives aux opérations avec des canaux nommés :
  - Identifiant unique du processus qui a créé le canal ou s'y est connecté
  - Nom complet du canal nommé
  - Type d'opération (création ou connexion)
- Données relatives aux requêtes WMI :
  - Identifiant unique du processus qui a lancé l'opération WMI
  - Type d'opération WMI
  - Nom de l'appareil cible pour la requête WMI
  - Compte utilisateur à l'origine de la requête WMI
  - Texte de la requête WMI
  - Espace de noms dans lequel la requête WMI est exécutée
  - Nom du filtre WMI
  - Nom de l'objet de consommation
  - Texte décrivant le fonctionnement de l'objet consommateur
- Données relatives aux requêtes LDAP :
  - Identifiant unique du processus qui a effectué la requête LDAP
  - Zone de recherche des requêtes LDAP
  - Filtre LDAP
  - Paramètre qui définit la partition Active Directory vers laquelle la requête a été dirigée
  - Attributs de recherche LDAP
- Données relatives aux appareils USB connectés :
  - Type de fonctionnement des appareils USB
  - Type d'appareil USB
  - Identifiant de l'appareil USB
  - Nom de l'appareil USB
  - Chemin d'accès à l'appareil USB
  - Indicateur précisant que l'appareil USB est un disque système
- Données relatives à la création, à la suppression et à la modification d'une tâche planifiée

    - Données relatives à la création, à la suppression et à la modification des services
    - Données relatives au montage et au démontage du système de fichiers
    - Données relatives au fonctionnement du module EDR Expert (on-premise) :
        - Informations sur le lancement et l'arrêt de l'agent
        - Informations sur l'installation et la désinstallation de l'agent
        - Identifiant unique pour le démarrage de l'agent
        - Identifiant système du processus de l'agent
        - Identifiant unique du processus de l'agent
        - Raison de la suspension de l'agent
        - Code de suspension du processus de l'agent
- Paramètres de filtrage des événements :
    - Noms des modules
    - Remplir les chemins d'accès aux objets
    - Hachages MD5 et SHA256 des objets
    - Identifiants des entrées du journal des événements Windows
    - Paramètres du certificat numérique
    - Sens du trafic, adresses IP, ports, protocoles, chemins complets vers les fichiers exécutables
    - Noms d'utilisateur
    - Types de connexion utilisateur
    - Types d'événements de télémétrie pour lesquels des filtres sont appliqués

Données des demandes du module EDR Expert à l'agent intégré de Kaspersky Endpoint Security :

- Paramètres de tâche généraux :
    - Type de tâche
    - Paramètres de planification de la tâche
    - Noms et mots de passe des comptes sous lesquels les tâches peuvent être exécutées
    - Versions des paramètres

    - Identifiants des objets mis en quarantaine
    - Chemins d'accès aux objets
    - Hachages MD5 et SHA256 des objets
    - Ligne de commande pour démarrer le processus avec les arguments
    - Indicateurs des actions supplémentaires effectuées à la fin des tâches
    - Identifiants des fichiers IOC à récupérer sur le serveur
    - Fichiers IOC
    - Nom du service
    - Type de démarrage du service
    - Dossiers pour lesquels les résultats de la tâche *Obtenir le cyberdiagnostic* doivent être reçus
    - Masques des noms d'objets et des extensions pour la tâche *Obtenir le cyberdiagnostic*
- Paramètres d'isolation du réseau :
    - Types de paramètres
    - Versions des paramètres
    - Listes des exclusions d'isolation du réseau et des paramètres d'exclusion : sens du trafic, adresses IP, ports, protocoles et chemins d'accès complets aux fichiers exécutables
    - Indicateurs des actions supplémentaires
    - Temps de désactivation de l'isolation automatique
- Paramètres de prévention d'exécution :
    - Types de paramètres
    - Versions des paramètres
    - Listes des règles de prévention d'exécution et paramètres des règles : chemins d'accès aux objets, types d'objets, et hachages MD5 et SHA256 des objets
    - Indicateurs des actions supplémentaires

Données des requêtes adressées par Kaspersky Endpoint Security au module EDR Expert

Lors de l'intégration avec la solution EDR Expert (on-premises), les données suivantes sont stockées localement sur les ordinateurs.

- Dans les demandes de synchronisation :
  - Identifiant unique
  - Partie de base de l'adresse Web du serveur
  - Nom de l'ordinateur
  - Adresse IP de l'ordinateur
  - Adresse MAC de l'ordinateur
  - Heure locale sur l'ordinateur
  - État d'autodéfense de Kaspersky Endpoint Security
  - Nom et version du système d'exploitation installé sur l'ordinateur
  - Version de Kaspersky Endpoint Security
  - Versions des paramètres d'application et des paramètres de tâche
  - États des tâches : identifiants des tâches, états d'exécution, codes d'erreur
- Dans les demandes d'obtention de fichiers depuis le serveur :
  - Identifiants uniques des fichiers
  - Identifiant unique de Kaspersky Endpoint Security
  - Identifiants uniques des certificats
  - Partie de base de l'adresse Web du serveur sur lequel le module Central Node est installé
  - Adresse IP de l'hôte
- Dans les rapports sur les résultats d'exécution des tâches :
  - Adresse IP de l'hôte
  - Informations sur les objets détectés lors d'une analyse IOC ou d'une analyse YARA
  - Indicateurs des actions supplémentaires effectuées à la fin des tâches
  - Erreurs d'exécution de tâche et codes de retour
  - États d'achèvement des tâches

    - Temps d'exécution de la tâche
    - Versions des paramètres utilisés pour l'exécution des tâches
    - Informations sur les objets envoyés au serveur, les objets mis en quarantaine et les objets restaurés depuis la quarantaine : chemins d'accès aux objets, hachages MD5 et SHA256, et identifiants des objets mis en quarantaine
    - Informations sur les processus démarrés ou arrêtés sur un ordinateur à la demande du serveur : PID et UniquePID, code d'erreur, et hachages MD5 et SHA256 des objets
    - Informations sur les services démarrés ou arrêtés sur l'ordinateur à la demande du serveur : nom du service, type de démarrage, code d'erreur, et hachages MD5 et SHA256 des images de fichiers des services
    - Informations sur les objets pour lesquels un vidage mémoire a été effectué dans le cadre d'une analyse YARA (chemins d'accès, identifiant du fichier de vidage)
    - Fichiers demandés par le serveur
- Données sur les processus en cours :
    - Nom du fichier exécutable, y compris le chemin complet et l'extension
    - Paramètres d'exécution automatique du processus
    - Identifiant du processus
    - Identifiant de la session de connexion
    - Nom de la session de connexion
    - Date et heure de démarrage du processus
    - Hachages MD5 et SHA256 de l'objet
- Données sur les fichiers :
    - Chemin du fichier
    - Nom du fichier.
    - Taille du fichier
    - Attributs du fichier
    - Date et heure de création du fichier
    - Date et heure de la dernière modification du fichier
    - Description du fichier
    - Nom de l'entreprise

- Hachages MD5 et SHA256 de l'objet
- Clé de registre (pour les points d'exécution automatique)

- Données dans les erreurs qui se produisent lors de la récupération des informations sur les objets :
  - Nom complet de l'objet qui a été traité lorsqu'une erreur s'est produite
  - Code d'erreur
- Données dans les résultats de l'analyse YARA :

  L'agent intégré de Kaspersky Endpoint Security transfère automatiquement les résultats de l'analyse YARA à Kaspersky Anti Targeted Attack Platform pour créer une chaîne de développement de menaces.

  Les données sont temporairement stockées localement dans la file d'attente pour l'envoi des résultats d'exécution de la tâche au serveur Kaspersky Anti Targeted Attack Platform. Les données sont supprimées du stockage temporaire une fois qu'elles ont été envoyées.

  - Hachages MD5 et SHA256 du fichier
  - Nom complet du fichier
  - Chemin du fichier
  - Taille du fichier
  - Nom du processus
  - Arguments du processus
  - Chemin d'accès au fichier du processus
  - Identifiant Windows (PID) du processus
  - Identifiant Windows (PID) du processus parent
  - Compte utilisateur qui a lancé le processus
  - Date et heure de démarrage du processus
- Données dans les résultats de l'analyse IOC :
  - Adresse IP de la table ARP
  - Adresse physique de la table ARP
  - Nom d'enregistrement DNS
  - Type d'enregistrement DNS
  - Nom d'hôte
  - Adresse IP
  - Identifiant de l'événement dans le journal

- Nom de la source de données dans le journal
- Nom du journal
- Nom d'utilisateur
- Date et heure de génération de l'événement au format ISO
- Hachages MD5 et SHA256 du fichier
- Nom complet du fichier
- Taille du fichier
- Adresse IP et port distants auxquels la connexion a été établie pendant l'analyse
- Adresse IP et port de l'adaptateur local
- Protocole
- Nom du processus
- Arguments du processus
- Chemin d'accès au fichier du processus
- Identifiant Windows (PID) du processus
- Identifiant Windows (PID) du processus parent
- Compte utilisateur qui a lancé le processus
- Date et heure de démarrage du processus
- Chemin d'accès à la clé de registre
- Nom de la clé de registre
- Valeur texte de la clé de registre
- Nom du service
- Description du service
- Chemin et nom du service DLL
- Chemin et nom du fichier exécutable du service
- Identifiant Windows (PID) du service
- Type de service
- État du service
- Mode de lancement du service

- Nom du système d'exploitation
- Version du système d'exploitation
- Nom du réseau informatique sans domaine
- Domaine ou groupe de travail
- Nom d'utilisateur
- Nom du volume
- Lettre du volume
- Type de volume

Kaspersky Network Detection and Response (KATA)

Toutes les données que l'application stocke localement sur l'ordinateur sont supprimées de l'ordinateur lors de la désinstallation de Kaspersky Endpoint Security.

Données télémétriques

- **Données relatives aux fichiers**
  - Identifiants uniques du fichier
  - Type de fichiers
  - Chemin d'accès complet
  - Taille du fichier
  - Attributs du fichier
  - Identifiant de zone
  - Date et heure de création du fichier
  - Date et heure de la dernière modification du fichier
  - Nom du fichier d'origine
  - Nom de l'application
  - Version de l'application.
  - Fournisseur de l'application

    - Description du fichier
    - Version du fichier.
    - Hachages MD5 et SHA256 de l'objet
    - Résultat de la vérification de la signature du fichier
    - Date et heure de création de la signature du fichier
    - Chaînes de certificats utilisées dans le fichier de signature
    - Type de chaîne de certificats
    - Certificats dans la chaîne
    - Nom de l'émetteur du certificat
    - Nom du titulaire du certificat
    - Numéro de série du certificat
    - Algorithme de l'empreinte du certificat
    - Empreinte du certificat
    - Durée de validité du certificat
- **Données relatives à la session de connexion**
    - Identifiant de la session de connexion
    - Nom du compte de l'utilisateur connecté
    - Type de compte utilisateur
    - Type de session
    - Adresse IP de l'ordinateur à partir duquel la tentative de connexion a été effectuée
    - Adresse IP de l'ordinateur local à partir duquel la tentative de connexion a été effectuée
    - Indicateur signalant que la session associée à cet événement dispose de privilèges élevés et d'autorisations d'administrateur
    - Paramètre indiquant si d'autres sessions sont associées à cette session de connexion
    - Protocole utilisé pour la session du terminal
    - Protocole IPv4 utilisé pour la session du terminal

- **Données relatives à la communication réseau**
  - Début et fin de la période pendant laquelle les données ont été collectées
  - Liste des connexions
  - Adresse IP locale de l'ordinateur
  - Adresse MAC locale de l'ordinateur
  - Adresse IP distante de l'ordinateur
  - Adresse MAC distante de l'ordinateur
  - Adresse IP de la passerelle
  - Nombre de paquets de données transmis
  - Nombre de paquets de données reçus
  - Nombre total d'octets transférés
  - Protocole de transfert de données
  - Champ EtherType de trame Ethernet
  - Préfixe de la charge utile du premier paquet de l'intervalle
  - Adresse IPv4 de l'interface réseau par laquelle la communication a été capturée
- **Données relatives à la connexion réseau**
  - Identifiant unique du processus qui a établi la connexion
  - Protocole de transfert de données
  - Adresse IP locale utilisée pour établir la connexion
  - Adresse IP distante du terminal de la connexion
  - Méthode HTTP
  - Chemin d'accès sans nom d'hôte
  - Nom d'hôte
  - État dynamique du processus au moment de la connexion
  - Sens de connexion
  - État dynamique du processus
  - Champ EtherType de trame Ethernet

- **Données capturées lors de l'écoute sur un port réseau**
  - Identifiant unique du processus qui a établi la connexion
  - Protocole de transfert de données
  - Adresse locale
  - État dynamique du processus au moment de la connexion
- **Résultat de la vérification de la connexion**
  - Paramètres réseau de l'hôte
  - Description de l'interface réseau
  - Nom de domaine DNS
  - Adresse MAC locale de l'ordinateur
  - Numéro de mesure de la connexion IP
  - Liste des adresses IP
  - Adresse IP
  - Masque de réseau
  - Adresse IP de la passerelle
  - Adresse MAC de la passerelle
  - Liste des correctifs installés
  - Numéro de correctif
  - Date d'installation du correctif
  - Modèle d'appareil
  - Fournisseur de l'appareil
  - ID de l'hôte dans Kaspersky Security Center
  - Description de l'antivirus Kaspersky installé
  - Nom du module antivirus Kaspersky installé
  - Version du module antivirus Kaspersky installé
  - Version de la base de données du module antivirus Kaspersky installé
  - Date de la dernière mise à jour de la base de données du module antivirus Kaspersky installé
  - État du module antivirus Kaspersky installé

    - Liste des clés de licence
    - Numéro de série
    - Type de clé
    - Date d'expiration de la clé
    - État de la clé
- **Données relatives à la création de processus sur l'hôte**
    - Identifiant unique du processus
    - Identifiant unique du processus parent
    - Identifiant système unique du processus
    - Commande permettant de lancer un processus
    - Identifiant de la session de connexion
    - Identifiant de la session du terminal
    - Identifiant unique du fichier de processus
    - Niveau d'intégrité du processus
    - Liste des jetons des droits du processus
    - Droits d'attribut
    - Liste des identifiants uniques des fichiers interprétés
    - État du processus
    - Commande permettant de lancer un processus
- **Données relatives à l'arrêt du processus**
    - Identifiant unique du processus
- **Données relatives à la menace détectée**
    - Informations sur les menaces
    - Verdict de menace
    - Numéro d'enregistrement AMR
    - Version de la base de données antivirus
    - Mode de détection des menaces
    - Identifiant unique de la menace

- Technologie de protection
- Informations sur l'objet infecté
- Type d'objet infecté
- Nom de l'objet infecté
- Hachages MD5 et SHA256 de l'objet
- Identifiant unique du processus infecté
- Identifiant unique de l'objet infecté
- Identifiant unique du processus qui a téléchargé l'objet infecté depuis Internet
- URL à partir de laquelle l'objet infecté a été téléchargé
- Adresse d'email de l'expéditeur qui a envoyé l'objet infecté
- Protocole réseau par lequel provient l'objet infecté
- Adresse locale d'où provient l'objet infecté
- Adresse externe d'où provient l'objet infecté
- Type de contenu de l'objet
- Contexte de la menace détectée
- Contenu de l'objet
- Indicateur signalant que la détection des menaces s'est exécutée en arrière-plan

- **Données relatives au traitement des menaces**
  - Informations sur les menaces
  - Verdict de menace
  - Numéro d'enregistrement AMR
  - Version de la base de données antivirus
  - Mode de détection des menaces
  - Nom de l'objet infecté
  - Hachages MD5 et SHA256 de l'objet
  - Identifiant unique du processus infecté
  - Identifiant unique de l'objet infecté
  - Protocole réseau par lequel provient l'objet infecté

- Adresse locale d'où provient l'objet infecté
- Adresse externe d'où provient l'objet infecté
- État du traitement des menaces
- Raison pour laquelle la menace n'a pas pu être éliminée
- Adresse physique locale

- **Données relatives aux utilisateurs**
  - SID de l'utilisateur
  - ID de l'utilisateur
  - Nom d'utilisateur
  - Nom complet de l'utilisateur
  - Description de l'utilisateur
  - Si le compte est actif ou bloqué
  - Si le mot de passe a expiré
  - Si une modification du mot de passe est nécessaire
  - Si la modification du mot de passe est autorisée
  - Type de compte utilisateur
  - Si la connexion automatique est activée pour ce compte
  - Liste des groupes dont l'utilisateur fait partie

Intégration à Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Toutes les données que l'application stocke localement sur l'ordinateur sont supprimées de l'ordinateur lors de la désinstallation de Kaspersky Endpoint Security.

Lors de l'intégration avec la plateforme Kaspersky Unified Monitoring and Analysis Platform (KUMA), les données relatives aux paramètres de connexion sont transférées, ainsi que tous les événements enregistrés dans les journaux Windows.

Voici les principaux journaux des événements Windows : System, Security, Application, ForwardedEvents et HardwareEvents. Les utilisateurs peuvent également créer et utiliser des journaux personnalisés afin de répondre à leurs besoins.

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.

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 Kaspersky Private Security Network (KPSN) ou désactivez l'utilisation de KSN. Pour en savoir plus sur le fonctionnement du KPSN, 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.

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 enregistrées aux États-Unis et/ou dans d'autres pays.

Amazon, Amazon Web Services et AWS sont des marques de commerce d'Amazon.com, Inc. ou de ses sociétés affiliées.

Apple, FireWire, iTunes, Mac et Safari sont des marques de commerce d'Apple Inc.

Arm est une marque déposée d'Arm Limited (ou de ses filiales) aux États-Unis et/ou 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.

Cisco, Cisco AnyConnect et IOS sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans certains autres pays.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop et XenServer sont des marques déposées ou des marques de commerce de Cloud Software Group, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays.

Cloudflare, Cloudflare Workers et le logo Cloudflare sont des marques de commerce et/ou des marques déposées de Cloudflare, Inc. aux États-Unis et dans d'autres juridictions.

Core est une marque commerciale d'Intel Corporation ou de ses filiales.

dBase est une marque de dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC et les autres marques sont des marques commerciales de Dell Inc. ou de ses filiales.

Docker et le logo Docker sont des marques de commerce ou des marques déposées de Docker, Inc. aux États-Unis et/ou dans d'autres pays. Docker, Inc. et d'autres parties peuvent également avoir des droits de marque de commerce dans d'autres termes utilisés dans le présent document.

ESET est une marque de commerce ou une marque déposée d'ESET spol. s.r.o. ou l'entité ESET respective.

Foxit est une marque déposée de Foxit Corporation.

Radmin est une marque déposée de Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome sont des marques de commerce de Google LLC.

HUAWEI, FusionCompute et FusionSphere sont des marques commerciales de Huawei Technologies Co., Ltd.

ICQ est une marque déposée et/ou une marque de service d'ICQ LLC.

Intel est une marque commerciale d'Intel Corporation ou de ses filiales.

IBM est une marque d'International Business Machines Corporation déposées dans plusieurs juridictions à travers le monde.

Lenovo et Lenovo 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 de commerce de Mail.ru, LLC.

McAfee est une marque ou une marque déposée de McAfee LLC ou de ses filiales aux États-Unis et/ou dans d'autres pays.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server et Windows Store sont des marques de commerce du groupe Microsoft.

Mozilla, Firefox et Thunderbird sont des marques commerciales de la Fondation Mozilla aux États-Unis et dans d'autres pays.

NetApp est la marque de commerce ou la marque déposée de NetApp, Inc. aux États-Unis et/ou dans d'autres pays.

OpenSSL est une marque déposée appartenant à OpenSSL Software Foundation.

OpenStack est une marque déposée de la OpenStack Foundation aux États-Unis et dans d'autres pays.

Oracle, Java et JavaScript sont des marques déposées de la société Oracle et/ou de ses filiales.

Python est une marque de commerce ou une marque déposée de la Python Software Foundation.

Realtek est une marque de commerce de Realtek Semiconductor Corporation.

SAMSUNG est une marque de commerce de SAMSUNG aux États-Unis ou dans d'autres pays.

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.

Trend Micro est une marque de commerce ou une marque déposée de Trend Micro Incorporated.

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, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools et VMware vSphere sont des marques de commerce et/ou des marques déposées de VMware, Inc. aux États-Unis et dans d'autres pays.

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le fichier d'installation de l'application.