kaspersky

Kaspersky Endpoint Security for Linux

© 2026 AO Kaspersky Lab

Contenu

Aide de Kaspersky Endpoint Security 12.4 for Linux

À propos de Kaspersky Endpoint Security 12.4 for Linux

- À propos des modes d'utilisation de l'application Kaspersky Endpoint Security
  - Utilisation de l'application en mode Light Agent
  - Utilisation de l'application en mode Endpoint Detection and Response Agent
- Distribution
- Configurations logicielles et matérielles
  - Exigences matérielles
  - Configuration logicielle
  - Configuration logicielle supplémentaire requise pour le mode Light Agent
  - Versions prises en charge de Kaspersky Security Center
  - Versions des solutions prises en charge sur les plate-formes KATA et OSMP

Nouveautés

Problèmes résolus

Préparation à l'installation de l'application Kaspersky Endpoint Security

Installation et configuration initiale de l'application Kaspersky Endpoint Security

- Installation et configuration initiale de l'Agent d'administration de Kaspersky Security Center
- Installation des plug-ins d'administration de Kaspersky Endpoint Security
  - Installation du plug-in Internet de Kaspersky Endpoint Security
  - Installation du plug-in MMC de Kaspersky Endpoint Security
- Installation et configuration initiale de l'application à l'aide de Kaspersky Security Center
  - Création d'un paquet d'installation dans Web Console
  - Paramètres de configuration initiale dans Web Console
  - Création d'un paquet d'installation dans la Console d'administration
  - Paramètres de configuration initiale dans la Console d'administration
  - Préparation d'une archive avec des bases de données de l'application pour créer un paquet d'installation avec des bases de données intégrées
  - Paramètres du fichier de configuration autoinstall.ini
  - Préparation de l'application pour une utilisation via Kaspersky Security Center
- Installation et configuration initiale de l'application à l'aide de la ligne de commande
  - Installation de l'application à l'aide d'une ligne de commande
  - Configuration initiale de l'application en mode interactif
    - Sélectionnez le mode d'utilisation : standard ou Light Agent
    - Déterminer le rôle de la machine virtuelle
    - Activer le mode de protection de l'infrastructure VDI
    - Sélectionnez le mode d'utilisation : standard ou Endpoint Detection and Response Agent
    - Sélection des paramètres régionaux du service
    - Consultation du Contrat de licence utilisateur final et de la Politique de confidentialité
    - Acceptation du Contrat de licence utilisateur final
    - Acceptation de la Politique de confidentialité
    - Utilisation de Kaspersky Security Network
    - Suppression des utilisateurs de groupes privilégiés
    - Attribution du rôle d'administrateur à l'utilisateur

Configuration du mécanisme d'interception des événements système
Activation de la configuration automatique de SELinux
Configuration de la source des mises à jour
Configuration du serveur proxy
Démarrage d'une mise à jour de la base de données d'une application
Activation de la mise à jour automatique des bases de l'application
Activation de l'application
Configuration initiale de l'application en mode automatique
Paramètres du fichier de configuration de la configuration initiale de l'application
Configuration des règles d'autorisation dans le système SELinux
Lancement de l'application sous Astra Linux en mode environnement logiciel fermé
Lancement de l'application sous ALT SP en mode environnement logiciel fermé
Configuration du système d'exploitation OSnova pour que l'application fonctionne
Optimisation de l'utilisation des ressources par l'application
Recommandations pour les rôles de serveur typiques
Analyse du fonctionnement de l'application sur l'appareil
Analyse de la consommation de ressources par la tâche Protection contre les fichiers malicieux
Identifier les objets les plus fréquemment vérifiés
Recommandations pour la Protection contre les fichiers malicieux et les tâches d'analyse
Configuration des exclusions de l'analyse
Configuration des exclusions à partir de l'interception des opérations de fichiers
Spécification de la restriction d'utilisation de la mémoire par application
Recommandations pour la Protection contre les menaces Internet et la Protection contre les menaces réseau
Mise à jour d'une ancienne version de l'application
À propos de la mise à jour des plug-ins de gestion de Kaspersky Endpoint Security
Mise à jour de l'application via Kaspersky Security Center
Mise à jour de l'application via la ligne de commande
Particularités de définition des valeurs des paramètres lors de la mise à jour de l'application
Suppression d'une application
À propos de la désinstallation d'une application et de l'Agent d'administration à l'aide de Kaspersky Security Center
Suppression de l'application via la ligne de commande
Suppression de l'Agent d'administration à l'aide de la ligne de commande
Suppression des plug-ins d'administration de Kaspersky Endpoint Security
Licence de l'application
À propos du Contrat de licence
À propos de la licence
À propos du certificat de licence
À propos de la clé de licence
À propos du code d'activation
À propos du fichier clé
À propos de l'abonnement
Comparaison des fonctions de l'application selon la licence
Activation des applications et gestion des clés de licence
Activation de l'application via Kaspersky Security Center
Gestion des clés de licence en ligne de commande

Afficher les informations sur les clés de licence utilisées
Afficher les informations sur les clés d'un appareil via Web Console
Afficher les informations sur les clés de l'appareil via la Console d'administration
Afficher les informations sur la licence et la clé dans la ligne de commande
À propos des données
Données fournies lors de l'utilisation d'un code d'activation
Données fournies lors du téléchargement des mises à jour depuis les serveurs de mise à jour de Kaspersky
Données transférées lors de l'utilisation de l'application en mode Light Agent
Données transmises à l'application Kaspersky Security Center
Données fournies lorsque vous cliquez sur des liens depuis l'interface de l'application
Données fournies lors de l'utilisation de Kaspersky Security Network
Données fournies lors de l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum
Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response (KATA)
Données fournies lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)
Données fournies lors de l'intégration avec Kaspersky Network Detection and Response (KATA)
Données fournies lors de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform
Concept d'administration de l'application
Administration de l'application via Kaspersky Security Center
À propos des plug-ins d'administration de Kaspersky Endpoint Security
À propos des politiques de Kaspersky Security Center
À propos des tâches de Kaspersky Endpoint Security créées dans Kaspersky Security Center
Connexion et déconnexion de Web Console et de Cloud Console
Administration des stratégies dans Web Console
Création d'une stratégie dans Web Console
Modification des paramètres de stratégie dans Web Console
Paramètres d'une stratégie dans Web Console
Gestion des stratégies dans la Console d'administration
Création de la stratégie à l'aide de Console d'administration
Modification des paramètres de stratégie dans la Console d'administration de Kaspersky Security Center
Paramètres d'une stratégie dans la Console d'administration
Gestion des tâches dans Web Console
Création des tâches dans Web Console
Modification des paramètres de tâche dans Web Console
Démarrer, arrêter, suspendre et reprendre des tâches dans Web Console
Gestion des tâches dans la Console d'administration
Création des tâches dans la Console d'administration
Modification des paramètres de tâche dans la Console d'administration
Démarrer, arrêter, suspendre et reprendre des tâches dans la Console d'administration
Administrer l'application via la ligne de commande
Activation de l'achèvement automatique de la commande kesl-control (complétion bash)
Gestion des tâches sur la ligne de commande
Afficher une liste de tâches dans la ligne de commande
Consultation de l'état de la tâche sur la ligne de commande
Création d'une tâche dans la ligne de commande
Démarrer, arrêter, mettre en pause et reprendre une tâche à partir de la ligne de commande
Suppression de la tâche dans la ligne de commande
Affichage des paramètres de la tâche dans la ligne de commande

Modification des paramètres de la tâche dans la ligne de commande
Modification des paramètres de la tâche via le fichier de configuration
Modification des paramètres de la tâche à l'aide des clés de la ligne de commande
Restauration des paramètres de tâche par défaut dans la ligne de commande
Planification de la tâche dans la ligne de commande
Gestion des paramètres généraux de l'application via la ligne de commande
Affichage des paramètres généraux de l'application
Modification des paramètres généraux de l'application
Utilisation du filtre pour limiter les résultats des requêtes
Exportation et importation des paramètres de l'application
Gestion des rôles d'utilisateur à l'aide de la ligne de commande
Affichage d'une liste d'utilisateurs et de rôles
Attribution d'un rôle à un utilisateur
Révocation d'un rôle d'un utilisateur
Lancement et arrêt de l'application
Démarrage et arrêt d'une application à l'aide de Web Console
Démarrage et arrêt d'une application à l'aide de la Console d'administration
Démarrer et arrêter une application à l'aide de la ligne de commande
Afficher l'état de la protection de l'appareil et les informations sur les performances de l'application
Afficher l'état de protection de l'appareil dans Web Console
Affichage de l'état de protection de l'appareil dans la Console d'administration
Affichage des informations sur l'application dans Web Console
Affichage des informations sur le fonctionnement de l'application dans la Console d'administration
Afficher des informations sur le fonctionnement d'une application dans la ligne de commande
Affichage des statistiques du fonctionnement de l'application
Afficher les statistiques sur le fonctionnement de l'application dans Web Console
Afficher les statistiques sur le fonctionnement de l'application dans la Console d'administration
Affichage de la liste de points de montage dans Web Console
Affichage de la liste des points de montage dans la Console d'administration
Affichage des statistiques du fonctionnement de l'application et de la liste des points de montage dans la ligne de commande
Collecte de métriques d'état du système
Mise à jour des bases et des modules de l'application
À propos de la mise à jour des bases de données et des modules
À propos des sources et des schémas de mise à jour
Mise à jour des bases de données et des modules de l'application dans Web Console
Mise à jour des bases de données et des modules de l'application dans la Console d'administration
Mise à jour des bases de données et des modules de l'application dans la ligne de commande
Mise à jour à l'aide de Kaspersky Update Utility
Annulation de la mise à jour des bases et des modules de l'application
Protection contre les fichiers malicieux
Configuration de la protection contre les menaces de fichiers dans Web Console
Configuration de la protection contre les fichiers malicieux dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre <Nouvelle zone d'analyse>
Fenêtre Paramètres d'analyse
Fenêtre Actions en cas de détection d'une menace

Exclusions de la Protection contre les fichiers malicieux
Fenêtre Zones d'exclusion
Fenêtre <Nouvelle zone d'exclusion>
Fenêtre Exclusions d'après le masque
Fenêtre Exclusions d'après le nom de la menace
Fenêtre Exclusions par processus
Fenêtre Processus de confiance
Configuration de la Protection contre les fichiers malicieux via la ligne de commande
Paramètres de la tâche de protection contre les fichiers malicieux
Optimisation de la vérification des répertoires réseau
Particularités de l'analyse des liens symboliques et matériels
Analyse des logiciels malveillants
Analyse des logiciels malveillants dans Web Console
Fenêtre d'ajout d'une zone d'analyse
Section Zones d'analyse
Fenêtre Zones d'analyse
Section Zones d'exclusion
Fenêtre Zones d'exclusion
Fenêtre d'ajout d'une zone d'exclusion
Fenêtre Exclusions d'après le masque
Fenêtre Exclusions d'après le nom de la menace
Analyse des logiciels malveillants dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre <Nouvelle zone d'analyse>
Fenêtre Paramètres de la zone d'analyse
Fenêtre Zones d'analyse
Fenêtre Paramètres d'analyse
Fenêtre Actions en cas de détection d'une menace
Section Exclusions
Fenêtre Zones d'exclusion
Fenêtre Nouvelle zone d'exclusion
Fenêtre Exclusions d'après le masque
Fenêtre Exclusions d'après le nom de la menace
Analyse des logiciels malveillants dans la ligne de commande
Paramètres de la tâche prédéfinie Analyse des logiciels malveillants
Analyse personnalisée des fichiers et des répertoires dans la ligne de commande
Analyse des zones critiques
Analyse des zones critiques dans Web Console
Fenêtre d'ajout d'une zone d'analyse
Section Zones d'analyse
Fenêtre Zones d'analyse
Section Zones d'exclusion
Fenêtre Zones d'exclusion
Fenêtre d'ajout d'une zone d'exclusion
Fenêtre Exclusions d'après le masque
Fenêtre Exclusions d'après le nom de la menace

- Analyse des zones critiques dans la Console d'administration
  - Fenêtre Zones d'analyse
  - Fenêtre Nouvelle zone d'analyse
  - Fenêtre Paramètres de la zone d'analyse
  - Fenêtre Zones d'analyse
  - Fenêtre Paramètres d'analyse
  - Fenêtre Actions en cas de détection d'une menace
  - Section Exclusions
  - Fenêtre Zones d'exclusion
  - Fenêtre Nouvelle zone d'exclusion
  - Fenêtre Exclusions d'après le masque
  - Fenêtre Exclusions d'après le nom de la menace
- Analyse des zones critiques via la ligne de commande

Analyse des disques amovibles
- Configuration de l'analyse des disques amovibles dans Web Console
- Configuration de l'analyse des disques amovibles dans la Console d'administration
- Configuration de l'Analyse des disques amovibles sur la ligne de commande

Analyser les conteneurs.
- Surveillance des conteneurs
  - Configuration de la surveillance des conteneurs dans Web Console
  - Configuration de la surveillance des conteneurs dans la Console d'administration
    - Fenêtre Paramètres d'analyse de conteneur
  - Configurer la surveillance des conteneurs dans la ligne de commande
- Analyse à la demande du conteneur et des images
  - Analyse du conteneur dans Web Console
    - Section Zones d'exclusion
    - Fenêtre Exclusions d'après le masque
    - Fenêtre Exclusions d'après le nom de la menace
  - Analyse du conteneur dans la Console d'administration
    - Fenêtre Paramètres d'analyse de conteneur
    - Fenêtre Paramètres d'analyse
    - Fenêtre Actions en cas de détection d'une menace
    - Section Exclusions
    - Fenêtre Exclusions d'après le masque
    - Fenêtre Exclusions d'après le nom de la menace
  - Analyse du conteneur sur la ligne de commande
    - Paramètres de la tâche Analyse du conteneur
    - Analyse personnalisée du conteneur et des images
    - Intégration à Jenkins

Gestion du pare-feu
- À propos des règles de paquet réseau
- À propos des règles dynamiques
- À propos des réseaux préconfigurés disponibles
- Gestion du pare-feu dans Web Console
- Gestion du pare-feu dans la Console d'administration
  - Fenêtre Règles de paquet réseau
  - Fenêtre Ajout d'une règle de paquet réseau

Fenêtre Ajout d'adresses IP
Fenêtre Réseaux disponibles
Fenêtre Connexion réseau
Gestion du pare-feu dans la ligne de commande
Configuration d'une liste de règles pour les paquets réseau sur la ligne de commande
Configuration des zones réseau sur la ligne de commande
Protection contre les menaces Internet
Configuration de la protection contre les menaces internet dans Web Console
Configuration de la protection contre les menaces internet dans la Console d'administration
Fenêtre Adresses Internet de confiance
Fenêtre Paramètres d'analyse
Configuration de la Protection contre les menaces Internet sur la ligne de commande
Analyse du trafic réseau
À propos des modes d'interception du trafic réseau
Configuration de l'analyse du trafic réseau dans Web Console
Configuration de l'analyse du trafic réseau dans la Console d'administration
Fenêtre Domaines de confiance
Fenêtre Certificats de confiance
Fenêtre Exclusions de l'interception du trafic
Fenêtre Exclusion de l'interception du trafic
Fenêtre Ports contrôlés
Configuration de l'analyse du trafic réseau dans la ligne de commande
Affichage et modification des paramètres de vérification du trafic réseau
Affichage des exclusions liées à l'analyse des connexions chiffrées
Gestion de la liste des certificats racines de confiance
Configuration et affichage des exclusions à l'interception du trafic
Exclusions à l'interception du trafic par le système d'exploitation
Protection contre les menaces réseau
Configuration de la protection contre les menaces réseau dans Web Console
Configuration de la protection contre les menaces réseau dans la Console d'administration
Fenêtre Exclusions
Configuration de la Protection contre les menaces réseau sur la ligne de commande
Protection contre les menaces par emails
Configuration de la protection contre les menaces par emails dans Web Console
Configuration de la protection contre les menaces par emails dans la Console d'administration
Fenêtre Paramètres de la protection contre les menaces par emails
Fenêtre Filtre des pièces jointes
Configuration de la protection contre les menaces par emails dans la ligne de commande
Protection BadUSB
Configuration de la protection BadUSB dans Web Console
Configuration de la protection BadUSB dans la Console d'administration
Configuration de la protection BadUSB dans la ligne de commande
Protection contre le chiffrement malveillant à distance
Configuration de la protection contre le chiffrement dans Web Console
Configuration de la protection contre le chiffrement dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre Nouvelle zone d'analyse

Fenêtre Paramètres de la protection
Fenêtre Zones d'exclusion
Fenêtre Nouvelle zone d'exclusion
Fenêtre Exclusions d'après le masque
Configuration de la Protection contre le chiffrement sur la ligne de commande
Gestion des appareils bloqués
Contrôle des applications
À propos des règles du contrôle des applications
Mode de test des règles du Contrôle des applications
Configuration du contrôle des applications dans Web Console
Configuration du contrôle des applications dans la Console d'administration
Fenêtre Règles du Contrôle des applications
Fenêtre Ajouter une nouvelle règle
Fenêtre Catégories d'applications
Fenêtre Utilisateur ou groupe
Configuration du Contrôle des applications sur la ligne de commande
Paramètres de la tâche Contrôle des applications
Créer et modifier une liste des catégories
Consultation de la liste des catégories
Configuration de la liste des règles du Contrôle des applications
Exportation et importation des paramètres du Contrôle des applications
Inventaire
Configuration de l'inventaire dans Web Console
Fenêtre d'ajout d'une zone d'analyse
Section Zones d'exclusion
Fenêtre Zones d'exclusion
Fenêtre d'ajout d'une zone d'exclusion
Configuration de l'inventaire dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre Nouvelle zone d'analyse
Section Exclusions
Fenêtre Zones d'exclusion
Fenêtre Nouvelle zone d'exclusion
Configuration de l'inventaire dans la ligne de commande
Paramètres de la tâche d'inventaire
Consultation de la liste des applications détectées
Contrôle des appareils
Configuration du contrôle des appareils dans Web Console
Configuration du contrôle des appareils dans la Console d'administration
Fenêtre Appareils de confiance
Fenêtre Appareil de confiance (ID de l'appareil)
Fenêtre Appareils sur les appareils clients
Fenêtre Liste des appareils en fonction des événements du Contrôle des appareils
Fenêtre Accès à un appareil de confiance
Fenêtre Utilisateur ou groupe
Fenêtre Type d'appareil
Fenêtre Configuration de la règle d'accès aux appareils

Fenêtre Utilisateur ou groupe
Fenêtre Planification d'accès
Fenêtre Bus de connexion
Configuration du modèle de message du Contrôle des appareils
Configuration du Contrôle des appareils dans la ligne de commande
Paramètres du Contrôle des appareils
Afficher et exporter une liste des appareils connectés dans la ligne de commande
Administration de la liste des appareils de confiance à partir de la ligne de commande
Autorisation d'accès temporaire à l'appareil
Octroi d'accès à un appareil dans Web Console
Obtention d'un accès temporaire à un appareil dans la ligne de commande
Contrôle Internet
À propos des règles d'accès aux ressources Web
Configuration du Contrôle Internet dans Web Console
Configuration du Contrôle Internet dans la Console d'administration
Fenêtre Règle du Contrôle Internet
Fenêtre Sélectionner les catégories de contenu
Fenêtre Sélectionner les catégories de type de données
Fenêtre Sélectionner les adresses
Fenêtre Sélectionner un groupe d'adresses
Fenêtre Ajout d'un groupe d'adresses
Fenêtre Sélectionner les utilisateurs
Fenêtre Utilisateur ou groupe
Fenêtre Planification d'accès
Configuration des modèles de messages du Contrôle Internet
Configuration du Contrôle Internet dans la ligne de commande
Paramètres de la tâche Contrôle Internet
Affichage et modification des paramètres de contrôle Internet
Règles de formation des masques d'adresses de ressources Web
Contrôle de l'intégrité du système
Surveillez l'intégrité du système en temps réel
Configuration du contrôle de l'intégrité du système dans Web Console
Configuration du contrôle de l'intégrité du système dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre Nouvelle zone d'analyse
Fenêtre Zones d'exclusion
Fenêtre Nouvelle zone d'exclusion
Fenêtre Exclusions d'après le masque
Configuration du Contrôle de l'intégrité du système en ligne de commande
Vérification de l'intégrité du système
Contrôle de l'intégrité du système dans Web Console
Fenêtre d'ajout d'une zone d'analyse
Section Zones d'exclusion
Fenêtre Zones d'exclusion
Fenêtre d'ajout d'une zone d'exclusion
Fenêtre Exclusions d'après le masque

Contrôle de l'intégrité du système dans la Console d'administration
Fenêtre Zones d'analyse
Fenêtre Nouvelle zone d'analyse
Section Zones d'exclusion
Fenêtre Zones d'exclusion
Fenêtre Nouvelle zone d'exclusion
Fenêtre Exclusions d'après le masque
Configuration de la vérification de l'intégrité du système en ligne de commande
Détection comportementale
Configuration de la détection comportementale dans Web Console
Configuration de la détection comportementale dans la Console d'administration
Fenêtre Exclusions par processus
Fenêtre Processus de confiance
Configuration de la Détection comportementale sur la ligne de commande
Protection contre les Exploits
Configuration de la protection contre les Exploits dans Web Console
Configuration de la protection contre les exploits dans la Console d'administration
Fenêtre Exclusions de la Protection contre les Exploits
Fenêtre Exclusion de la Protection contre les Exploits
Configuration de la protection contre les Exploits dans la ligne de commande
Utilisation de Kaspersky Security Network
Configuration de l'utilisation de Kaspersky Security Network dans Web Console
Configuration de l'utilisation de Kaspersky Security Network dans la Console d'administration
Paramètres de Kaspersky Security Network
Déclaration de Kaspersky Security Network
Déclaration de Kaspersky Private Security Network
Configuration de l'utilisation de Kaspersky Security Network sur la ligne de commande
Vérification de la connexion à Kaspersky Security Network à l'aide de la ligne de commande
Activer ou désactiver le mode cloud à l'aide de la ligne de commande
Paramètres supplémentaires de fonctionnement de l'application
Configuration du serveur proxy
Configuration des paramètres du serveur proxy dans Web Console
Configuration des paramètres du serveur proxy dans la Console d'administration
Fenêtre Exclusions pour le serveur proxy
Configuration des paramètres du serveur proxy via la ligne de commande
Configuration des exclusions globales
Configuration des exclusions globales dans Web Console
Configuration des exclusions globales dans la Console d'administration
Fenêtre Chemin du point de montage
Configuration des exclusions globales sur la ligne de commande
Exclure la mémoire de processus de l'analyse
Sélection du mode d'interception pour les opérations sur les fichiers
Configuration de la détection des applications que les intrus peuvent utiliser pour causer des dommages
Activer la surveillance de la stabilité des applications
Configuration des paramètres de lancement de l'application
Limite d'utilisation de la mémoire résidente par une application
Limite d'utilisation de la mémoire et du processeur

Limite du nombre de tâches d'analyse personnalisée
Configuration de l'envoi des informations vers le stockage de Kaspersky Security Center
Configuration des autorisations de gestion des tâches
Arrêter le lancement des tâches lors de l'utilisation de la batterie
Configuration des paramètres d'interception des événements système
Vérification de la possibilité d'installer un module du noyau à actualiser
Mode « Sécurisé » lors de l'utilisation d'un module de noyau mis à jour
Configuration des paramètres d'interception dans Web Console
Configuration des paramètres d'interception dans la Console d'administration
Configuration des paramètres d'interception dans la ligne de commande
Configuration des paramètres avancés de la télémétrie
Sauvegarde
Configuration des paramètres de la sauvegarde dans Web Console
Configuration des paramètres de la sauvegarde dans la Console d'administration
Configuration des paramètres de la Sauvegarde via la ligne de commande
Utilisation des objets de Sauvegarde sur la ligne de commande
Intégration avec les solutions Detection and Response
À propos des actions pour répondre aux commandes des solutions Detection and Response
Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)
Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premise)
Configuration de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans Web Console
Configuration de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans la ligne de commande
Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)
Gestion des certificats pour la connexion aux serveurs OSMP
Intégration avec Kaspersky Anti Targeted Attack Platform
Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans Web Console
Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans la Console d'administration
Configuration de connexion aux serveurs KATA
+-/Configuration des paramètres généraux de connexion aux serveurs KATA
Configuration des paramètres du transfert des données aux serveurs KATA
Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans la ligne de commande
Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)
Gestion des certificats pour la connexion au serveur KATA
Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans Web Console
Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans la Console d'administration
Configuration de connexion aux serveurs NDR
+-/Configuration des paramètres généraux de connexion aux serveurs NDR
Configuration des paramètres du transfert des données aux serveurs NDR
Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans la ligne de commande
Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)
Gestion des certificats pour la connexion au serveur NDR
Intégration avec Sandbox
Configuration de l'intégration avec Sandbox dans Web Console
Configuration de l'intégration avec Sandbox dans ligne de commande
Paramètres d'intégration avec Sandbox
Gestion des certificats pour la connexion au serveur Sandbox

Intégration avec Kaspersky Endpoint Detection and Response Optimum
Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum
Activation ou désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans Web Console
Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans la ligne de commande
Consultation de l'état d'intégration avec Kaspersky Endpoint Detection and Response (KATA)
Afficher des informations sur la menace détectée et les actions de réponse
Intégration avec la solution Kaspersky Managed Detection and Response
Recommandations pour la création d'une image de référence en vue d'une intégration correcte avec MDR
Téléchargement du fichier de configuration KPSN pour l'intégration avec Kaspersky Managed Detection and Response
Configuration de l'intégration avec Kaspersky Managed Detection and Response dans Web Console
Configuration de l'intégration avec Kaspersky Managed Detection and Response dans la Console d'administration
Configuration de l'intégration avec Kaspersky Managed Detection and Response dans la ligne de commande
Isolation réseau
Activer ou désactiver manuellement l'isolation réseau d'un appareil dans Web Console
Configuration de la durée d'isolement du réseau en mode automatique
Configuration des paramètres de l'isolation réseau en mode manuel
Configuration des exclusions de l'isolement du réseau dans Web Console
Configuration des exclusions de l'isolement du réseau en mode automatique
Ajouter une fenêtre d'exclusion de l'isolement du réseau
Fenêtre Dictionnaire des profils réseau
Gestion de l'isolation réseau des appareils à partir de la ligne de commande
Travailler avec la quarantaine
Mise en quarantaine d'un fichier à l'aide de Web Console
Configuration des paramètres de la quarantaine dans Web Console
Configuration des paramètres de la quarantaine dans la Console d'administration
Configuration des paramètres de la quarantaine dans la ligne de commande
Travailler avec des fichiers de quarantaine dans la ligne de commande
Démarrage du processus
Terminer le processus
Reception d'un fichier depuis un appareil
Suppression d'un fichier de votre appareil
Trouver des indicateurs de compromission
Rechercher des indicateurs de compromission dans Web Console
Trouver des indicateurs de compromission dans la ligne de commande
Exigences pour les fichiers IOC
Prévention de l'exécution des objets
Configurer la prévention du lancement des objets dans Web Console
Configuration de la prévention du lancement des objets dans la Console d'administration
Contrôler la prévention du lancement des objets dans la ligne de commande
Cloud Sandbox
Intégration avec Kaspersky Unified Monitoring and Analysis Platform
Configuration de l'intégration avec KUMA dans Web Console
Configuration de l'intégration avec KUMA dans la Console d'administration
Fenêtre Serveurs KUMA
Fenêtre Serveur KUMA

Fenêtre Paramètres de connexion aux serveurs KUMA
Fenêtre d'ajout d'un certificat de serveur
Fenêtre d'ajout d'un certificat client
Configuration de l'intégration avec KUMA dans la ligne de commande
Paramètres de la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform
Gestion des certificats pour la connexion au serveur KUMA
Configuration des paramètres d'utilisation de l'application en mode Light Agent
Configuration des paramètres du Light Agent dans Web Console
Configuration des paramètres du Light Agent dans la Console d'administration
Connexion au serveur d'intégration
Fenêtre Connexion au serveur d'intégration
Fenêtre Vérification du certificat du Serveur d'intégration
Fenêtre Authentification sur le Serveur d'intégration
Paramètres de détection des SVM
Tag de connexion à la SVM
Algorithme de sélection des SVM
Protection de la connexion
Afficher des informations sur l'utilisation d'une application en mode Light Agent dans la ligne de commande
Afficher les événements et les rapports
Configuration d'enregistrement des événements dans le journal du système d'exploitation
Configuration des paramètres du journal des événements de l'application
Consultation des événements dans Kaspersky Security Center
Affichage des événements en ligne de commande
Configuration des notifications contextuelles dans l'interface graphique
Administration de l'application via l'interface graphique
Interface graphique
Activer ou désactiver les modules de l'application
Démarrage et arrêt des tâches d'analyse
Lancement de l'analyse personnalisée et de l'analyse dans Sandbox
Démarrer et arrêter la tâche de mise à jour
Configuration de l'utilisation de Kaspersky Security Network
Consulter les rapports
Afficher les objets de la sauvegarde
Gestion des clés de licence
Ajout d'une clé de licence
Suppression de la clé de licence
Consultation des informations relatives à la licence
Obtention d'accès temporaire à l'appareil
Consultation des informations sur l'application
Création d'un fichier de traçage
Vérification de l'intégrité des modules d'application
Contacter le Support technique
Support technique via le Kaspersky CompanyAccount
Obtention d'informations pour le Support technique
À propos des fichiers de traçage de l'application
Configuration des paramètres de trace de l'application
À propos des fichiers de traçage du plug-in d'administration des applications

À propos des fichiers de vidage
Configuration des paramètres d'enregistrement des vidages
Diagnostic à distance de l'appareil à l'aide de Kaspersky Security Center
Annexes
Annexe 1. Commandes de gestion de Kaspersky Endpoint Security
Commandes de gestion des paramètres et des tâches de l'application
Commandes de gestion des paramètres généraux de l'application
Commandes de gestion des paramètres des tâches
Commandes de gestion des tâches
Commandes pour contrôler la prévention du lancement des objets
Commandes de gestion des paramètres généraux d'analyse du conteneur
Commandes de gestion des paramètres d'analyse du trafic réseau
Commandes de statistiques
Commandes d'affichage des événements
Commandes de gestion des événements de l'application
Commandes de gestion des clés de licence
Commandes de gestion du pare-feu
Commandes de contrôle pour les appareils bloqués
Commandes de gestion du Contrôle des appareils
Commandes de gestion du Contrôle des applications
Commandes de gestion du Contrôle Internet
Commandes de gestion de la sauvegarde
Commandes de gestion de la quarantaine
Commandes de gestion des utilisateurs et des rôles
Commandes d'administration du module Expert EDR (on-premise)
Commandes d'administration des modules NDR (KATA)
Commandes de contrôle d'isolation réseau des appareils
Commandes de gestion des paramètres d'intégration avec KUMA
Commandes de gestion des paramètres d'intégration avec Sandbox
Commandes de gestion de l'analyse IOC
Commandes applicatives en mode Light Agent pour la protection des environnements virtuels
Commandes pour gérer la collecte de métriques d'état du système
Annexe 2. Fichiers de configuration et paramètres de l'application par défaut
Règles d'édition des fichiers de configuration des tâches de l'application
Fichiers de configuration préinstallés
Paramètres des tâches de ligne de commande par défaut
Paramètres par défaut de la tâche File_Threat_Protection (ID:1)
Paramètres par défaut de la tâche Scan_My_Computer (ID:2)
Paramètres par défaut de la tâche Scan_File (ID:3)
Paramètres par défaut de la tâche Critical_Areas_Scan (ID:4)
Paramètres par défaut pour la tâche Update (ID:6)
Paramètres par défaut de la tâche System_Integrity_Monitoring (ID:11)
Paramètres par défaut de la tâche Firewall_Management (ID:12)
Paramètres par défaut de la tâche Anti_Cryptor (ID:13)
Paramètres par défaut de la tâche Web_Threat_Protection (ID:14)
Paramètres par défaut de la tâche Device_Control (ID:15)
Paramètres par défaut de la tâche Removable_Drives_Scan (ID:16)

Paramètres par défaut de la tâche Network_Threat_Protection (ID:17)
Paramètres par défaut pour les tâches Container_Scan (ID:18) et Custom_Container_Scan (ID:19)
Paramètres par défaut de la tâche Behavior_Detection (ID:20)
Paramètres par défaut de la tâche Application_Control (ID:21)
Paramètres par défaut de la tâche Inventory_Scan (ID:22)
Paramètres par défaut de la tâche KATAEDR (ID:24)
Paramètres par défaut pour la tâche Web_Control (ID:26)
Paramètres par défaut de la tâche Standalone_Sandbox (ID:29)
Paramètres par défaut de la tâche KATANDR (ID:31)
Paramètres par défaut de la tâche KUMA (ID:33)
Paramètres par défaut de la tâche Protection contre les menaces par emails (ID : 35)
Paramètres par défaut de la tâche Protection BadUSB (ID:37)
Paramètres généraux de l'application
Paramètres généraux d'analyse du conteneur
Paramètres d'analyse du trafic réseau
Paramètres de planification des tâches
Annexe 3. Codes de retour de la ligne de commande
Annexe 4. Configuration de la collaboration avec Kaspersky Antivirus for Linux Mail Server
Annexe 5. Paramètres de l'application dans Web Console
Protection contre les menaces contre l'hôte
Protection contre les fichiers malicieux
Protection BadUSB
Analyse des disques amovibles
Détection comportementale
Protection contre le chiffrement
Protection contre les Exploits
Protection des connexions réseau et des moyens de communications
Protection contre les menaces par emails
Protection contre les menaces Internet
Protection contre les menaces réseau
Pare-feu
Contrôles de sécurité
Contrôle des appareils
Contrôle Internet
Contrôle des applications
Contrôle de l'intégrité du système
Exclusions de l'analyse pour l'application
Paramètres généraux
Paramètres de détection
Kaspersky Security Network
Interaction avec l'utilisateur
Performances
Paramètres du réseau
Analyser les conteneurs.
Support technique
Rapports et stockage
Intégration avec KSC

Paramètres d'interaction avec le système d'exploitation
Paramètres des événements
Paramètres de la télémétrie
Agents intégrés
Managed Detection and Response
Endpoint Detection and Response Optimum
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Sandbox
Intégration avec KUMA
Mode Light Agent
Paramètres de détection des SVM
Paramètres de connexion au Serveur d'intégration
Tag de connexion à la SVM
Algorithme de sélection des SVM
Protection de la connexion
Annexe 6. Paramètres d'interaction avec les services externes
Interopérabilité avec les solutions Kaspersky
Kaspersky Security Center Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
Sources d'informations sur Kaspersky Endpoint Security
Glossaire
Abonnement
Activation de l'application
Appareil de confiance
Base des URL de phishing
Base des URL malveillantes
Bases d'applications
Certificat de licence
Clé active
Clé de réserve
Exclusion
Faux positif
Groupe d'administration
Licence
Light Agent
Masque de fichier
Objet infecté
Objets de démarrage automatique
Paramètres de l'application
Protection contre le chiffrement
Réparation d'objets
Serveur d'administration
Serveur d'intégration
Serveur Proxy
Serveurs de mise à jour de Kaspersky

Stratégie
Stratégie active
Stratégie de groupe
SVM
Système SIEM
Tâche de groupe
Informations sur le code tiers
Notice sur les marques de commerce

Aide de Kaspersky Endpoint Security 12.4 for Linux

Nouvelles fonctionnalités

Nouveautés de Kaspersky Endpoint Security 12.4 for Linux

Configurations logicielle et matérielle

Configurations logicielle et matérielle pour l'application

Comparaison des fonctionnalités

- Comparaison des fonctions de l'application selon la licence
- Particularités d'utilisation de l'application en mode Light Agent
- Particularités de fonctionnement de l'application en mode Endpoint Detection and Response Agent

Guide de démarrage

- Un guide rapide pour l'installation et la configuration initiale de l'application via la ligne de commande (l'application est utilisée en mode standard)
- Mise à niveau à partir de la version précédente de l'application
- Préparation de l'installation de l'application
- Installation et configuration initiale de l'application
- Mise à jour des bases de données et des modules de l'application dans la ligne de commande lors de la configuration initiale
- Mise à jour des bases de données de l'application dans la ligne de commande à l'aide d'une tâche prédéfinie de mise à jour (après la configuration initiale)
- Préparation de l'application pour une utilisation via Kaspersky Security Center

Licence

- Licences de l'application
- Activation des applications et gestion des clés de licence
- Activation de l'application lors de la configuration initiale dans la ligne de commande
- Activation de l'application et gestion des clés de licence dans la ligne de commande (après la configuration initiale)
- Activation de l'application via Kaspersky Security Center

Surveillance et rapports

- Afficher l'état de sécurité de l'appareil et les informations sur les performances des applications
- Afficher des informations sur le fonctionnement d'une application dans la ligne de commande
- Afficher les événements et les rapports

À propos des données et Protection des informations personnelles

- Fourniture de données

Fonctionnalités supplémentaires

- AConfiguration des paramètres d'utilisation de l'application en mode Light Agent
- Configuration des paramètres supplémentaires de fonctionnement de l'application
- Utilisation de Kaspersky Security Network
- Sauvegarde
- Intégration avec les solutions Detection and Response

Optimisation de la consommation des ressources du système d'exploitation

- Optimisation de l'utilisation des ressources

Contacter le Support Technique

- Étapes de base pour diagnostiquer les problèmes de l'application
- Contacter le Support technique

À propos de Kaspersky Endpoint Security 12.4 for Linux

Kaspersky Endpoint Security 12.4 for Linux ("Kaspersky Endpoint Security", "application") est conçu pour protéger les appareils exécutant des systèmes d'exploitation Linux® contre divers types de menaces, y compris les attaques réseau et frauduleuses.

L'application vous permet de protéger à la fois les appareils physiques et les machines virtuelles. Vous pouvez utiliser l'application Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Security for Virtualization Light Agent pour protéger les machines virtuelles exécutant des systèmes d'exploitation invités Linux.

L'application n'est pas destinée à être utilisée dans des processus technologiques utilisant des systèmes de gestion automatisés. Pour protéger les appareils de tels systèmes, il est recommandé d'utiliser l'application Kaspersky Industrial CyberSecurity for Linux Nodes.

Les principales fonctions de protection et de contrôle des appareils sont assurées par les modules fonctionnels et les tâches de l'application suivants :

- La **Protection contre les fichiers malicieux** permet d'éviter l'infection du système de fichiers de l'appareil de l'utilisateur. Le module *Protection contre les fichiers malicieux* démarre automatiquement au démarrage de Kaspersky Endpoint Security et analyse tous les fichiers ouverts, enregistrés et lancés en temps réel.

  Vous pouvez également analyser les appareils protégés à la demande à l'aide des tâches d'analyse suivantes :

  - **Analyse des logiciels malveillants**. L'application vérifie les objets du système de fichiers situés sur les disques locaux de l'appareil, ainsi que les ressources montées et partagées accessibles via les protocoles SMB et NFS à la recherche de logiciels malveillants. Vous pouvez utiliser cette tâche pour effectuer une analyse complète ou sélective de l'appareil.

  - **Analyse des zones critiques**. L'application analyse les secteurs d'amorçage, les objets de démarrage automatique, la mémoire des processus et la mémoire du noyau.

- **Analyse des disques amovibles**. Le module *Analyse des disques amovibles* vous permet de surveiller en temps réel la connexion des disques amovibles à l'appareil et d'analyser le disque amovible et ses secteurs de démarrage pour détecter la présence d'applications malveillantes. Kaspersky Endpoint Security peut analyser les lecteurs amovibles suivants : lecteurs CD/DVD, lecteurs Blu-ray, lecteurs flash (y compris les modems USB), disques durs externes et disquettes.

- **Analyse du conteneur**. Le module *Surveillance des conteneurs (Analyse du conteneur, Surveillance des conteneurs)* permet d'analyser les espaces de noms et les conteneurs en cours d'exécution à la recherche d'applications malveillantes en temps réel. L'intégration avec le système d'administration de conteneurs Docker, l'environnement CRI-O, les utilitaires Podman et runc est prise en charge. À l'aide de la tâche *Analyse du conteneur*, vous pouvez analyser des conteneurs et des images à la demande.

- **Protection contre les menaces Internet**. Le module *Protection contre les menaces Internet* vous permet d'analyser le trafic entrant, d'empêcher le téléchargement de fichiers malveillants depuis Internet et de bloquer le phishing, la publicité et d'autres sites dangereux. Kaspersky Endpoint Security peut analyser les connexions chiffrées.

- **Protection contre les menaces réseau**. Le module *Protection contre les menaces réseau* vous permet d'analyser le trafic réseau entrant à la recherche d'actions typiques des attaques réseau.

- **Gestion du pare-feu**. Le module *Gestion du Pare-feu* vous permet de contrôler les paramètres du pare-feu du système d'exploitation et de filtrer toutes les activités réseau conformément aux règles de paquets réseau que vous avez configurées.

- **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 de virus et d'autres pièces jointes malveillantes.

- **Protection BadUSB**. Le module *Protection BadUSB* empêche les appareils USB infectés de se connecter à votre ordinateur en imitant un clavier.

- **Protection contre le chiffrement**. Le module *Protection contre le chiffrement* vous permet de vérifier l'accès des appareils distants aux fichiers situés dans des répertoires locaux avec accès réseau via les protocoles SMB/NFS et de protéger les fichiers contre le chiffrement malveillant à distance.

- **Contrôle des appareils**. Le module *Contrôle des appareils* permet de contrôler l'accès des utilisateurs aux appareils installés ou connectés à l'appareil client (par exemple, disques durs, caméras ou modules Wi-Fi). Cela vous permet de protéger l'appareil client contre les infections lorsque des appareils externes sont connectés et d'éviter la perte ou les fuites de données. L'accès des utilisateurs aux appareils est contrôlé par les modes d'accès et les règles d'accès que vous configurez.

- **Contrôle des applications**. Le module *Contrôle des applications* vous permet de contrôler le lancement des applications sur les appareils des utilisateurs. Cela réduit le risque d'infection de l'appareil en limitant l'accès aux applications. Le démarrage de l'application est contrôlé par les règles du Contrôle des applications que vous configurez.

- **Inventaire**. La tâche *Inventaire* permet d'obtenir des informations sur tous les fichiers exécutables des applications conservés sur les appareils clients. Ces informations peuvent être utiles, par exemple, pour créer des règles de Contrôle des applications.

- **Contrôle Internet**. Le module *Contrôle Internet* gère l'accès des utilisateurs aux ressources Web. Cela vous permet de réduire la consommation de trafic et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur tente d'ouvrir un site dont l'accès est restreint par le Contrôle Internet, l'application Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement.

- **Détection comportementale**. Le module *Détection comportementale* permet de contrôler l'activité malveillante des applications dans le système d'exploitation. En cas de détection d'une activité malveillante, l'application Kaspersky Endpoint Security peut arrêter le processus de l'application qui exécute l'activité malveillante.

- Le **contrôle de l'intégrité du système** vous permet de suivre les modifications apportées aux fichiers et répertoires du système d'exploitation. Le module *Contrôle de l'intégrité du système* surveille en temps réel les actions effectuées avec les objets de la zone de surveillance spécifiée dans les paramètres du modules. À l'aide de la tâche *Vérification de l'intégrité du système*, vous pouvez effectuer une vérification de l'intégrité du système à la demande. Le contrôle est effectué en comparant l'état actuel des objets inclus dans la zone de surveillance avec l'état initial de ces objets, préalablement enregistré sous la forme d'un instantané de l'état du système.

Kaspersky Endpoint Security vous permet de détecter les objets infectés et de neutraliser les menaces qui y sont détectées. Dans ce cas, l'application peut utiliser :

- Les bases de l'application pour détecter et désinfecter les fichiers infectés. L'application recherche la présence éventuelle de menaces dans chaque fichier dans le cadre de l'analyse : le code du fichier est comparé à un code qui ressemble à une menace particulière.

- Kaspersky Security Network. L'exploitation des données de Kaspersky Security Network garantit une réaction plus rapide de l'application Kaspersky Endpoint Security face aux nouvelles menaces. Elle améliore également les performances de certains modules de la protection et réduit le risque de faux positifs.

Avant la désinfection ou la suppression, Kaspersky Endpoint Security enregistre des copies de sauvegarde des fichiers dans la sauvegarde situé sur l'appareil. Si le fichier désinfecté contenait des informations importantes devenues totalement ou partiellement inaccessibles suite au traitement, vous pouvez restaurer le fichier à partir d'une copie de celui-ci.

Lors de l'exécution des tâches d'analyse, Kaspersky Endpoint Security peut désinfecter et supprimer les fichiers protégés contre toute modification : les fichiers avec les attributs immutable et append-only et les fichiers dans les répertoires avec les attributs immutable et append-only. La sauvegarde conserve des copies de ces fichiers créés avant traitement ou suppression. Vous pouvez restaurer des fichiers à partir de sauvegardes si nécessaire. Une fois les tâches d'analyse terminées, les attributs immuables et append-only des fichiers désinfectés ne sont pas enregistrés.

L'application Kaspersky Endpoint Security peut fonctionner en mode informatif. Le *mode d'information* est un mode de fonctionnement d'une application dans lequel, si une menace est détectée, les modules et les tâches de l'application ne tentent pas de désinfecter ou de supprimer les objets malveillants, de refuser l'accès ou de bloquer l'activité des applications. Au lieu de cela, l'application informe uniquement l'utilisateur de la menace détectée.

Kaspersky Endpoint Security prend en charge la possibilité de s'intégrer à d'autres solutions de Kaspersky pour étendre les capacités de l'application :

- L'intégration avec Kaspersky Managed Detection and Response permet de s'assurer que les menaces visant votre organisation sont détectées, identifiées et éliminées en permanence.

- L'intégration avec Kaspersky Anti Targeted Attack Platform protège l'infrastructure informatique de votre organisation et assure la détection rapide des menaces telles que les attaques "zero-day", les attaques ciblées et les attaques ciblées complexes.

- L'intégration avec Kaspersky Endpoint Detection and Response Optimum protège l'infrastructure informatique de l'organisation contre les menaces telles que les exploits, les ransomwares, les attaques sans fichier et l'utilisation par des attaquants d'outils système légitimes pour nuire aux appareils ou aux données.

- L'intégration avec Kaspersky Unified Monitoring and Analysis Platform garantit la réception, le traitement et le stockage des événements de sécurité des informations ; l'analyse et la corrélation des données ; la recherche par événements et la création des notifications sur l'identification des signes de menaces pour la sécurité des informations.

- L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) protège contre la plupart des cyber-risques et couvre les principaux scénarios de menaces.

Pour maintenir l'application à jour, des fonctions supplémentaires de l'application sont fournies :

- Activation de l'application à l'aide d'un fichier clé ou d'un code d'activation.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent).

- Mise à jour les bases et les modules de l'application depuis les serveurs de mise à jour de Kaspersky, via le Serveur d'administration ou depuis une source de mise à jour planifiée ou à la demande définie par l'utilisateur.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'application reçoit les mises à jour des bases de données et des modules d'application du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent).

- Limitation de l'accès des utilisateurs aux fonctions de l'application en fonction des rôles des utilisateurs.
- Notification de l'administrateur sur les événements qui ont eu lieu pendant l'utilisation de l'application.
- Vérification de l'intégrité des modules de l'application à l'aide de l'utilitaire de vérification d'intégrité.

Vous pouvez administrer l'application Kaspersky Endpoint Security à l'aide des moyens suivants :

- Utilisation de Kaspersky Security Center via Kaspersky Security Center Web Console, Kaspersky Security Center Cloud Console ou la Console d'administration.
- À l'aide des commandes d'administration à partir de la ligne de commande.
- À l'aide de l'interface utilisateur graphique.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, Kaspersky Security Center est requis pour gérer l'application. L'application ne peut pas être administrée à l'aide de Kaspersky Security Center Cloud Console et de l'interface utilisateur graphique.

La fonctionnalité des mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

À propos des modes d'utilisation de l'application Kaspersky Endpoint Security

Vous pouvez utiliser Kaspersky Endpoint Security dans l'un des modes suivants :

- En mode standard pour protéger les postes de travail et les serveurs (ci-après, « Mode Standard »). Kaspersky Endpoint Security est utilisé comme application autonome pour protéger les appareils exécutant des systèmes d'exploitation Linux.
- En mode Light Agent pour protéger les environnements virtuels dans le cadre de la solution Kaspersky Security for Virtualization Light Agent (ci-après, « mode Light Agent »). Kaspersky Endpoint Security est utilisé comme module Light Agent de la solution Kaspersky Security for Virtualization Light Agent pour protéger les machines virtuelles exécutant les systèmes d'exploitation invités Linux.
- En mode Endpoint Detection and Response Agent, les solutions Detection and Response de Kaspersky et les applications antivirus tierces (ci-après également "mode Endpoint Detection and Response Agent") peuvent fonctionner conjointement sur les appareils protégés.

L'application ne peut être utilisée que dans un seul mode à la fois.

Par défaut, l'application est utilisée en mode standard.

Utilisation de l'application en mode Light Agent

Si vous souhaitez utiliser l'application en mode Light Agent, vous devez procéder comme suit :

1. Exécuter l'installation de l'application Kaspersky Endpoint Security en mode Light Agent sur chaque machine virtuelle devant être protégée à l'aide de Kaspersky Security for Virtualization Light Agent. Vous pouvez également installer l'application sur un modèle de machine virtuelle.

   Avant d'installer l'application, vous devez installer l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles et les modèles de machines virtuelles.

   Lors de l'installation, vous devez préciser que l'application sera utilisée en mode Light Agent de l'une des manières suivantes :

   - lors de la configuration initiale de l'application en mode interactif ou automatique (en cas d'installation par ligne de commande) ;
   - dans les propriétés du paquet d'installation de l'application ou dans le fichier de configuration autoinstall.ini inclus dans le paquet d'installation (s'il est installé à l'aide de Kaspersky Security Center).

   Une fois Kaspersky Endpoint Security installé, il n'est pas possible de modifier le mode d'utilisation de l'application.

Lorsque vous sélectionnez le mode Light Agent, vous pouvez également configurer les paramètres suivants pour le fonctionnement de Kaspersky Endpoint Security en mode Light Agent :

- Le rôle de la machine virtuelle que vous souhaitez protéger dans l'infrastructure virtuelle : serveur ou poste de travail. Le rôle de la machine virtuelle détermine sous quelle licence l'application sera utilisée sur cette machine virtuelle et la quantité de fonctionnalités disponibles.

- Mode de protection de l'infrastructure VDI. Il est recommandé d'activer ce mode si vous installez l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. Le mode de protection de l'infrastructure VDI vous permet d'optimiser le fonctionnement de Kaspersky Endpoint Security sur les machines virtuelles temporaires.

2. Configurez les paramètres de connexion du Light Agent à la SVM et les paramètres de connexion du Light Agent au Serveur d'intégration.

   Kaspersky Endpoint Security en mode Light Agent interagit avec d'autres modules de la solution Kaspersky Security for Virtual Environments Light Agent : le Serveur d'intégration et le Serveur de protection installés sur la SVM (pour plus de détails, consultez l'de la solution Kaspersky Security for Virtual Environments Light Agent). Pour interagir avec le Serveur de Protection, Kaspersky Endpoint Security établit et maintient une connexion avec la SVM sur laquelle ce Serveur de Protection est installé.

   Une connexion au Serveur d'intégration est requise si vous souhaitez que les Light Agents reçoivent des informations sur la SVM via le Serveur d'intégration, ou si vous souhaitez sécuriser la connexion entre le Serveur de sécurité et le Light Agent.

   Vous pouvez configurer les paramètres de connexion dans les propriétés la stratégie de Kaspersky Endpoint Security à l'aide de la Console d'administration de Kaspersky Security Center ou à l'aide de Kaspersky Security Center Web Console.

Vous pouvez obtenir des informations sur les paramètres de l'application en mode Light Agent, sur la connexion au Serveur d'intégration et à la SVM à l'aide des commandes de l'application :

- `kesl-control --ksvla-info`

- `kesl-control --viis-info`

- `kesl-control --svm-info`

Les informations sur le mode d'utilisation de l'application sont affichées dans Kaspersky Security Center dans les propriétés de l'application Kaspersky Endpoint Security sur l'appareil géré dans la section **Modules**. Les informations sont affichées dans la ligne **Mode Light Agent pour la protection des environnements virtuels** comme suit :

- l'état *en cours d'exécution* signifie que l'application est utilisée en mode Light Agent ;

- L'état *non installé* signifie que l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.

À propos de l'activation de l'application en mode Light Agent

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, vous n'avez pas besoin d'activer l'application séparément. Vous activez tous les modules de la solution Kaspersky Security for Virtualization Light Agent en même temps. L'activation s'effectue du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant une clé de licence à la SVM. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

La licence de base de Kaspersky Security for Virtualization Light Agent peut ne pas inclure de fonctionnalités supplémentaires de l'application Kaspersky Endpoint Security (par exemple, la fonctionnalité d'intégration avec les solutions Detection and Response de Kaspersky). Dans ce cas, vous devez également ajouter une clé de licence à la SVM pour activer la fonctionnalité supplémentaire requise.

Après avoir activé la solution et connecté le Light Agent à la SVM, le module Serveur de protection envoie les informations sur la licence au Light Agent. Lors de la sélection d'une SVM pour la connexion, Light Agent prend en compte, entre autres paramètres, le type de clé de licence ajoutée à la SVM. Le Light Agent ne se connecte pas à la SVM si le type de clé ajoutée à la SVM ne correspond pas au rôle de la machine virtuelle protégée dans l'infrastructure virtuelle (serveur ou poste de travail). Pour plus d'informations sur les particularités de connexion du Light Agent à la SVM, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Vous pouvez afficher des informations sur la licence sous laquelle le Light Agent for Linux est utilisé à distance à l'aide de Kaspersky Security Center ou sur une machine virtuelle protégée avec le Light Agent à l'aide de la ligne de commande.

La gestion des clés de licence n'est pas prise en charge à l'aide de la tâche *Ajouter une clé* de Kaspersky Endpoint Security et à l'aide des commandes de Kaspersky Endpoint Security pour ajouter et supprimer des clés de licence.

À propos de la mise à jour des bases de données et des modules de l'application en mode Light Agent

Kaspersky Endpoint Security en mode Light Agent utilise les bases de données spéciales de logiciels malveillants nécessaires au fonctionnement de l'application 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. Pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent.

Les bases de données et les modules logiciels sur les machines virtuelles protégées sont mis à jour à l'aide d'une tâche locale spéciale *Mise à jour* de l'application Kaspersky Endpoint Security, qui spécifie un dossier sur la SVM comme source de mise à jour. La tâche de mise à jour démarre automatiquement. Vous ne pouvez pas supprimer cette tâche et modifier ses paramètres.

Les sources de mise à jour autres qu'un dossier sur les SVM ne sont pas prises en charge. L'utilisation de tâches de mise à jour de groupe n'est pas prise en charge.

La dernière mise à jour de la base de données des logiciels malveillants est également annulée du côté du Serveur de protection. Après l'annulation de la mise à jour des bases et des modules d'application sur la SVM, une tâche locale spéciale *Update* est lancée sur la machine virtuelle protégée. Cette tâche permet au Light Agent d'utiliser de nouveau l'ensemble précédent de bases de données malveillantes.

L'utilisation de la tâche locale et de groupe *Annulation de la mise à jour des bases* de l'application Kaspersky Endpoint Security n'est pas prise en charge.

Autres particularités de fonctionnement de l'application en mode Light Agent

Si Kaspersky Endpoint Security est utilisé en mode Light Agent :

- L'application ne peut pas être administrée à l'aide de Kaspersky Security Center Cloud Console et de l'interface utilisateur graphique.
- L'utilisation de bases cloud n'est pas prise en charge.
- Kaspersky Endpoint Security interagit avec les serveurs KSN à l'aide du serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge.
- L'utilisation du serveur proxy de l'application n'est pas prise en charge lors de la connexion au Serveur d'intégration, à la SVM et au serveurs KSN.

Utilisation de l'application en mode Endpoint Detection and Response Agent

L'application Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent vous permet d'utiliser les fonctionnalités des solutions Detection and Response de Kaspersky pour protéger les appareils sur lesquels des applications antivirus tierces sont installées.

En mode Endpoint Detection and Response Agent, les modules de protection et de contrôle standards de Kaspersky Endpoint Security ne sont pas utilisés pour protéger l'appareil. La protection standard de l'appareil est assurée par une application antivirus tierce. L'application Kaspersky Endpoint Security, en mode Endpoint Detection and Response Agent, surveille en permanence les processus exécutés sur l'appareil, les connexions réseau ouvertes et les fichiers modifiés, et assure l'intégration avec les avec les solutions Detection and Response suivantes :

- Kaspersky Endpoint Detection and Response Expert (on-premises) sur Open Single Management Platform (ci-après, "OSMP").
- Les modules Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sont intégrés à Kaspersky Anti Targeted Attack Platform (ci-après, "KATA").

Kaspersky Endpoint Security for Linux version 12.4 peut fonctionner conjointement avec l'application antivirus Dr. Web. Vous pouvez installer Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent sur un appareil avec Dr. Web.

Les applications doivent être installées dans l'ordre suivant : d'abord l'application antivirus tierce, puis l'Agent d'administration de Kaspersky Security Center, et enfin Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent. En effet, le programme d'installation de l'application tierce peut détecter les applications Kaspersky comme incompatibles et les supprimer. Après la mise à jour d'une application tierce sur un appareil, il est recommandé de vérifier le bon fonctionnement de Kaspersky Endpoint Security et de l'Agent d'administration, car le programme d'installation de l'application tierce analyse à nouveau l'appareil à la recherche de logiciels incompatibles et peut supprimer les applications Kaspersky.

Configuration de l'application dans le mode Endpoint Detection and Response Agent

Si vous souhaitez utiliser l'application Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, vous devez procéder comme suit :

1. Exécuter l'installation de l'application Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent sur chaque machine virtuelle à protéger.

   Vous pouvez consulter des informations sur le mode d'utilisation de l'application en utilisant la ligne de commande en exécutant la commande `kesl-control --app-info`.

2. Activer l'application Vous devez ajouter à l'application une clé de licence distincte, « Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on » (ci-après également dénommée « clé EDR Expert (on-premise) »).

   > Pour activer l'application en mode Endpoint Detection and Response Agent, seule une clé permettant d'accéder à des fonctionnalités supplémentaires est requise. Il n'est pas nécessaire d'ajouter la clé de licence primaire à l'application.

3. Activer l'intégration avec les solutions de Detection and Response que vous souhaitez utiliser pour protéger votre appareil :

   - Pour intégrer Kaspersky Endpoint Detection and Response Expert (on-premise) sur la plateforme OSMP, vous devez activer le module EDR Expert (on-premise) et gérer les paramètres d'intégration dans Kaspersky Security Center Web Console ou sur la ligne de commande.

   - Pour intégrer Kaspersky Endpoint Detection and Response sur la plateforme Kaspersky Anti Targeted Attack Platform, vous devez activer le module EDR Expert (on-premise) et gérer les paramètres d'intégration dans Kaspersky Security Center Web Console, dans la Console d'administration ou sur la ligne de commande.

   - Pour intégrer Kaspersky Network Detection and Response (NDR) à Kaspersky Anti Targeted Attack Platform, vous devez activer le module NDR (KATA) et configurer les paramètres d'intégration dans Kaspersky Security Center Web Console, la Console d'administration ou dans la ligne de commande.

   Vous pouvez vérifier l'état de fonctionnement des modules EDR Expert (on-premise) et NDR (KATA) :

   - Dans les propriétés de l'appareil dans Web Console (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → **Général** → **Modules**).

   - À l'aide de la ligne de commande, en exécutant la commande `kesl-control --app-info`.

Particularités de fonctionnement de l'application en mode Endpoint Detection and Response Agent

Si vous utilisez Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, l'ensemble des modules et des tâches disponibles pour l'application est limité. Après l'installation, les paramètres de l'application sont configurés comme suit :

- Modules entièrement gérables assurant l'intégration avec les solutions Detection and Response :
  - EDR Expert (on-premises).
  - NDR (KATA).

  Ces modules sont désactivés par défaut ; vous devez les activer pour que l'application fonctionne en mode Endpoint Detection and Response Agent. Vous pouvez personnaliser les paramètres d'intégration, y compris la fonctionnalité de prévention du lancement des objets.
- L'accès aux fichiers n'est pas bloqué pendant l'analyse : la case **Bloquer l'accès aux fichiers pendant l'analyse** est décochée (`FileBlockDuringScan=No`). Ce paramètre ne peut pas être modifié.
- Les modules Protection contre les fichiers malicieux et Protection contre le chiffrement sont disponibles en mode de fonctionnalités limitées : lorsqu'une menace est détectée, ces modules ne tentent pas de désinfecter ou de supprimer les objets malveillants, de refuser l'accès ou de bloquer l'activité de l'application, mais envoient uniquement des informations sur la détection de la menace à des serveurs qui assurent l'intégration avec les solutions Detection and Response.

  Vous pouvez activer ou désactiver la Protection contre les fichiers malicieux et la Protection contre le chiffrement, et configurer les paramètres des modules, à l'exception des actions lors de la détection d'une menace. Les paramètres suivants ne peuvent pas être modifiés :
  - Module Protection contre les fichiers malicieux : **Action lors de la détection d'une menace** : **Ignorer** (`ActionOnThreat=Skip`).
  - Module Protection contre le chiffrement : **Action lors de la détection du chiffrement** : **Informer** (`ActionOnDetect=Notify`).
- Le module Détection comportementale est entièrement administrable.
- Tous les autres modules de protection et de contrôle sont désactivés et inaccessibles à l'administration.

Lors de l'intégration à Kaspersky Endpoint Detection and Response Expert (on-premise) ou à Kaspersky Endpoint Detection and Response (KATA), dans le cadre d'une action de réponse aux menaces, Kaspersky Endpoint Security peut contrôler le lancement des fichiers exécutables et des scripts sur l'appareil. La fonctionnalité Prévention du lancement des objets est disponible avec les limitations suivantes :

- Si un script est exécuté depuis l'interpréteur, l'application n'a aucun contrôle sur le lancement du script.
- L'application ne contrôle pas l'ouverture des fichiers des applications Office sur l'appareil.

Distribution

Sur le site de Kaspersky vous pouvez télécharger les fichiers fournis avec l'application Kaspersky Endpoint Security, ainsi que les fichiers utilisés dans la procédure d'installation à distance de l'application à l'aide de Kaspersky Security Center.

Le paquet de l'application Kaspersky Endpoint Security comprend les fichiers suivants :

- kesl-12.4.0-<numéro de version>.i386.rpm, kesl-12.4.0-<numéro de version>_i386.deb

  Ils contiennent les principaux fichiers de l'application. Ces paquets peuvent être installés sur des systèmes d'exploitation de 32 bits conformément au type de gestionnaire de paquet.

- kesl-12.4.0-<numéro de version>.x86_64.rpm, kesl-12.4.0-<numéro de version>_amd64.deb

  Ils contiennent les principaux fichiers de l'application. Ces paquets peuvent être installés sur des systèmes d'exploitation de 64 bits conformément au type de gestionnaire de paquet.

- kesl-12.4.0-<numéro de version>.aarch64.rpm, kesl-12.4.0-<numéro de version>_arm64.deb

  Ils contiennent les principaux fichiers de l'application. Les paquets destinés au gestionnaire de paquets correspondant peuvent être installés sur des systèmes d'exploitation 64 bits pour l'architecture Arm®.

- kesl-gui-12.4.0-<numéro de version>.i386.rpm, kesl-gui-12.4.0-<numéro de version>_i386.deb

  Ils contiennent les fichiers de l'interface utilisateur graphique de l'application. Ces paquets peuvent être installés sur des systèmes d'exploitation de 32 bits conformément au type de gestionnaire de paquet.

- kesl-gui-12.4.0-<numéro de version>.x86_64.rpm, kesl-gui_12.4.0-<numéro de version>_amd64.deb

  Ils contiennent les fichiers de l'interface utilisateur graphique de l'application. Ces paquets peuvent être installés sur des systèmes d'exploitation de 64 bits conformément au type de gestionnaire de paquet.

- kesl-gui-12.4.0-<numéro de version>.aarch64.rpm, kesl-gui-12.4.0-<numéro de version>_arm64.deb

  Ils contiennent les fichiers de l'interface utilisateur graphique de l'application. Ces paquets peuvent être installés sur des systèmes d'exploitation de 64 bits pour l'architecture Arm conformément au type de gestionnaire de paquets.

- kesl-12.4.0.<numéro de version>.zip

  Contient les fichiers utilisés dans la procédure d'installation à distance de l'application à l'aide de Kaspersky Security Center, y compris les fichiers license.<identifiant de la langue> et ksn_license.<identifiant de la langue>.

  > L'Agent d'administration de Kaspersky Security Center n'est pas inclus dans le paquet. Vous pouvez le télécharger depuis la page de téléchargement des applications dans la section **Kaspersky Security Center**.

- ksn_license.<identifiant de langue>

  Contient le texte de la Déclaration de Kaspersky Security Network.

- license.<identifiant de langue>

  Contient le texte du Contrat de licence utilisateur final. Le Contrat de licence utilisateur final indique les conditions dans le cadre desquelles vous pouvez utiliser l'application.

Si vous décidez de modifier vous-même les fichiers de configuration de l'application d'une manière non décrite dans la documentation de l'application ou dans les recommandations des experts du Support technique, ces modifications pourraient entraîner des ralentissements et des pannes dans le fonctionnement de l'application et du système d'exploitation, une diminution du niveau de protection de votre appareil, une violation de la disponibilité et de l'intégrité des informations traitées ainsi que l'activation de l'envoi de statistiques complémentaires à KSN.

Configurations logicielles et matérielles

Cette section contient la configuration matérielle et logicielle requise pour Kaspersky Endpoint Security.

Exigences matérielles

L'application Kaspersky Endpoint Security requiert les configurations matérielles suivantes :

Configuration matérielle minimale requise

- Un processeur doté d'une architecture AMD64, de 2 GHz ou plus, comportant deux cœurs ou plus et prenant en charge les instructions SSE2.
- un secteur de pagination d'au moins 1 Go ;
- 2 Go de RAM disponible pour les applications pour les systèmes d'exploitation 64 bits (1 Go de RAM disponible pour les applications pour les systèmes d'exploitation 32 bits).
- 4 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;

  Un espace disque supplémentaire est nécessaire pour stocker les fichiers de traçage de l'application et les fichiers de vidage de l'application.

  Lors de l'analyse des archives et des objets composés, la Protection contre les fichiers malicieux et les tâches d'analyse nécessitent également un espace disque supplémentaire, dont la quantité dépend du type et de la taille décompressée de ces objets lorsque les paramètres `ScanArchived=Yes` et/ou `ScanSfxArchived=Yes` sont définis (par défaut, ces paramètres sont définis sur `Yes` pour les tâches d'analyse et sur `No` pour la Protection contre les fichiers malicieux).

  Il est recommandé de prévoir suffisamment d'espace dans le répertoire /tmp pour analyser les archives et les objets composés. Vous pouvez également limiter la taille des archives analysées (décompressées) à l'aide du paramètre `SizeLimit` pour chaque tâche.

- Lors de l'utilisation d'une interface graphique, le moniteur doit pouvoir afficher des fenêtres de 1 000 pixels de large et 600 pixels de haut (si la mise à l'échelle de l'écran est utilisée, ces dimensions sont également mises à l'échelle).

- Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, une interface réseau virtualisée avec une bande passante de 100 Mbit/s est requise.

Configuration matérielle minimale requise pour l'architecture Arm

- Processeur Armv8.2-A Kunpeng 920 ou Armv8-A Baikal-M (BE-M1000) ou la plateforme terminal m-TrusT.

- un secteur de pagination d'au moins 1 Go ;

- 2 Go de RAM disponibles pour l'application.

- 3 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;

  Un espace disque supplémentaire est nécessaire pour stocker les fichiers de traçage de l'application et les fichiers de vidage de l'application.

  Lors de l'analyse des archives et des objets composés, la Protection contre les fichiers malicieux et les tâches d'analyse nécessitent également un espace disque supplémentaire, dont la quantité dépend du type et de la taille décompressée de ces objets lorsque les paramètres `ScanArchived=Yes` et/ou `ScanSfxArchived=Yes` sont définis (par défaut, ces paramètres sont définis sur `Yes` pour les tâches d'analyse et sur `No` pour la Protection contre les fichiers malicieux).

  Il est recommandé de prévoir suffisamment d'espace dans le répertoire /tmp pour analyser les archives et les objets composés. Vous pouvez également limiter la taille des archives analysées (décompressées) à l'aide du paramètre `SizeLimit` pour chaque tâche.

- Lors de l'utilisation d'une interface graphique, le moniteur doit pouvoir afficher des fenêtres de 1 000 pixels de large et 600 pixels de haut (si la mise à l'échelle de l'écran est utilisée, ces dimensions sont également mises à l'échelle).

L'utilisation de Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels sur les systèmes d'exploitation pour l'architecture Arm n'est pas prise en charge.

Configuration logicielle

Pour installer Kaspersky Endpoint Security, l'un des systèmes d'exploitation suivants doit être installé sur l'appareil :

- Systèmes d'exploitation 32 bits pris en charge :

  - Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

- Systèmes d'exploitation 64 bits pris en charge :
  - AlmaLinux OS 8.6, 8.7, 8.8, 8.9
  - AlmaLinux OS 9.4, 9.5, 9.6
  - AlterOS® 2025.
  - Amazon™ Linux 2023
  - Astra Linux Common Edition 2.12
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)
  - Astra Linux Special Edition RUSB.10015-03 (operational update 7.6)
  - Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)
  - Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)
  - Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)

    Sur les appareils dotés des systèmes d'exploitation Astra Linux en modes de contrôle d'accès obligatoire et d'environnement logiciel fermé, l'utilisation de Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels n'est pas prise en charge.

  Le fonctionnement du système d'exploitation Astra sur une tablette en mode mobile n'est pris en charge que sous forme de bureau.

  - CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
  - CentOS Stream 8
  - CentOS Stream 9
  - CentOS Stream 10
  - Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
  - Debian GNU/Linux 13.0, 13.1, 13.2
  - EMIAS 1.0 ;
  - EulerOS 2.0 SP10
  - Fedora Linux 41

- Kylin Desktop OS V10 SP1.
- Linux Mint 21.3
- Linux Mint 22.2
- Mostech 12 release 2021.1
- openSUSE Leap 15.6
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9
- Oracle Linux 9.4, 9.5, 9.6
- Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9
- Red Hat Enterprise Linux 9.4, 9.5, 9.6
- Red Hat Enterprise Linux 10.0, 10.1
- Rocky Linux 8.6, 8.7, 8.8, 8.9
- Rocky Linux 9.4, 9.5, 9.6
- SberLinux 8.10, 9.1, 9.5, 9.6
- SberOS 3.4.0, 3.5.0
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS
- ALT Education 10
- ALT Education 11
- ALT Workstation 11
- ALT Server 11
- ALT SP Workstation version 10.
- ALT SP Server version 10
- Atlant, version Alcyone, 2022.02
- GosLinux 7.2.

- M OS 12 Server version 2021.1.
- MOS OS 15.5 Arbat
- MSVSphere 9.4 Workstation.
- SERVEUR MSVSPHERE 9.4 Server
- OS MESH 12 Pour tous les utilisateurs (sans télémétrie et sans support DIT) release 2021.1
- OS MESH 12 Pour les écoles de Moscou pour panneaux interactifs (avec télémétrie et support DIT) release 2021,1
- OS MESH 12 pour les écoles de Moscou pour ordinateurs et ordinateurs portables (avec télémétrie et support DIT) release 2021,1
- OSnova 2.14.
- OSnova 3.0.5
- RED OS® 7.3.
- RED OS 8.0
- ROSA « Cobalt » 7.9 Workstation
- ROSA « Cobalt » 7.9 Server
- ROSA « Chrome » 12 Workstation.
- ROSA « Chrome » 12 Server
- SynthesisM-Client 8.6
- SynthesisM-Serveur 8.6

- Systèmes d'exploitation 64 bits pour l'architecture Arm :
  - Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)
  - CentOS Stream 9
  - EulerOS 2.0 SP10
  - SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7
  - Ubuntu 22.04 LTS
  - ALT SP Workstation version 10
  - ALT SP Server version 10
  - RED OS 8.0

Sur les appareils dotés de systèmes d'exploitation pour l'architecture Arm, l'utilisation de Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels n'est pas prise en charge.

En raison des limitations techniques, l'application fanotify ne prend pas en charge les systèmes de fichiers suivants : autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, fuse, fuse.gvfsd-fuse, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

Configuration logicielle supplémentaire requise pour le mode Light Agent

L'application Kaspersky Endpoint Security peut être utilisé comme Light Agent dans le cadre de Kaspersky Security for Virtualization Light Agent version 6.4. Vous pouvez consulter les exigences relatives aux infrastructures virtuelles pour exécuter l'application en mode Light Agent dans l'aide de Kaspersky Security for Virtualization Light Agent.

Les machines virtuelles sur lesquelles Kaspersky Endpoint Security est installé en mode Light Agent sont soumises aux exigences logicielles et matérielles de l'application Kaspersky Endpoint Security, avec les limitations spécifiées.

Le BIOS de la machine virtuelle protégée doit prendre en charge la spécification SMBIOS version 2.1 ou ultérieure.

Les paquets suivants doivent être installés sur les machines virtuelles que vous souhaitez protéger, en fonction de l'infrastructure virtuelle sur laquelle Kaspersky Security for Virtualization Light Agent est déployé :

- Dans l'infrastructure Microsoft Hyper-V, le paquet des services d'intégration Integration Services doit être installé sur les machines virtuelles.
- Dans une infrastructure VMware vSphere, le paquet VMware Tools doit être installé sur les machines virtuelles.
- Dans l'infrastructure XenServer, XenTools doit être installé sur les machines virtuelles.
- Dans l'infrastructure HUAWEI FusionSphere, les machines virtuelles doivent avoir les outils HUAWEI installés.
- Dans l'infrastructure KVM, OpenStack, VK Private Cloud, TIONICS Cloud Platform, Astra Linux, ALT Virtualization Server, Basis.DynamiX et Basis Dynamix Standard, QEMU Guest Agent doit être installé sur les machines virtuelles.

Versions prises en charge de Kaspersky Security Center

L'application Kaspersky Endpoint Security est compatible avec les versions suivantes de Kaspersky Security Center :

- Kaspersky Security Center Windows 14, 14.2, 15.1 : Kaspersky Endpoint Security peut être administré via la Console d'administration à l'aide du plug-in d'administration MMC et via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web.

- Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2 : le plug-in Internet d'administration peut être utilisé pour administrer Kaspersky Endpoint Security via Kaspersky Security Center Web Console.

Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent), il est recommandé d'utiliser les versions suivantes de Kaspersky Security Center pour administrer l'application :

- Kaspersky Security Center Windows 14.2, 15.1.

- Kaspersky Security Center 15.4, 16.0, 16.1, 16.2.

Pour administrer l'application Kaspersky Endpoint Security via Kaspersky Security Center, l'Agent d'administration de Kaspersky Security Center est requis.

L'Agent d'administration de Kaspersky Security Center n'est pas inclus dans le kit de distribution de Kaspersky Endpoint Security. Vous pouvez le télécharger depuis la page de téléchargement des applications dans la section **Kaspersky Security Center**.

Si vous utilisez l'intégration des applications avec le module Kaspersky Endpoint Detection and Response de Kaspersky Anti Targeted Attack Platform, il est recommandé d'utiliser les versions suivantes de Kaspersky Security Center pour gérer l'application :

- Kaspersky Security Center Windows 14.2, 15.1.

- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Si vous utilisez l'intégration des applications avec le module Kaspersky Endpoint Detection and Response Optimum, il est recommandé d'utiliser les versions suivantes de Kaspersky Security Center pour gérer l'application :

- Kaspersky Security Center Windows 15.1.

- Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

Versions des solutions prises en charge sur les plate-formes KATA et OSMP

L'application Kaspersky Endpoint Security est compatible avec les versions suivantes des solutions de Kaspersky Anti Targeted Attack Platform :

- Kaspersky Anti Targeted Attack Platform 6.0 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) et Sandbox).
- Kaspersky Anti Targeted Attack Platform 6.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) et Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.0 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) et Sandbox).
- Kaspersky Anti Targeted Attack Platform 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA) et Sandbox).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA) et Sandbox).

Pour plus d'informations sur la solution Kaspersky Anti Targeted Attack Platform, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security est compatible avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0 sur Open Single Management Platform (ci-après également appelée OSMP).

Pour plus d'informations sur Kaspersky Endpoint Detection and Response Expert (on-premise) 8.0, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premise).

Nouveautés

Les nouveautés et les améliorations suivantes figurent dans l'application Kaspersky Endpoint Security :

- * Un nouveau module fonctionnel Protection contre les menaces par emails a été ajouté. Ce module analyse les pièces jointes des messages entrants et sortants à la recherche de virus et autres pièces jointes malveillantes.
- * Un nouveau module fonctionnel Protection BadUSB a été ajouté. Le module empêche la connexion des appareils USB infectés imitant des claviers à l'appareil client.
- Amélioration du module Contrôle des appareils. Il est désormais possible d'accorder un accès temporaire aux appareils bloqués à la demande de l'utilisateur.
- Le module Protection contre les Exploits a été amélioré. Vous pouvez désormais configurer des exclusions d'analyse spécifiques aux modules pour les objets.
- Le module de noyau mis à jour a été amélioré.
  - Le module de noyau mis à jour vous permet désormais d'optimiser l'interception des opérations sur les fichiers. Les performances de l'application sont améliorées grâce à l'utilisation d'un cache de fichiers et de processus ne nécessitant pas de vérification.
  - Avec le module de noyau mis à jour, vous pouvez désormais affiner les exclusions globales. Si le mécanisme d'interception basé sur fanotify est utilisé, les points de montage spécifiés sont entièrement exclus de l'interception des opérations sur les fichiers. Le module de noyau mis à jour vous permet d'exclure des répertoires locaux ou distants spécifiques montés sur l'appareil.
- Le module EDR (KATA), qui assure l'intégration avec Kaspersky Endpoint Detection and Response (KATA), a été renommé EDR Expert (OSMP). Ce module fournit également la tâche Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises). La tâche d'intégration a été renommée *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)* (KATAEDR, ID : 24).
- * L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) est réalisée : une solution de cybersécurité pour entreprises qui protège contre la plupart des cyber-risques et couvre les principaux scénarios de menaces. Les modules de Kaspersky Endpoint Detection and Response Expert (on-premises) sont déployés sur la plateforme de gestion unique Open Single Management Platform (OSMP). L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) prend en charge toutes les fonctionnalités de l'Intégration de Kaspersky Endpoint Detection and Response (KATA), ainsi que de nouvelles fonctionnalités :
  - Lancement de l'analyse YARA. Une *analyse YARA* est un processus au cours duquel Kaspersky Endpoint Security utilise des fichiers YARA pour rechercher des signatures d'activités malveillantes sur l'appareil.
  - Collecte de données forensiques : données numériques pouvant servir de preuves dans le cadre d'enquêtes sur des incidents liés à la cybercriminalité et aux fuites de données.
  - Envoi des données d'événements étendues (télémétrie) au serveur de collecte de télémétrie sur OSMP.
  - Envoi des données de télémétrie uniquement avec un indicateur d'attaque (Indicator of Attack, IOA). Vous pouvez désormais configurer des filtres personnalisés dans la stratégie de Web Console.

- Activation du module EDR Expert (OSMP), qui permet l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) et Kaspersky Endpoint Detection and Response (KATA), par l'ajout d'une clé de licence.

- Sélection du mode d'intégration dans les paramètres de la tâche *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)* via la ligne de commande ou dans les propriétés de la stratégie dans Web Console.

- L'application peut désormais être utilisée en mode Endpoint Detection and Response Agent, les solutions Detection and Response de Kaspersky et les applications antivirus tierces peuvent fonctionner conjointement sur les appareils protégés. Dans ce mode, les modules de protection et de contrôle standards de Kaspersky Endpoint Security ne sont pas utilisés pour protéger l'appareil. La protection standard de l'appareil est alors assurée par une application tierce.

- Ajout de la possibilité de créer des fichiers de traçage de l'application lors du premier lancement après l'installation. Vous pouvez désormais activer la création de fichiers de traçage lors du premier lancement de l'application dans Web Console, dans la Console d'administration ou dans les paramètres du fichier de configuration de l'installation initiale.

- L'interface de la stratégie dans Web Console a été mise à jour. La structure des sections dans la stratégie a été modifiée pour faciliter la recherche des fonctions nécessaires.

- Ajout de la possibilité de sélectionner le mode d'interception du trafic utilisé par l'application : eBPF ou l'utilitaire iptables.

- Ajout de la possibilité de sélectionner une source de télémétrie (eBPF uniquement ou eBPF et auditd). Pour auditd, vous pouvez également sélectionner le mode de fonctionnement (mode exclusif ou mode multicast).

- Désormais, vous pouvez sélectionner le mode d'envoi des fichiers et des répertoires vers la sandbox pour analyse : manuel, automatique uniquement, automatique et manuel.

- Les fonctionnalités de l'application ont été étendues lors de l'utilisation en mode Light Agent :

  - Un mécanisme d'interception des événements système basé sur le module de noyau mis à jour est disponible.

  - Le module fonctionne Prévention des Exploits est disponible.

  - Le niveau de détection des menaces est amélioré.

- Ajout de la possibilité d'utiliser Kaspersky Private Security Network (KPSN) directement, sans passer par le service proxy KSN sur le Serveur d'administration.

- Il est désormais possible de créer des stratégies pour les utilisateurs autonomes dans Web Console et la Console d'administration. Ces stratégies sont appliquées lorsque l'appareil quitte le réseau d'organisation.

- Lors de l'affichage et de l'exportation de la liste des points de montage dans Web Console ou dans la Console d'administration, ou lors de l'affichage de cette liste via la ligne de commande, les informations indiquant que le point de montage a été trouvé dans un espace de noms sont désormais également affichées.

- Ajout d'un mécanisme alternatif pour recevoir la télémétrie système dans le module Détection comportementale sur les systèmes d'exploitation 64 bits avec la version du noyau 4.18 et supérieure avec prise en charge d'eBPF, qui vous permet de libérer les ressources du sous-système d'audit du noyau auditd.

- Ajout de la possibilité d'inclure les informations suivantes dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response :
  - indicateur précisant que l'événement s'est produit dans un conteneur ;
  - identifiant de l'espace de noms du conteneur ;
  - nom du conteneur.
- La liste des systèmes d'exploitation pris en charge est mise à jour.

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 le plug-in web 12.4.0.8289

Identifiant	Description
10724878	Lors de l'application de la stratégie à l'appareil, la valeur `RestartServiceManually` a été utilisée pour la configuration de `InterceptorApplyStrategy`, au lieu de la valeur par défaut, `RestartServiceAutomatically`.

Préparation à l'installation de l'application Kaspersky Endpoint Security

Actions générales

Avant de lancer l'installation de l'application Kaspersky Endpoint Security, vous devez effectuer les opérations suivantes :

- Vérifiez que votre appareil répond aux exigences matérielles et logicielles de l'application.
- Assurez-vous qu'aucun logiciel antivirus tiers n'est installé sur votre appareil.
- Assurez-vous que l'application Kaspersky Endpoint Agent for Linux n'est pas installée sur votre appareil. Si Kaspersky Endpoint Agent for Linux est installé, un message s'affiche lors de l'installation et vous invite à le désinstaller manuellement.
- Si vous prévoyez de gérer l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, effectuez les étapes préparatoires pour installer l'Agent d'administration de Kaspersky Security Center sur l'appareil (pour plus de détails, consultez l'aide de Kaspersky Security Center).

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, Kaspersky Security Center est requis pour gérer l'application.

- Si vous souhaitez utiliser le système de contrôle d'accès SELinux, vous devez vous assurer que l'utilitaire semanage est installé sur votre système d'exploitation. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.
- Si vous souhaitez utiliser une interface utilisateur graphique, vous devez vous assurer que les dépendances nécessaires à l'installation du paquet de l'interface graphique sont disponibles sur votre appareil. Si l'appareil se trouve dans une boucle réseau fermée et n'a pas accès aux répertoires du gestionnaire de paquets, il est recommandé de vérifier la liste des dépendances sur l'appareil de référence (libice6, libsm6, libx11-6, libx11-xcb1, libxcb-icccm4, libxcb-image0, libxcb-keysyms1, libxcb-randr0, libxcb-render-util0, libxcb-render0, libxcb-shape0, libxcb-shm0, libxcb-sync1, libxcb-xfixes0, libxcb-xinerama0, libxcb-xkb1, libxcb1, libxi6, libxml2, zlib1g), puis de télécharger et de distribuer les paquets à tous les appareils avant d'installer l'interface graphique.
- Si vous souhaitez utiliser l'interface utilisateur graphique, vous devez vous assurer que l'utilitaire Zenity est installé sur le système d'exploitation.
- Sur les appareils dotés de systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, assurez-vous que les éléments suivants sont installés :
  - paquets pour compiler des applications et exécuter des tâches (gcc, binutils, glibc, glibc-devel, make) ;
  - Paquet contenant les fichiers d'en-tête du noyau du système d'exploitation pour la compilation des modules de Kaspersky Endpoint Security
- Sur un appareil sous SUSE Linux Enterprise Server 15, installez le paquet insserv-compat.

- Dans les systèmes d'exploitation Astra Linux, la fonction d'interdiction du traçage ptrace (Disable ptrace capability) est activée par défaut, ce qui peut affecter le fonctionnement de l'application Kaspersky Endpoint Security. Pour un fonctionnement correct de Kaspersky Endpoint Security, il est recommandé de désactiver l'interdiction de traçage ptrace lors de l'installation d'Astra Linux. Si Astra Linux est déjà installé, consultez le site Web du centre d'aide Astra Linux pour obtenir des instructions sur l'activation et la désactivation de ce mode (**Configuration des mécanismes de protection et de blocage**, section **Blocage des traçages ptrace**).

  Vous pouvez désactiver le traçage ptrace en spécifiant la paire paramètre-valeur du noyau `kernel.yama.ptrace_scope=3`. Ensuite, ce qui suit se produira dans l'application :

  - Il ne sera pas possible de créer des fichiers de vidage du processus kesl lorsque l'application échoue.
  - Le module Détection comportementale ne pourra pas récupérer les paramètres d'environnement du processus.
  - Sur les systèmes d'exploitation avec des versions de noyau supérieures à 5.7, le module Contrôle des applications ne pourra pas lire les arguments de la ligne de commande et traiter les variables d'environnement, car la lecture de /proc/pid/syscall, /proc/pid/mem est interdite. Sur les systèmes d'exploitation dotés de la version de noyau 5.0, le module Contrôle des applications ne fonctionnera pas correctement.
  - La vérification de la mémoire du processus et de la mémoire du noyau dans les tâches de vérification ne fonctionnera pas, car la lecture de /proc/pid/mem est interdite.
  - La vérification de la mémoire YARA des processus en mode de contrôle d'accès obligatoire n'est pas garantie, car la lecture de /proc/pid/mem est interdite.

- Pour que les tâches Gestion du pare-feu, Protection contre les menaces Internet et Protection contre les menaces réseau fonctionnent, vous devez installer le paquet de l'utilitaire iptables sur votre appareil.

- Pour que le Plug-in d'administration MMC de Kaspersky Endpoint Security fonctionne, Microsoft® Visual C++® 2015 Redistributable Update 3 RC (voir https://www.microsoft.com/en-us/download/details.aspx?id=52685) doit être installé sur l'appareil sur lequel le Serveur d'administration de Kaspersky Security Center est installé.

- Pour lancer et faire fonctionner correctement l'application, vous devez vous assurer que le compte root est le propriétaire des répertoires suivants et que seul le propriétaire y a accès en écriture : /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

- Assurez-vous que le système d'exploitation est configuré avec les restrictions de descripteur de fichier recommandées par le fabricant du système d'exploitation. Pour vérifier la limite, exécutez la commande `cat /proc/sys/fs/file-max`. Lorsque l'application est en cours d'exécution, la consommation de descripteurs dans le système d'exploitation peut augmenter considérablement. En général, il est recommandé de désactiver la limite de fichiers en définissant le paramètre `fs.file-max=9223372036854775807` dans le fichier /etc/sysctl.conf. Après avoir modifié la valeur de ce paramètre, vous devez redémarrer le système d'exploitation.

Étapes supplémentaires avant d'installer Kaspersky Endpoint Security en mode Light Agent

Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent), vous devez en outre effectuer les étapes suivantes avant d'installer l'application Kaspersky Endpoint Security :

- Assurez-vous que les machines virtuelles que vous souhaitez protéger répondent aux exigences générales du mode Light Agent.

- Assurez-vous que les paramètres de l'équipement réseau ou du logiciel qui contrôle le trafic entre les machines virtuelles permettent au trafic réseau de passer par les ports utilisés pour l'interaction entre l'application Kaspersky Endpoint Security en mode Light Agent et les autres modules de Kaspersky Security for Virtualization Light Agent. Les ports utilisés par le Light Agent sont répertoriés dans l'aide de Kaspersky Security for Virtualization Light Agent.

Installation et configuration initiale de l'application Kaspersky Endpoint Security

Avant de lancer l'installation de l'application Kaspersky Endpoint Security, vous devez réaliser les préparatifs d'installation.

Les scénarios ci-dessus décrivent comment procéder à l'installation et à la configuration initiale de Kaspersky Endpoint Security, à l'installation de l'Agent d'administration de Kaspersky Security Center ainsi qu'à l'installation des plug-ins d'administration de Kaspersky Endpoint Security. Le scénario d'installation dépend du mode dans lequel vous envisagez d'utiliser l'application Kaspersky Endpoint Security.

Une fois Kaspersky Endpoint Security installé, il n'est pas possible de modifier le mode d'utilisation de l'application.

Mode standard

Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode standard, la procédure d'installation de l'application comprend les étapes suivantes :

1. **Installation et configuration initiale de l'Agent d'administration**

   Si vous prévoyez d'administrer l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, installez l'Agent d'administration de Kaspersky Security Center sur l'appareil protégé et configurez ses paramètres.

2. **Installation du plug-in d'administration de Kaspersky Endpoint Security**

   Si vous envisagez d'administrer l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, installez le plug-in d'administration de Kaspersky Endpoint Security. En fonction de la Console d'administration de Kaspersky Security Center, les plug-ins d'administration suivants sont utilisés :

   - Le plug-in Internet d'administration de Kaspersky Endpoint Security vous permet d'administrer le fonctionnement de l'application via Kaspersky Security Center Cloud Console et Kaspersky Security Center Web Console. Le plug-in Internet est installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée.

   - Le plug-in d'administration MMC de Kaspersky Endpoint Security vous permet d'administrer l'application à l'aide de la Console d'administration de Kaspersky Security Center. Le plugin MMC est installé sur l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center.

3. **Installation des paquets de l'application et de l'interface utilisateur graphique**

   Kaspersky Endpoint Security est distribué sous forme de paquets aux formats DEB et RPM. Il existe des paquets distincts pour l'application et l'interface graphique de l'application. Installez Kaspersky Endpoint Security et, si nécessaire, l'interface graphique depuis les paquets au format nécessaire.

   Vous pouvez procéder à l'installation de l'une des manières suivantes :

   - À l'aide de Kaspersky Security Center.

   - Via la ligne de commande.

4. **Configuration initiale de Kaspersky Endpoint Security**

   Une configuration initiale est requise pour préparer l'application à l'utilisation et activer la protection de l'appareil client.

   Si vous avez installé l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, la configuration initiale a été effectuée automatiquement lors de l'installation conformément aux paramètres spécifiés dans le paquet d'installation. Une fois l'installation terminée, préparez l'application pour l'utiliser.

   Si vous avez installé l'application Kaspersky Endpoint Security à partir de la ligne de commande, une fois l'installation terminée, lancez l'Assistant de configuration initiale et effectuez la configuration initiale en mode interactif ou en mode automatique.

   Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

Mode Light Agent

L'utilisation de Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels sur les systèmes d'exploitation pour l'architecture Arm n'est pas prise en charge.

Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, la procédure d'installation de l'application comprend les étapes suivantes :

1. **Installation et configuration initiale de l'Agent d'administration**

   Installez l'Agent d'administration de Kaspersky Security Center sur les machines virtuelles et les modèles de machines virtuelles et configurez ses paramètres.

   Si vous installez l'Agent d'administration sur un modèle à partir duquel des machines virtuelles temporaires seront créées, il est recommandé de configurer les paramètres qui vous permettent d'optimiser les performances sur les machines virtuelles temporaires. Pour plus d'informations sur l'installation de machines virtuelles sur un modèle, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

2. **Installation du plug-in d'administration de Kaspersky Endpoint Security**

   Installez le plug-in d'administration de Kaspersky Endpoint Security. En fonction de la Console d'administration de Kaspersky Security Center, les plug-ins d'administration suivants sont utilisés :

   - Le plug-in Internet d'administration de Kaspersky Endpoint Security vous permet d'administrer le fonctionnement de l'application via Kaspersky Security Center Cloud Console et Kaspersky Security Center Web Console. Le plug-in Internet est installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée.

   - Le plug-in d'administration MMC de Kaspersky Endpoint Security vous permet d'administrer l'application à l'aide de la Console d'administration de Kaspersky Security Center. Le plugin MMC est installé sur l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center.

3. **Installation des paquets de l'application et configuration initiale de Kaspersky Endpoint Security**

   Kaspersky Endpoint Security est distribué sous forme de paquets aux formats DEB et RPM. Installez Kaspersky Endpoint Security à partir d'un paquet au format requis. Il existe des paquets distincts pour l'application et l'interface graphique de l'application.

L'interface graphique de l'application n'est pas prise en charge si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Vous pouvez installer l'application de l'une des manières suivantes :

- À l'aide de Kaspersky Security Center.

  Avant de démarrer l'installation, vous devez spécifier les paramètres de configuration initiaux de l'application dans les paramètres du paquet d'installation ou dans le fichier de configuration inclus dans le paquet d'installation.

  Vous devez sélectionner le mode Light Agent (paramètre `KSVLA_MODE=Yes` dans le fichier de configuration). Si vous installez Kaspersky Endpoint Security sur un modèle à partir duquel seront créées les machines virtuelles temporaires, il est recommandé d'activer également le mode de protection de l'infrastructure VDI pour optimiser le fonctionnement de l'application sur les machines virtuelles temporaires (paramètre `VDI_MODE=Yes` dans le fichier de configuration).

  Les valeurs des paramètres sont sensibles à la casse.

- Via la ligne de commande. Si vous installez à l'aide de la ligne de commande, vous sélectionnez la manière dont vous souhaitez utiliser l'application lors de la configuration initiale de l'application en mode interactif ou automatique.

4. **Configuration initiale de Kaspersky Endpoint Security**

Une configuration initiale est requise pour préparer l'application à l'utilisation et activer la protection de l'appareil client.

Si vous avez installé l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, la configuration initiale a été effectuée automatiquement lors de l'installation conformément aux paramètres spécifiés dans le paquet d'installation. Une fois l'installation terminée, préparez l'application pour l'utiliser.

Si vous avez installé l'application Kaspersky Endpoint Security à partir de la ligne de commande, une fois l'installation terminée, lancez l'Assistant de configuration initiale et effectuez la configuration initiale en mode interactif ou en mode automatique. Lors de la configuration initiale, vous devez sélectionner le mode Light Agent de l'une des manières suivantes :

- Saisissez `yes` à l'étape "Utilisation de l'application en mode Light Agent" dans l'Assistant de configuration initiale.

- Définissez le paramètre `KSVLA_MODE=Yes` dans le fichier de configuration d'installation initiale.

  La valeur du paramètre est sensible à la casse.

Si vous installez l'application Kaspersky Endpoint Security sur un modèle à partir duquel des machines virtuelles temporaires seront créées, il est recommandé de configurer également un paramètre permettant d'optimiser les performances sur les machines virtuelles temporaires. Pour plus d'informations sur l'installation de machines virtuelles sur un modèle, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

Mode Endpoint Detection and Response Agent

Il est recommandé d'installer ce module après avoir installé les applications antivirus tierces sur l'appareil.

Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent pour protéger les environnements virtuels, la procédure d'installation de l'application comprend les étapes suivantes :

1. **Installation et configuration initiale de l'Agent d'administration**

   Si vous prévoyez d'administrer l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, installez l'Agent d'administration de Kaspersky Security Center sur l'appareil protégé et configurez ses paramètres.

2. **Installation du plug-in d'administration de Kaspersky Endpoint Security**

   Si vous envisagez d'administrer l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, installez le plug-in d'administration de Kaspersky Endpoint Security. En fonction de la Console d'administration de Kaspersky Security Center, les plug-ins d'administration suivants sont utilisés :

   - Le plug-in Internet d'administration de Kaspersky Endpoint Security vous permet d'administrer le fonctionnement de l'application via Kaspersky Security Center Cloud Console et Kaspersky Security Center Web Console. Le plug-in Internet est installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée.

   - Le plug-in d'administration MMC de Kaspersky Endpoint Security vous permet d'administrer l'application à l'aide de la Console d'administration de Kaspersky Security Center. Le plugin MMC est installé sur l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center.

3. **Installation des paquets de l'application et configuration initiale de Kaspersky Endpoint Security**

   Kaspersky Endpoint Security est distribué sous forme de paquets aux formats DEB et RPM. Installez Kaspersky Endpoint Security à partir d'un paquet au format requis. Il existe des paquets distincts pour l'application et l'interface graphique de l'application.

   Vous pouvez installer l'application de l'une des manières suivantes :

   - À l'aide de Kaspersky Security Center.

     Avant de démarrer l'installation, vous devez spécifier les paramètres de configuration initiaux de l'application dans les paramètres du paquet d'installation ou dans le fichier de configuration inclus dans le paquet d'installation.

     Vous devez sélectionner le mode Endpoint Detection and Response Agent (dans le fichier de configuration : paramètre `ENDPOINT_AGENT_MODE=Yes`).

     La valeur du paramètre est sensible à la casse.

   - Via la ligne de commande. Si vous installez à l'aide de la ligne de commande, vous sélectionnez la manière dont vous souhaitez utiliser l'application lors de la configuration initiale de l'application en mode interactif ou automatique.

4. **Configuration initiale de Kaspersky Endpoint Security**

   Une configuration initiale est requise pour préparer l'application à l'utilisation et activer la protection de l'appareil client.

Si vous avez installé l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, la configuration initiale a été effectuée automatiquement lors de l'installation conformément aux paramètres spécifiés dans le paquet d'installation. Une fois l'installation terminée, préparez l'application pour l'utiliser.

Si vous avez installé l'application Kaspersky Endpoint Security à partir de la ligne de commande, une fois l'installation terminée, lancez l'Assistant de configuration initiale et effectuez la configuration initiale en mode interactif ou en mode automatique. Lors de la configuration initiale, vous devez sélectionner le mode Endpoint Detection and Response Agent de l'une des manières suivantes :

- Saisissez `yes` à l'étape "Utilisation de l'application en mode Endpoint Detection and Response Agent" dans l'Assistant de configuration initiale.
- Définissez le paramètre `ENDPOINT_AGENT_MODE=Yes` dans le fichier de configuration d'installation initiale.

  La valeur du paramètre est sensible à la casse.

Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

Installation et configuration initiale de l'Agent d'administration de Kaspersky Security Center

L'Agent d'administration assure la communication entre l'appareil client et le Serveur d'administration de Kaspersky Security Center. Par conséquent, il doit être installé sur chaque appareil client qui sera connecté au système de gestion centralisée à distance de Kaspersky Security Center.

Avant de commencer l'installation de l'Agent d'administration sur des appareils dotés de systèmes d'exploitation Linux, vous devez effectuer certaines étapes préparatoires. Pour obtenir une description de la préparation des appareils pour l'installation de l'Agent d'administration, consultez l'aide de Kaspersky Security Center. L'ensemble des actions nécessaires dépend du système d'exploitation.

Vous pouvez installer et effectuer la configuration initiale de l'Agent d'administration :

- À distance depuis le poste de travail de l'administrateur à l'aide de Kaspersky Security Center Web Console ou à l'aide de la Console d'administration. Pour une installation à distance, utilisez le paquet d'installation de l'Agent d'administration.
- En utilisant la ligne de commande :
  - En mode silencieux avec le fichier de réponse. Un fichier de réponses est un fichier texte contenant un ensemble personnalisé de paramètres pour l'installation et la configuration initiale de l'Agent d'administration. Pour une description des paramètres d'installation et de la configuration initiale de l'Agent d'administration, consultez l'aide de Kaspersky Security Center (section « Installation de l'Agent d'administration pour Linux en mode silencieux (avec fichier de réponses) »).
  - De manière interactive à partir d'un paquet RPM ou DEB selon le type de gestionnaire de paquets. Dans ce cas, après l'installation, vous devez effectuer la configuration initiale de l'Agent d'administration à l'aide d'un script.

Pour plus d'informations sur l'installation de l'Agent d'administration, consultez l'aide de Kaspersky Security Center.

Installation des plug-ins d'administration de Kaspersky Endpoint Security

Les plug-ins d'administration suivants de Kaspersky Endpoint Security permettent d'administrer Kaspersky Endpoint Security à l'aide de Kaspersky Security Center :

- le plug-in Internet d'administration de Kaspersky Endpoint Security vous permet de gérer l'application via Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console ;
- Le plug-in MMC d'administration de Kaspersky Endpoint Security vous permet d'administrer le fonctionnement de l'application via la Console d'administration de Kaspersky Security Center.

Vous pouvez installer simultanément des plug-ins de gestion pour différentes versions de l'application Kaspersky Endpoint Security. De cette façon, vous pourrez administrer l'application en utilisant des stratégies créées avec différentes versions du plug-in d'administration.

Si vous utilisez la Console d'administration de Kaspersky Security Center pour gérer l'application, vous pouvez également convertir les stratégies et les tâches créées à l'aide des versions précédentes du plug-in d'administration vers les nouvelles versions.

Installation du plug-in Internet de Kaspersky Endpoint Security

Le plug-in Internet d'administration de Kaspersky Endpoint Security doit être installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée. La fonctionnalité du plug-in Internet est disponible pour tous les administrateurs qui ont accès à Kaspersky Security Center Web Console dans un navigateur.

Vous pouvez installer le plug-in Internet selon un des moyens suivants :

- À l'aide de l'Assistant de configuration initiale de Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console vous invite automatiquement à exécuter l'assistant de configuration initiale lors de la première connexion de Kaspersky Security Center Web Console au Serveur d'administration. Vous pouvez également exécuter l'assistant de configuration initiale dans l'interface de Kaspersky Security Center Web Console (**Découverte et déploiement des appareils → Déploiement et attribution → Assistant de configuration initiale**). 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 Kaspersky Security Center Web Console, consultez l'aide de Kaspersky Security Center.

- Manuellement, à l'aide d'une distribution de la liste des plugins Web de Kaspersky ou d'une source tierce.

Pour installer manuellement le plug-in Internet de Kaspersky Endpoint Security :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Paramètres → Plug-ins Web**.

   Une liste des plug-ins Internet installés s'ouvrira.

2. Commencez à installer le plug-in Web de Kaspersky Endpoint Security de l'une des manières suivantes :

- Installation à partir de la liste des plug-ins Web de Kaspersky :

  a. Cliquez sur le bouton **Ajouter**.

  Une liste de tous les plug-ins Web de Kaspersky disponibles s'ouvrira. La liste est mise à jour automatiquement lorsque de nouvelles versions de plug-ins Web sont publiées.

  b. Recherchez le plug-in Web de **Kaspersky Endpoint Security <numéro de version> for Linux** dans la liste et cliquez sur son nom.

  c. Dans la fenêtre qui s'ouvre avec une description du plug-in Web, cliquez sur le bouton **Installer le plug-in**.

  d. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

  e. La fenêtre **Configuration du plug-in Internet** s'ouvre.

  > Dans Kaspersky Security Center Web Console version 14.2, vous devez actualiser la page du navigateur pour que la fenêtre **« Configuration du plug-in Internet »** s'ouvre.

  f. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

- Installation d'un plug-in Internet à partir d'une source tierce (les archives nécessaires à l'installation des plug-ins Internet sont incluses dans le kit de distribution ou peuvent être téléchargées depuis le site de Kaspersky) :

  a. Cliquez sur le bouton **Ajouter à partir d'un fichier**.

  b. Dans la fenêtre qui s'ouvre, précisez le chemin d'accès à l'archive ZIP avec la distribution du plug-in Web et le chemin d'accès au fichier signé au format TXT. Ce fichier se trouve dans l'archive avec le plug-in Web.

  c. Cliquez sur le bouton **Ajouter**.

  d. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

  e. La fenêtre **Configuration du plug-in Internet** s'ouvre.

  > Dans Kaspersky Security Center Web Console version 14.2, vous devez actualiser la page du navigateur pour que la fenêtre **« Configuration du plug-in Internet »** s'ouvre.

  f. Attendez la fin de l'installation et cliquez sur le bouton **OK** dans la fenêtre d'informations.

Le nouveau plug-in apparaît dans la liste des plug-ins Web installés (**Paramètres** → **Plug-ins Web**).

> Si, dans les propriétés du Serveur d'administration de Kaspersky Security Center, vous avez sélectionné une langue qui n'est pas incluse dans le kit de distribution de l'application Kaspersky Endpoint Security, le Contrat de licence utilisateur final et toute l'interface de Kaspersky Security Center Web Console seront affichés en anglais.

Installation du plug-in MMC de Kaspersky Endpoint Security

Le plug-in MMC d'administration de Kaspersky Endpoint Security doit être installé sur l'appareil où la Console d'administration de Kaspersky Security Center a été installée.

Avant d'installer le plug-in MMC d'administration de Kaspersky Endpoint Security, il faut s'assurer que Kaspersky Security Center et Redist C ++ 2015 (Microsoft Visual C ++ 2015 Redistributable) sont installés.

Pour installer le plug-in MMC :

Sur l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center, exécutez le fichier exécutable klcfginst.msi.

Le fichier est inclus dans le kit de distribution de l'application Kaspersky Endpoint Security.

Après l'installation, le plug-in MMC d'administration s'affiche dans la liste des plug-ins MMC d'administration installés dans les propriétés du Serveur d'administration de Kaspersky Security Center.

Pour afficher la liste des plug-ins MMC d'administration installés :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le **nœud Serveur d'administration <nom du serveur>** et ouvrez la fenêtre des propriétés du Serveur d'administration de l'une des manières suivantes :

   - à l'aide de l'élément **Propriétés** du menu contextuel du nœud du **Serveur d'administration <nom du serveur>** ;

   - en cliquant sur le lien **Propriétés du Serveur d'administration** situé dans la zone de travail du nœud **Serveur d'administration <nom du serveur>** dans le groupe **Serveur d'administration**.

2. Dans la liste de gauche, dans la section **Avancés**, sélectionnez la section **Informations sur les plug-ins d'administration installés des applications**.

   Dans la partie droite de la fenêtre, la liste des plug-ins d'administration installés affiche le plug-in MMC d'administration de Kaspersky Endpoint Security : **Kaspersky Endpoint Security <numéro de version> for Linux**.

Installation et configuration initiale de l'application à l'aide de Kaspersky Security Center

Vous pouvez installer l'application Kaspersky Endpoint Security sur un appareil client à distance depuis le poste de travail de l'administrateur à l'aide de Kaspersky Security Center Web Console ou de la Console d'administration.

L'installation à l'aide de Kaspersky Security Center comprend les étapes suivantes :

1. Création d'un paquet d'installation.

Le paquet d'installation de l'application de Kaspersky Endpoint Security est utilisé pour effectuer l'installation à distance. Le paquet d'installation de Kaspersky Endpoint Security est commun à tous les systèmes d'exploitation et types d'architecture de processeur pris en charge. Vous pouvez créer un paquet d'installation à l'aide de Kaspersky Security Center Web Console ou à l'aide de la Console d'administration.

Vous pouvez spécifier les paramètres de configuration initiaux de l'application dans les propriétés du paquet d'installation ou dans le fichier de configuration autoinstall.ini inclus dans le paquet d'installation.

Vous devez configurer les paramètres initiaux de l'application si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent) ou en mode Endpoint Detection and Response Agent. Par défaut, l'application est utilisée en mode standard.

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent, lors de la création du paquet d'installation, vous pouvez ajouter au paquet :

- clé de licence pour activer automatiquement l'application lors de l'installation ;
- bases de données pré-téléchargées de l'application, afin de ne pas mettre à jour en plus les bases de données après l'installation.

Vous pouvez également activer l'application et mettre à jour les bases de données ultérieurement tout en préparant l'application à l'utilisation.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation de l'application lors de l'installation et la distribution automatique des clés de licence ne sont pas prises en charge. Kaspersky Endpoint Security reçoit les informations de licence du Serveur de protection après la connexion à la SVM ; Kaspersky Endpoint Security n'a pas besoin d'être activé séparément.

2. Déploiement de l'application Kaspersky Endpoint Security sur les appareils du réseau de l'organisation.

   Kaspersky Security Center Web Console prend en charge les principales méthodes de déploiement suivantes :

   - Installation de l'application à l'aide de l'assistant de déploiement de protection.
   - Installation de l'application à l'aide de la tâche d'installation à distance de l'application.

   La Console d'administration de Kaspersky Security Center prend en charge les principales méthodes de déploiement suivantes :

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

   Pour une description des procédures de déploiement, consultez l'aide de Kaspersky Security Center.

   Si nécessaire, vous pouvez consulter le journal d'installation à distance de l'application à l'aide du diagnostic à distance de l'appareil client de Kaspersky Security Center.

3. Préparation de l'application pour utilisation.

   Avant de commencer à utiliser l'application, vous devez terminer la configuration initiale de l'application et préparer l'application à l'utilisation.

Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

Pour administrer le fonctionnement de l'application Kaspersky Endpoint Security installée sur les appareils clients à l'aide de Kaspersky Security Center, vous devez placer ces appareils dans des groupes d'administration. Avant de lancer l'installation de l'application Kaspersky Endpoint Security, vous pouvez créer dans Kaspersky Security Center des groupes d'administration où vous placerez les appareils dotés de l'application et configurer des règles automatiques de déplacements des appareils vers les groupes d'administration. Si les règles de déplacement des appareils vers les groupes d'administration ne sont pas configurées, Kaspersky Security Center place tous les appareils sur lesquels l'Agent d'administration est installé et connecté au Serveur d'administration dans la liste **Appareils non attribués**. Dans ce cas, vous devez déplacer manuellement les appareils vers les groupes d'administration (pour les détails, consultez l'aide de Kaspersky Security Center).

Création d'un paquet d'installation dans Web Console

Dans Kaspersky Security Center Web Console, vous pouvez créer un paquet d'installation de l'une des manières suivantes :

- À partir du fichier d'archive que vous avez préalablement préparé.
- À partir d'un paquet de distribution hébergé sur les serveurs de Kaspersky.

Si vous prévoyez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels ou en mode Endpoint Detection and Response Agent, vous devez spécifier le mode d'utilisation de l'application dans les paramètres de configuration initiale. Vous pouvez spécifier les paramètres de configuration initiale de l'application dans les propriétés du paquet d'installation créé sous l'onglet **Paramètres** ou dans le fichier de configuration inclus dans le paquet d'installation.

Pour préparer un fichier d'archive pour créer un paquet d'installation :

1. Téléchargez l'archive kesl.zip depuis la page de téléchargement de l'application. Elle se trouve dans **Kaspersky Endpoint Security for Linux** (**Distribution complémentaire → Fichiers pour l'installation à distance du produit**).
2. Décompressez l'archive kesl.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center. Placez dans ce même dossier les fichiers de la distribution qui correspondent au type de système d'exploitation sur lequel vous souhaitez installer l'application, ainsi que le type de gestionnaire de paquets sur celui-ci :
   - Pour installer Kaspersky Endpoint Security :
     - kesl-12.4.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
     - kesl_12.4.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
     - kesl-12.4.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
     - kesl-12.4.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)

- kesl-12.4.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
- kesl_12.4.0-<numéro de version>_arm64.deb (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec dpkg)

- Pour installer l'interface graphique de l'application :
  - kesl-gui-12.4.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
  - kesl-gui-12.4.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
  - kesl-gui-12.4.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
  - kesl-gui-12.4.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)
  - kesl-gui-12.4.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
  - kesl-gui_12.4.0-<numéro de version>_arm64.deb (pour système d'exploitation 64 bits pour l'architecture Arm avec dpkg)

  Si vous ne souhaitez pas installer l'interface graphique, n'utilisez pas ces fichiers. La taille du paquet d'installation sera alors inférieure.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'interface utilisateur graphique n'est pas prise en charge.

Si vous ne prévoyez pas d'installer l'interface graphique, vous devez la désactiver en définissant le paramètre approprié dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini (`USE_GUI=No`). Dans le cas contraire, l'installation se terminera par une erreur.

Si vous souhaitez utiliser le paquet d'installation que vous créez pour différents systèmes d'exploitation ou différents gestionnaires de paquets, placez les fichiers pour tous les types de systèmes d'exploitation et gestionnaires de paquets nécessaires dans le dossier.

3. Si vous prévoyez d'utiliser l'application Kaspersky Endpoint Security en mode standard et souhaitez utiliser les bases de données pré-téléchargées de l'application :
   a. Placez les archives préparées avec les bases de données pour tous les types de systèmes d'exploitation requis dans le dossier.
   b. Dans les paramètres de configuration initiale de l'application, désactivez le lancement de la tâche de mise à jour de la base de données après l'installation de l'application. Vous pouvez configurer le paramètre approprié dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini (`UPDATE_EXECUTE=No`). Le fichier autoinstall.ini se trouve dans le dossier où vous avez extrait l'archive kesl.zip.
4. Si vous souhaitez configurer les paramètres de configuration initiale de l'application à l'aide d'un fichier de configuration, ouvrez le fichier de configuration autoinstall.ini et apportez les modifications nécessaires.

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, vous devez établir la valeur du paramètre `KSVLA_MODE=Yes` dans le fichier de configuration autoinstall.ini.

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, vous devez établir la valeur du paramètre `ENDPOINT_AGENT_MODE=Yes` dans le fichier de configuration autoinstall.ini.

Les valeurs des paramètres dans le fichier autoinstall.ini sont sensibles à la casse.

Vous pouvez également configurer les paramètres de configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé dans l'onglet **Paramètres**.

5. Placez tous les fichiers préparés dans une archive ZIP, CAB, TAR ou TAR.GZ avec un nom arbitraire.

Pour créer un paquet d'installation de Kaspersky Endpoint Security dans Kaspersky Security Center Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez l'une des sections suivantes :

   - **Découverte et déploiement des appareils → Déploiement et attribution → Paquets d'installation**.
   - **Opérations → Stockages → Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

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

   L'Assistant de création du paquet d'installation démarre.

3. Sélectionnez un mode de création d'un paquet d'installation :

   - **Créez un paquet d'installation à partir d'un fichier**. Le paquet d'installation sera créé à partir du fichier d'archive que vous avez préalablement préparé. Vous devez sélectionner cette option si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels.
   - **Créer un paquet d'installation pour l'application Kaspersky**. Le paquet d'installation sera créé à partir d'un distributif hébergé sur les serveurs de Kaspersky.

   Kaspersky Security Center Cloud Console ne prend pas en charge la création de paquets d'installation à partir d'un fichier.

4. Selon la méthode de création de paquet sélectionnée :

   - Spécifiez le nom du paquet, cliquez sur le bouton **Parcourir** et spécifiez le chemin d'accès à l'archive que vous avez préparée pour créer le paquet d'installation.
   - Sélectionnez la distribution de l'application Kaspersky Endpoint Security. Dans la fenêtre de droite, lisez les informations sur la distribution et cliquez sur le bouton **Télécharger et créer le paquet d'installation**. Le processus de création du fichier d'installation démarre.

5. Lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données. Avant de poursuivre la création du paquet d'installation, vous devez confirmer que vous avez lu le Contrat de licence utilisateur final et la Politique de confidentialité dans leur intégralité et que vous en acceptez les conditions.

6. Quittez l'Assistant.

   Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation. Le paquet d'installation permet d'installer l'application sur les appareils du réseau de l'entreprise ou de mettre à jour la version de l'application.

7. Si nécessaire, configurez les paramètres de configuration initiale de l'application. Pour ce faire, ouvrez les propriétés du paquet d'installation et accédez à l'onglet **Paramètres**.

   Dans la version de Kaspersky Security Center Web Console antérieure à 14.2, la configuration des paramètres de la configuration initiale de l'application dans les propriétés du paquet d'installation de Kaspersky Endpoint Security n'est pas prise en charge. Utilisez le fichier de configuration autoinstall.ini pour configurer les paramètres.

Paramètres de configuration initiale dans Web Console

Dans Kaspersky Security Center Web Console, vous pouvez spécifier les paramètres de configuration initiaux de l'application Kaspersky Endpoint Security dans les propriétés du paquet d'installation sous l'onglet **Paramètres**. Les paquets d'installation créés sont disponibles dans la fenêtre principale de Web Console dans l'une des sections suivantes :

- **Découverte et déploiement des appareils → Déploiement et attribution → Paquets d'installation**.
- **Opérations → Stockages → Paquets d'installation**.

Vous pouvez également indiquer les paramètres de configuration initiale de l'application dans le fichier de configuration inclus dans le paquet d'installation.

Paramètres de la configuration initiale de l'application

Paramètre	Description
Langue des événements dans KSC	Sélectionnez la langue à utiliser pour localiser les événements de l'application envoyés à Kaspersky Security Center : • **Système** (valeur par défaut) : la langue de localisation du système d'exploitation. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais est utilisé pour localiser les événements. • L'une des langues nationales prises en charge par l'application Kaspersky Endpoint Security. L'application utilise l'encodage UTF-8. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.

Paramètre	Description
Activer l'application	Cochez la case si vous souhaitez activer l'application lors de l'installation. Saisissez le code d'activation dans le champ qui s'ouvre. La case est décochée par défaut. Vous pouvez également activer l'application après l'installation. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Source des mises à jour	Sélectionnez la source de mises à jour pour les bases et les modules de l'application : • **Serveurs de mise à jour de Kaspersky** (valeur par défaut). • **Kaspersky Security Center**. • **Autres sources sur le réseau local ou sur Internet**. Si vous sélectionnez cette option, saisissez l'adresse de la source de mises à jour dans le champ qui s'ouvre. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Exécuter la tâche de mise à jour des bases après l'installation	Si la case est cochée, après l'installation de l'application, la tâche de mise à jour des bases de données et des modules de l'application est lancée. La case est cochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Indiquer les paramètres du serveur proxy	Cochez cette case si vous utilisez un serveur proxy pour accéder à Internet. Dans le champ qui s'ouvre, saisissez l'adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<IP address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Installer le code source du noyau	Si la case est cochée, pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, lorsque la protection contre les fichiers malicieux est lancée, la compilation du module du noyau est automatiquement démarrée. La case est cochée par défaut.
Utiliser l'interface graphique	Cochez cette case si vous prévoyez d'installer et d'utiliser l'interface graphique de l'application. Les fichiers d'installation de l'interface graphique doivent être ajoutés au paquet d'installation. La case est décochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Indiquer un utilisateur ayant le rôle d'administrateur (admin)	Cochez la case si vous voulez spécifier l'utilisateur auquel attribuer le rôle d'administrateur (admin). Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`. Dans le champ qui s'ouvre, saisissez le nom d'utilisateur.
Configurer automatiquement SELinux	Si la case est cochée, SELinux est automatiquement configuré pour fonctionner avec Kaspersky Endpoint Security. La case est cochée par défaut.

Paramètre	Description
Supprimer les utilisateurs des groupes privilégiés	Cochez la case pour supprimer automatiquement les utilisateurs des groupes privilégiés kesladmin et keslaudit avant d'installer l'application. La case est décochée par défaut. Si la case est cochée et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.
Désactiver les modules de protection et les tâches d'analyse la première fois que vous lancez l'application après l'installation	Cochez la case si vous souhaitez exécuter l'application avec les module de protection et les tâches d'analyse désactivés après l'installation. Une installation avec des modules de protection désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si vous activez les modules et les tâches nécessaires, alors après le redémarrage de l'application, les modules et les tâches activés continueront de fonctionner.
Activer le traçage de l'application lors du premier lancement après l'installation	Cochez cette case si vous souhaitez activer la création d'un fichier de traçage lors du premier lancement de l'application après son installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.
Mode d'utilisation de l'application	Sélectionnez le mode d'utilisation de l'application. • **Mode standard pour protéger les postes de travail et les serveurs** (valeurs par défaut). Si cette option est sélectionnée, l'application est utilisée comme une application autonome pour protéger les postes de travail et les serveurs exécutant des systèmes d'exploitation Linux. • **Endpoint Detection and Response Agent**. Si cette option est sélectionnée, l'application permet la collaboration entre les solutions Detection and Response de Kaspersky et les solutions antivirus tierces sur les appareils protégés. • **Light Agent pour la protection des environnements virtuels**. Si cette option est sélectionnée, l'application est utilisée en mode Light Agent pour la protection des environnements virtuels (dans le cadre de Kaspersky Security for Virtualization Light Agent).
Activer le mode de protection de l'infrastructure VDI	Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.
La machine virtuelle protégée est utilisée comme serveur	Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. Par défaut, la case est cochée (la machine virtuelle est utilisée dans l'infrastructure virtuelle comme serveur). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.
Mécanisme d'interception	Sélectionnez le mécanisme d'interception des événements système que l'application utilisera dans son travail : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, un module de noyau mis à jour est installé lors de l'installation de l'application. L'application utilise ce module pour intercepter les événements système. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Paramètre	Description
Si le module de noyau mis à jour ne parvient pas à démarrer	Sélectionnez l'action que l'application exécutera en cas d'erreur lors du démarrage du module de noyau mis à jour : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Création d'un paquet d'installation dans la Console d'administration

Avant de créer un paquet d'installation pour l'application Kaspersky Endpoint Security, vous devez préparer les fichiers qui seront inclus dans le paquet.

Si vous prévoyez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels ou en mode Endpoint Detection and Response Agent, vous devez spécifier le mode d'utilisation de l'application dans les paramètres de configuration initiale. Vous pouvez spécifier les paramètres de configuration initiale de l'application lors de la création du paquet d'installation ou après sa création dans les propriétés du paquet d'installation dans la section **Paramètres**, ainsi que dans le fichier de configuration inclus dans le paquet d'installation.

Pour préparer les fichiers pour la création d'un paquet d'installation :

1. Téléchargez l'archive kesl.zip depuis la page de téléchargement de l'application. Elle se trouve dans **Kaspersky Endpoint Security for Linux** (**Distribution complémentaire → Fichiers pour l'installation à distance du produit**).

2. Décompressez l'archive kesl.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center. Placez dans ce même dossier les fichiers de la distribution qui correspondent au type de système d'exploitation sur lequel vous souhaitez installer l'application, ainsi que le type de gestionnaire de paquets sur celui-ci :

   - Pour installer Kaspersky Endpoint Security :

     - kesl-12.4.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
     - kesl_12.4.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
     - kesl-12.4.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
     - kesl-12.4.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)

- kesl-12.4.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
- kesl_12.4.0-<numéro de version>_arm64.deb (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec dpkg)

- Pour installer l'interface graphique de l'application :
  - kesl-gui-12.4.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
  - kesl-gui-12.4.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
  - kesl-gui-12.4.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
  - kesl-gui-12.4.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)
  - kesl-gui-12.4.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
  - kesl-gui_12.4.0-<numéro de version>_arm64.deb (pour système d'exploitation 64 bits pour l'architecture Arm avec dpkg)

  Si vous ne souhaitez pas installer l'interface graphique, n'utilisez pas ces fichiers. La taille du paquet d'installation sera alors inférieure.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'interface utilisateur graphique n'est pas prise en charge.

Si vous ne prévoyez pas d'installer l'interface graphique, vous devez choisir de ne pas l'utiliser en définissant le paramètre approprié lors de la création du paquet d'installation, dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini (`USE_GUI=No`). Dans le cas contraire, l'installation se terminera par une erreur.

Si vous souhaitez utiliser le paquet d'installation que vous créez pour différents systèmes d'exploitation ou différents gestionnaires de paquets, placez les fichiers pour tous les types de systèmes d'exploitation et gestionnaires de paquets nécessaires dans le dossier.

3. Si vous prévoyez d'utiliser l'application Kaspersky Endpoint Security en mode standard et souhaitez utiliser les bases de données pré-téléchargées de l'application :
   a. Placez les archives préparées avec les bases de données pour tous les types de systèmes d'exploitation requis dans le dossier.
   b. Dans les paramètres de configuration initiale de l'application, désactivez le lancement de la tâche de mise à jour de la base de données après l'installation de l'application. Vous pouvez modifier le paramètre correspondant lors de la création du paquet d'installation, dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini (`UPDATE_EXECUTE=No`). Le fichier autoinstall.ini se trouve dans le répertoire où vous avez extrait l'archive kesl.zip.
4. Si vous souhaitez configurer les paramètres de configuration initiale de l'application à l'aide d'un fichier de configuration, ouvrez le fichier de configuration autoinstall.ini et apportez les modifications nécessaires.

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, vous devez établir la valeur du paramètre `KSVLA_MODE=Yes` dans le fichier de configuration autoinstall.ini.

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, vous devez établir la valeur du paramètre `ENDPOINT_AGENT_MODE=Yes` dans le fichier de configuration autoinstall.ini.

Les valeurs des paramètres dans le fichier autoinstall.ini sont sensibles à la casse.

Vous pouvez également configurer les paramètres de configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé dans la section **Paramètres**.

Pour créer un paquet d'installation de Kaspersky Endpoint Security dans la Console d'administration de Kaspersky Security Center :

1. Dans l'arborescence de la console, sélectionnez **Avancés** → **Installation à distance** → **Paquets d'installation**.
2. Cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du paquet d'installation démarre.
3. Cliquez sur le bouton **Créer un paquet d'installation pour l'application Kaspersky**.
4. Saisissez le nom du nouveau paquet d'installation, puis passez à l'étape suivante de l'Assistant.
5. Sélectionnez la distribution de l'application Kaspersky Endpoint Security. Pour ce faire, ouvrez la fenêtre Windows® standard de sélection à l'aide du bouton **Parcourir** et accédez au fichier kesl.kud. Le fichier se trouve dans le dossier où vous avez décompressé l'archive kesl.zip.

   La fenêtre affichera le nom et la version de l'application.

   Passez à l'étape suivante de l'Assistant.
6. Lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données.

   Avant de poursuivre la création du paquet d'installation, vous devez confirmer que vous avez lu le Contrat de licence utilisateur final et la Politique de confidentialité dans leur intégralité et que vous en acceptez les conditions. Pour marquer votre accord, cochez les deux cases dans la fenêtre qui s'ouvre.

   Passez à l'étape suivante de l'Assistant.
7. Si nécessaire, configurez les paramètres de configuration initiale de l'application.

   Vous pouvez également configurer les paramètres de configuration initiale de l'application ultérieurement dans les propriétés du paquet d'installation créé dans la section **Paramètres**.
8. L'assistant charge les fichiers indispensables à l'installation de l'application sur le Serveur d'administration de Kaspersky Security Center. Attendez la fin du téléchargement.
9. Quittez l'Assistant.

Le paquet d'installation créé figure dans l'arborescence de la Console d'administration de Kaspersky Security Center au sein du dossier **Avancés** → **Installation à distance** → **Paquets d'installation**. Vous pouvez utiliser le même paquet d'installation à plusieurs reprises.

Paramètres de configuration initiale dans la Console d'administration

Dans la Console d'administration de Kaspersky Security Center, vous pouvez spécifier les paramètres de configuration initiale de l'application Kaspersky Endpoint Security lors de la création d'un paquet d'installation ou dans les propriétés du paquet d'installation dans la section **Paramètres**. Les paquets d'installation créés sont accessibles dans l'arborescence de la Console d'administration dans le dossier **Avancés → Installation à distance → Paquets d'installation**.

Vous pouvez également indiquer les paramètres de configuration initiale de l'application dans le fichier de configuration inclus dans le paquet d'installation.

Paramètres de la configuration initiale de l'application

Paramètre	Description
Langue des événements dans KSC	Sélectionnez la langue à utiliser pour localiser les événements de l'application envoyés à Kaspersky Security Center : • **Système** (valeur par défaut) : la langue de localisation du système d'exploitation. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais est utilisé par défaut. • Une des langues nationales. L'application utilise l'encodage UTF-8. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.
Code d'activation	Si vous souhaitez activer l'application lors de l'installation, saisissez le code d'activation. Vous pouvez également activer l'application après l'installation. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Sélectionner la source de mise à jour	En cliquant sur le bouton **Configurer**, une fenêtre s'ouvre dans laquelle vous pouvez sélectionner la source des mises à jour pour les bases de données et les modules de l'application : • **Serveurs de mise à jour de Kaspersky** (valeur par défaut). • **Kaspersky Security Center**. • **Autres sources sur le réseau local ou sur Internet**. Si vous sélectionnez cette option, saisissez l'adresse de la source de mises à jour dans le champ **Adresse**. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Exécuter la tâche de mise à jour des bases après l'installation	Si la case est cochée, après l'installation de l'application, la tâche de mise à jour des bases de données et des modules de l'application est lancée. La case est cochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.

Paramètre	Description
Adresse du serveur proxy	Si vous utilisez un serveur proxy pour accéder à Internet, saisissez l'adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<IP address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Installer le code source du noyau	Si la case est cochée, pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, lorsque la protection contre les fichiers malicieux est lancée, la compilation du module du noyau est automatiquement démarrée. La case est cochée par défaut.
Utiliser l'interface graphique	Cochez cette case si vous prévoyez d'installer et d'utiliser l'interface graphique de l'application. Les fichiers d'installation de l'interface graphique doivent être ajoutés au paquet d'installation. La case est décochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.
Utilisateur avec rôle d'administrateur (admin)	Saisissez le nom d'utilisateur auquel est attribué le rôle d'administrateur (admin). Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`.
Configurer automatiquement SELinux	Si la case est cochée, SELinux est automatiquement configuré pour fonctionner avec Kaspersky Endpoint Security. La case est cochée par défaut.
Supprimer les utilisateurs des groupes privilégiés	Cochez la case pour supprimer automatiquement les utilisateurs des groupes privilégiés kesladmin et keslaudit avant d'installer l'application. La case est décochée par défaut. Si la case est cochée et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.
Désactiver les modules de protection et les tâches d'analyse la première fois que vous lancez l'application après l'installation	Cochez la case si vous souhaitez exécuter l'application avec les module de protection et les tâches d'analyse désactivés après l'installation. Une installation avec des modules de protection désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si vous activez les modules et les tâches nécessaires, alors après le redémarrage de l'application, les modules et les tâches activés continueront de fonctionner.
Activer le traçage de l'application lors du premier lancement après l'installation	Cochez cette case si vous souhaitez activer la création d'un fichier de traçage lors du premier lancement de l'application après son installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.
Mode d'utilisation de l'application	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Mode d'utilisation de l'application**. Cette fenêtre vous permet de sélectionner le mode d'utilisation de l'application. • **Mode standard pour protéger les postes de travail et les serveurs** (valeurs par défaut). Si cette option est sélectionnée, l'application est utilisée comme une application autonome pour protéger les postes de travail et les serveurs exécutant des systèmes d'exploitation Linux. • **Endpoint Detection and Response Agent**. Si cette option est sélectionnée, l'application permet la collaboration entre les solutions Detection and Response de Kaspersky et les solutions antivirus tierces sur les appareils protégés. • **Light Agent pour la protection des environnements virtuels**. Si cette option est sélectionnée, l'application est utilisée en mode Light Agent pour la protection des environnements virtuels (dans le cadre de Kaspersky Security for Virtualization Light Agent).

Paramètre	Description
La machine virtuelle protégée est utilisée comme serveur (fenêtre **Mode d'utilisation de l'application**)	Le rôle de la machine virtuelle sur laquelle l'application sera installée : serveur ou poste de travail. Par défaut, la case est cochée (la machine virtuelle est utilisée dans l'infrastructure virtuelle comme serveur). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.
Activer le mode de protection de l'infrastructure VDI (fenêtre **Mode d'utilisation de l'application**)	Cochez la case pour activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de l'application sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. La case est décochée par défaut. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.
Interception des événements système.	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Paramètres d'interception des événements système**. Cette fenêtre vous permet également de sélectionner le mécanisme d'interception des événements système utilisé par l'application : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, un module de noyau mis à jour est installé lors de l'installation de l'application. L'application utilise ce module pour intercepter les événements système. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.
Si le module de noyau mis à jour ne parvient pas à démarrer (fenêtre **Paramètres d'interception des événements système**)	Sélectionnez l'action que l'application exécutera en cas d'erreur lors du démarrage du module de noyau mis à jour : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Préparation d'une archive avec des bases de données de l'application pour créer un paquet d'installation avec des bases de données intégrées

Vous pouvez créer un paquet d'installation pour une installation à distance, qui contient des bases de données pré-téléchargées de l'application. Cela peut être nécessaire, par exemple, si vous installez l'application sur un appareil doté du système d'exploitation Astra Linux Special Edition. Si un paquet d'installation avec des bases de données intégrées est utilisé pour l'installation, l'application est installée avec des bases de données fonctionnelles ; il n'est pas nécessaire de mettre à jour les bases de données immédiatement après l'installation.

Pour créer une archive avec les bases de données pour installer les applications :

1. Installez et configurez initialement l'application Kaspersky Endpoint Security sur votre appareil à l'aide de la ligne de commande ou à l'aide de Kaspersky Security Center.

2. Exécutez une mise à jour des bases de l'application. Vous pouvez mettre à jour les bases de données lors de la configuration initiale de l'application ou après l'installation en exécutant une tâche de type Update sur la ligne de commande ou une tâche *Update* dans la Console d'administration de Kaspersky Security Center ou la Kaspersky Security Center Web Console.

3. Copiez le contenu du répertoire /var/opt/kaspersky/kesl/private/updates/ dans l'un des sous-répertoires suivants en fonction de l'architecture du système d'exploitation pour lequel vous créez un paquet d'installation avec bases de données intégrées : /i386/, /x86_64/ ou /arm64/.

4. Placez les répertoires avec les bases de données dans l'archive kesl-bases.tgz, en conservant la structure des répertoires imbriqués. Vous pouvez archiver un seul sous-répertoire avec des bases de données pour l'architecture de système d'exploitation souhaitée, ou tous les sous-répertoires avec des bases de données (/i386/, /x86_64/ ou /arm64/) dans une archive pour différentes architectures, si vous envisagez de créer un paquet d'installation pour l'installation sur plusieurs systèmes d'exploitation avec des architectures différentes.

Vous pouvez utiliser l'archive créée avec les bases de données de l'application lors de la création d'un paquet d'installation dans la Console d'administration de Kaspersky Security Center ou dans Kaspersky Security Center Web Console.

Paramètres du fichier de configuration autoinstall.ini

Dans le fichier de configuration autoinstall.ini, vous pouvez définir les paramètres indiqués dans le tableau ci-dessous. L'ensemble des paramètres applicables dépend de la manière dont l'application est utilisée.

Les valeurs des paramètres sont sensibles à la casse.

Paramètres du fichier de configuration autoinstall.ini

Paramètre	Description	Valeurs
KSVLA_MODE	Utilisation de Kaspersky Endpoint Security est utilisé en mode Light Agent.	`Yes` : Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent). `No` (valeur par défaut) : Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent (cf. le paramètre ENDPOINT_AGENT_MODE).
SERVER_MODE	Le rôle de la machine virtuelle protégée (serveur ou poste de travail). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.	`Yes` (valeur par défaut) : la machine virtuelle protégée est utilisée comme serveur. `No` : la machine virtuelle protégée est utilisée comme poste de travail.

Paramètre	Description	Valeurs
VDI_MODE	Activation du mode de protection de l'infrastructure VDI pour optimiser les performances des applications sur les machines virtuelles temporaires. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.	`Yes` : activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de Kaspersky Endpoint Security sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. `No` (valeur par défaut) : ne pas activer le mode de protection de l'infrastructure VDI.
ENDPOINT_AGENT_MODE	Utilisation de Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent.	`Yes` : Kaspersky Endpoint Security est utilisé en mode Endpoint Detection and Response Agent pour assurer le fonctionnement conjoint des solutions Detection and Response de Kaspersky et des solutions antivirus tierces sur les appareils protégés. `No` (valeur par défaut) : Kaspersky Endpoint Security est utilisé en mode standard ou en mode Light Agent (cf. le paramètre KSVLA_MODE).
EULA_AGREED	Paramètre obligatoire. Acceptation des dispositions du Contrat de licence Utilisateur final.	`Yes` (valeur par défaut) : accepter les conditions du Contrat de licence utilisateur final. `No` : refuser les conditions du Contrat de licence utilisateur final. Cela entraîne l'interruption de l'installation de l'application.
PRIVACY_POLICY_AGREED	Paramètre obligatoire. Acceptation des dispositions de la Politique de confidentialité.	`Yes` (valeur par défaut) : accepter les conditions de la Politique de confidentialité. `No` : ne pas accepter les conditions de la Politique de confidentialité. Cela entraîne l'interruption de l'installation de l'application.
USE_KSN	Paramètre obligatoire. Activation de l'utilisation de Kaspersky Security Network : Pour activer l'utilisation de KSN, vous devez accepter les termes de la Déclaration de Kaspersky Security Network. Si Kaspersky Endpoint Security est utilisé en mode standard et que vous avez activé l'utilisation de KSN, le mode cloud de l'application est automatiquement activé. Dans ce mode, Kaspersky Endpoint Security utilise une version allégée des bases de données des programmes malveillants.	`Yes` : accepter les conditions de la Déclaration de Kaspersky Security Network et activer l'utilisation de KSN. `No` (valeur par défaut) : ne pas accepter les conditions de la Déclaration de Kaspersky Security Network. La désactivation du KSN n'interrompt pas le processus d'installation de l'application.
GROUP_CLEAN	Paramètre obligatoire. Suppression automatique des utilisateurs des groupes privilégiés kesladmin et keslaudit avant l'installation de l'application.	`Yes` : supprimer les utilisateurs des groupes privilégiés. Si `Yes` est spécifié et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés. `No` : ne pas supprimer les utilisateurs des groupes privilégiés.

Paramètre	Description	Valeurs
LOCALE	Paramètre avancé. Paramètres régionaux du service pour la localisation des événements de l'application envoyés à Kaspersky Security Center. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.	Les paramètres régionaux au format défini dans la RFC 3066. Valeurs possibles : • `de_DE.UTF-8` : Allemand ; • `en_US.UTF-8` : Anglais ; • `fr_FR.UTF-8` : Français ; • `ja_JP.UTF-8` : Japonais ; • `ru_RU.UTF-8` : Russe ; • `zh_TW.UTF-8` : Chinois traditionnel. • `zh_CN.UTF-8` : Chinois simplifié ; Si le paramètre `LOCALE` n'est pas spécifié, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais (en_US.UTF-8 au format standard RFC 3066) est utilisé pour localiser les événements.
INSTALL_LICENSE	Code d'activation pour ajouter une clé de licence à l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`<code d'activation>` : si vous devez activer l'application pendant l'installation ; `None` : si vous n'avez pas besoin d'activer l'application lors de l'installation, par exemple, si l'application est installée dans un segment de réseau fermé sans accès à Internet.
UPDATER_SOURCE	Source des mises à jour des bases et des modules de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	`SCServer` : le serveur d'administration de Kaspersky Security Center est la source des mises à jour. `KLServers` : utilise les serveurs de Kaspersky comme source des mises à jour. Cette valeur est utilisée par défaut. `< adresse de la source de mise à jour >`.
PROXY_SERVER	Adresse du serveur proxy à utiliser pour la connexion à Internet. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	Adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<IP address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de l'application lors de la configuration initiale. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	`Yes` (valeur par défaut) : exécuter la tâche de mise à jour. `No` : ne pas lancer la tâche de mise à jour.

Paramètre	Description	Valeurs
KERNEL_SRCS_INSTALL	Démarrer automatiquement la compilation du module du noyau lorsque la tâche de protection contre les fichiers malicieux est démarrée (pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify).	`Yes` (valeur par défaut) : compiler le module du noyau lorsque la tâche de protection contre les fichiers malicieux démarre. `No` : ne pas compiler le module du noyau.
USE_GUI	Installation et utilisation de l'interface graphique de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	`Yes` : installer et utiliser l'interface graphique de l'application (les fichiers d'installation de l'interface graphique doivent être ajoutés dans le paquet d'installation). `No` (valeur par défaut) : ne pas utiliser l'interface graphique.
ADMIN_USER	Utilisateur auquel est attribué le rôle d'administrateur (admin). Le rôle d'administrateur permet de gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`.	
CONFIGURE_SELINUX	Configuration automatique de SELinux pour fonctionner avec l'application Kaspersky Endpoint Security.	`Yes` (valeur par défaut) : configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security. `No` – ne pas effectuer de configuration automatique de SELinux.
DISABLE_PROTECTION	Désactivation des modules fonctionnels d'une application après son installation. Une installation avec des modules désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si, après avoir installé l'application avec le paramètre `DISABLE_PROTECTION=Yes`, vous activez les modules nécessaires, alors après le redémarrage de l'application, les modules activés continueront de fonctionner.	`Yes` : désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation. `No` : ne pas désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation.
INTERCEPTOR_MODE	Le mécanisme d'interception des événements système utilisé par l'application Kaspersky Endpoint Security dans son travail. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`UseFanotify` (valeur par défaut) : utiliser la technologie fanotify pour intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.
INTERCEPTOR_FALLBACK_STRATEGY	L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`FallbackToFanotify` (valeur par défaut) : passer à l'utilisation de la technologie fanotify pour intercepter les événements système. `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système. Par conséquent, l'analyse des fichiers en temps réel n'est pas effectuée et le niveau de protection de l'appareil diminue.

Paramètre	Description	Valeurs
INTERCEPTOR_APPLY_STRATEGY	Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`RestartServiceAutomatically` (valeur par défaut) : redémarrer automatiquement l'application pour exécuter le module de noyau mis à jour. `RestartServiceManually` : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur. Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.
ENABLE_TRACES_ON_FIRST_STARTUP	Créer un fichier de traçage de l'application lors du premier lancement après l'installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.	`Yes` : créer un fichier de traçage de l'application lors du premier lancement après l'installation. `No` : ne pas créer le fichier de traçage au premier démarrage de l'application.

Si vous voulez modifier les paramètres dans le fichier de configuration autoinstall.ini, spécifiez les valeurs des paramètres au format <nom du paramètre>=<valeur du paramètre> sans espaces entre le nom du paramètre et sa valeur.

Préparation de l'application pour une utilisation via Kaspersky Security Center

Après avoir déployé l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous devez préparer l'application à fonctionner. Les actions à effectuer dépendent du mode dans lequel vous envisagez d'utiliser Kaspersky Endpoint Security.

Mode standard

Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode standard, après le déploiement de l'application, vous devez effectuer les étapes suivantes :

1. Activer l'application si l'activation n'a pas été effectuée à l'aide de la clé ajoutée au paquet d'installation de l'application.

   Vous pouvez créer et exécuter une tâche d'activation via la Console d'administration ou Kaspersky Security Center Web Console, mais également distribuer aux appareils une clé de licence provenant du stockage des clés de Kaspersky Security Center.

2. Mettez à jour les bases de données et les modules de l'application si les bases de données pré-téléchargées de l'application n'ont pas été ajoutées au paquet d'installation de l'application. Vous pouvez utiliser la tâche *Mise à jour*, créée automatiquement par l'Assistant d'installation initiale de Kaspersky Security Center après l'installation du plug-in MMC d'administration ou du plug-in Internet d'administration de Kaspersky Endpoint Security.

   L'application Kaspersky Endpoint Security assure la protection de l'appareil uniquement après la mise à jour des bases de l'application.

3. Configurez une stratégie pour la gestion centralisée de l'application à l'aide de la Console d'administration de Kaspersky Security Center (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) ou de Web Console. Vous pouvez utiliser une stratégie créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center après l'installation du plug-in MMC d'administration ou du plug-in Web d'administration de Kaspersky Endpoint Security.

   Vous pouvez également configurer des tâches d'administration de l'application à l'aide de la Console d'administration et de Web Console.

Mode Light Agent

Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, après le déploiement de l'application, vous devez procéder comme suit :

1. Configurer les paramètres de détection des SVM par les Light Agents. Pour ce faire, il faut créer et configurer une stratégie pour administrer de manière centralisée le fonctionnement de l'application sur les appareils clients. Pour gérer les stratégies, vous pouvez utiliser la Console d'administration (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) ou Web Console.

   Dans les propriétés de la stratégie, vous devez configurer les paramètres suivants :

   - Paramètres de connexion des Light Agents au Serveur d'intégration.
   - Paramètres de connexion des Light Agents à SVM.

2. Assurez-vous que les Light Agents sont connectés à la SVM et au Serveur d'intégration.

   Vous pouvez obtenir des informations de connexion à l'aide des commandes de Kaspersky Endpoint Security sur une machine virtuelle protégée :

   - Vous pouvez afficher des informations sur la connexion à la SVM à l'aide de la commande `kesl-control [-V] --svm-info`.
   - Vous pouvez afficher des informations sur la connexion au Serveur d'intégration à l'aide de la commande `kesl-control [-V] --viis-info`.

3. S'assurer que Kaspersky Endpoint Security utilisé comme Light Agent reçoit les informations sur la licence sous laquelle Kaspersky Security for Virtualization Light Agent est activé.

   Après avoir activé la solution sur la SVM et connecté les Light Agents à la SVM, le module Serveur de protection envoie les informations sur la licence aux Light Agents. Vous pouvez consulter les informations sur la licence utilisée par l'application Kaspersky Endpoint Security dans le cadre de la solution à distance à l'aide de Kaspersky Security Center ou sur une machine virtuelle protégée à l'aide de la ligne de commande.

4. S'assurer que les mises à jour des bases de données requises pour le fonctionnement du Light Agent sont installées sur les machines virtuelles protégées.

   Les bases de données sur les machines virtuelles protégées sont mises à jour à l'aide de la tâche spéciale *Mise à jour*, dans laquelle un dossier sur la SVM est spécifié comme source de mise à jour. La tâche de mise à jour démarre automatiquement.

   Vous pouvez vérifier la mise à jour des bases de données sur une machine virtuelle protégée avec Light Agent à l'aide de la commande `kesl-control --app-info`.

Vous pouvez également configurer les paramètres de l'application à l'aide des stratégies et des tâches de gestion de l'application dans la Console d'administration ou dans Web Console.

Installation et configuration initiale de l'application à l'aide de la ligne de commande

Vous pouvez installer l'application Kaspersky Endpoint Security sur un appareil client à l'aide de la ligne de commande.

L'installation à l'aide de la ligne de commande comprend les étapes suivantes :

1. Installation de l'application et de l'interface graphique de l'application. Selon le mode dans lequel vous envisagez d'utiliser l'application Kaspersky Endpoint Security, vous pouvez utiliser les options d'installation suivantes de l'application :

   - Si vous envisagez d'utiliser Kaspersky Endpoint Security en mode standard, vous pouvez :
     - installer une application avec l'interface graphique ;
     - installer l'application sans l'interface graphique ;
     - installez l'interface graphique sur l'appareil sur lequel l'application est installée.

       Il n'est pas possible d'installer l'interface graphique sur un appareil sur lequel l'application n'est pas installée.

   - Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent, vous devez installer l'application sans interface graphique de l'application. L'interface graphique n'est pas prise en charge.

   Si la version du gestionnaire de paquets apt est antérieure à 1.1.X, vous devez utiliser le gestionnaire de paquets dpkg (selon le système d'exploitation) pour effectuer l'installation.

2. Configuration initiale de l'application.

   Une configuration initiale est requise pour préparer l'application à l'utilisation et activer la protection de l'appareil client.

   Si la configuration initiale n'a pas été exécutée sur l'appareil, vous ne pouvez pas utiliser l'application ni mettre à jour la version de l'application sur cet appareil.

La configuration initiale de l'application est effectuée à l'aide de l'Assistant de configuration initiale inclus dans le kit de distribution de l'application Kaspersky Endpoint Security. Vous pouvez effectuer la configuration initiale de l'application en mode interactif ou automatique.

Installation de l'application à l'aide d'une ligne de commande

Installation de l'application sans l'interface graphique

Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# rpm -i kesl-12.4.0-<numéro de build>.i386.rpm
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# rpm -i kesl-12.4.0-<numéro de build>.x86_64.rpm
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation ALT 64 bits, exécutez la commande suivante :

```
# apt-get install kesl-12.4.0-<numéro de build>.x86_64.rpm
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# rpm -i kesl-12.4.0-<numéro de build>.aarch64.rpm
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format RPM sur un système d'exploitation ALT 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# apt-get install kesl-12.4.0-<numéro de build>.aarch64.rpm
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# apt-get install ./kesl_12.4.0-<numéro de build>_i386.deb
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format DEB sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# apt-get install ./kesl_12.4.0-<numéro de build>_amd64.deb
```

Pour installer Kaspersky Endpoint Security depuis un paquet au format DEB sur un système d'exploitation 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# apt-get install ./kesl_12.4.0-<numéro de build>_arm64.deb
```

Installation de l'interface graphique de l'application

Pour installer l'interface graphique depuis un paquet au format RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# rpm -i kesl-gui-12.4.0-<numéro de build>.i386.rpm
```

Pour installer l'interface graphique depuis un paquet au format RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# rpm -i kesl-gui-12.4.0-<numéro de build>.x86_64.rpm
```

Pour installer l'interface graphique depuis un paquet au format RPM sur un système d'exploitation ALT 64 bits, exécutez la commande suivante :

```
# apt-get install kesl-gui-12.4.0-<numéro de build>.x86_64.rpm
```

Pour installer l'interface graphique depuis un paquet au format RPM sur un système d'exploitation 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# rpm -i kesl-gui-12.4.0-<numéro de build>.aarch64.rpm
```

Pour installer l'interface graphique depuis un paquet au format RPM sur un système d'exploitation ALT 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# apt-get install kesl-gui-12.4.0-<numéro de build>.aarch64.rpm
```

Pour installer l'interface graphique depuis un paquet au format DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# apt-get install ./kesl-gui_12.4.0-<numéro de build>_i386.deb
```

Pour installer l'interface graphique depuis un paquet au format DEB sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# apt-get install ./kesl-gui_12.4.0-<numéro de build>_amd64.deb
```

Pour installer l'interface graphique depuis un paquet au format DEB sur un système d'exploitation 64 bits pour l'architecture Arm, exécutez la commande suivante :

```
# apt-get install ./kesl-gui_12.4.0-<numéro de build>_arm64.deb
```

Configuration initiale de l'application en mode interactif

Pour effectuer la configuration initiale de l'application en mode interactif, vous devez lancer l'Assistant de configuration initiale de l'application Kaspersky Endpoint Security.

L'Assistant de configuration initiale doit être exécuté avec les privilèges root.

Pour exécuter l'Assistant de configuration initiale, exécutez la commande suivante :

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

L'Assistant de configuration requiert de l'application Kaspersky Endpoint Security des valeurs de paramètres étape par étape. Lorsque l'Assistant a terminé son exécution et que la console a été libérée, cela signifie que le processus de configuration initiale de l'application est terminé.

Pour vérifier le code retour, exécutez la commande suivante :

```
echo $?
```

Si la commande renvoie 0, la configuration post-installation de l'application est terminée avec succès.

L'application Kaspersky Endpoint Security assure la protection de l'appareil uniquement après la mise à jour des bases de l'application.

Sélectionnez le mode d'utilisation : standard ou Light Agent

À cette étape, indiquez si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels en tant que module de la solution Kaspersky Security for Virtualization Light Agent.

- Saisissez `yes` si vous souhaitez utiliser Kaspersky Endpoint Security en mode Light Agent.
- Saisissez `no` si vous souhaitez utiliser Kaspersky Endpoint Security en mode standard, comme une application autonome pour la protection des postes de travail et des serveurs.

  Si vous prévoyez d'utiliser l'application en mode Endpoint Detection and Response Agent, à cette étape, vous devez également entrer `no`. Vous pourrez choisir le mode Endpoint Detection and Response Agent à l'étape suivante.

Une fois la configuration initiale terminée, vous ne pouvez pas modifier la façon dont vous utilisez l'application.

Déterminer le rôle de la machine virtuelle

Cette étape s'affiche uniquement si, lors de la première étape, vous avez choisi d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels.

À cette étape, spécifiez le rôle de la machine virtuelle (serveur ou poste de travail) sur laquelle vous installez l'application Kaspersky Endpoint Security :

- Saisissez `yes` si vous utilisez une machine virtuelle comme serveur.
- Saisissez `no` si vous utilisez la machine virtuelle comme poste de travail.

Le rôle de la machine virtuelle détermine sous quelle licence l'application sera utilisée sur cette machine virtuelle et la quantité de fonctionnalités disponibles.

Activer le mode de protection de l'infrastructure VDI

Cette étape s'affiche uniquement si, lors de la première étape, vous avez choisi d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels.

À cette étape, vous pouvez activer le mode de protection de l'infrastructure VDI. Ce mode vous permet d'optimiser le fonctionnement de Kaspersky Endpoint Security sur les machines virtuelles temporaires. Lorsque le mode de protection VDI est activé, les mises à jour nécessitant un redémarrage de la machine virtuelle ne sont pas installées. Lors de la réception de mises à jour nécessitant un redémarrage, le Light Agent installé sur une machine virtuelle envoie un message à Kaspersky Security Center concernant la nécessité de mettre à jour le modèle des machines virtuelles protégées.

Saisissez `yes` si vous souhaitez activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de Kaspersky Endpoint Security sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées.

Saisissez `no` si vous ne souhaitez pas activer le mode de protection de l'infrastructure VDI. Recommandé si Kaspersky Endpoint Security est installé sur une machine virtuelle permanente ou sur un modèle de machine virtuelle à partir duquel des machines virtuelles permanentes seront créées.

Sélectionnez le mode d'utilisation : standard ou Endpoint Detection and Response Agent

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors de la première étape. L'application ne peut pas être utilisée simultanément en mode Light Agent et en mode Endpoint Detection and Response Agent.

À cette étape, indiquez si vous prévoyez d'utiliser Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent :

- Saisissez `yes` si vous souhaitez utiliser Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, comme une application permettant le fonctionnement conjoint des solutions Kaspersky Detection and Response et des solutions antivirus tierces sur les appareils protégés.
- Saisissez `no` si vous souhaitez utiliser Kaspersky Endpoint Security en mode standard, comme une application autonome pour la protection des postes de travail et des serveurs.

Une fois la configuration initiale terminée, vous ne pouvez pas modifier la façon dont vous utilisez l'application.

Sélection des paramètres régionaux du service

À cette étape, l'application affiche la liste des paramètres régionaux pris en charge au format défini dans la RFC 3066.

Vous devez indiquer les paramètres régionaux dans le format dans lequel ils sont répertoriés. Cette norme sera utilisée :

- pour localiser les textes du Contrat de licence utilisateur final, de la Politique de confidentialité et de la Déclaration de Kaspersky Security Network, qui s'affichent lors de l'installation initiale ;
- pour la localisation des événements de l'application envoyés à Kaspersky Security Center.

La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.

Consultation du Contrat de licence utilisateur final et de la Politique de confidentialité

Cette étape permet de prendre connaissance du Contrat de licence utilisateur final conclu entre vous et Kaspersky et de la Politique de confidentialité qui décrit le traitement et le transfert de données.

Acceptation du Contrat de licence utilisateur final

Cette étape correspond à l'acceptation ou au refus des conditions du Contrat de licence utilisateur final.

Après avoir quitté le mode de consultation, saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions du Contrat de licence utilisateur final.
- `no` (ou `n`), si vous refusez les conditions du Contrat de licence utilisateur final.

Si vous avez refusé les conditions du Contrat de licence utilisateur final, la configuration de l'application Kaspersky Endpoint Security est interrompue.

Acceptation de la Politique de confidentialité

Cette étape correspond à l'acceptation ou au refus des conditions de la Politique de confidentialité.

Après avoir quitté le mode de consultation, saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions de la Politique de confidentialité ;
- `no` (ou `n`), si vous refusez les conditions de la Politique de confidentialité.

Si vous avez refusé les conditions de la Politique de confidentialité, la configuration de l'application Kaspersky Endpoint Security est interrompue.

Utilisation de Kaspersky Security Network

Cette étape correspond à l'acceptation ou au refus des conditions d'utilisation de Kaspersky Security Network. Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire /opt/kaspersky/kesl/doc/.

Saisissez une des valeurs suivantes :

- `yes` (ou `y`), si vous acceptez les conditions de la Déclaration de Kaspersky Security Network ; Le mode étendu de KSN sera activé.
- `no` (ou `n`), si vous refusez les conditions de la Déclaration de Kaspersky Security Network.

Le rejet de l'utilisation de Kaspersky Security Network n'entraîne pas l'arrêt de configuration initiale de l'application Kaspersky Endpoint Security. Vous pouvez activer, désactiver ou modifier le mode de Kaspersky Security Network à tout moment.

Si Kaspersky Endpoint Security est utilisé en mode standard et que vous avez activé l'utilisation de Kaspersky Security Network, le mode Cloud de l'application est automatiquement activé. Dans ce mode, Kaspersky Endpoint Security utilise une version allégée des bases de données de logiciels malveillants. En mode Light Agent pour la protection des environnements virtuels, l'utilisation de bases de données légères de logiciels malveillants n'est pas prise en charge.

Suppression des utilisateurs de groupes privilégiés

Cette étape n'est visible que si des utilisateurs se trouvent dans le groupe kesladmin et/ou dans le groupe keslaudit.

Dans cette étape, spécifiez si les utilisateurs doivent être supprimés des groupes privilégiés kesladmin et keslaudit. Les utilisateurs inclus dans les groupes kesladmin et keslaudit ont un accès privilégié aux fonctions de l'application.

Saisissez `yes` pour supprimer tous les utilisateurs détectés du groupe kesladmin et/ou keslaudit. Les utilisateurs dont le groupe primaire est kesladmin ou keslaudit seront déplacés vers le groupe nogroup. Si le groupe nogroup est manquant, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés.

Saisissez `no` si vous ne souhaitez pas que l'application supprime les utilisateurs des groupes privilégiés.

Attribution du rôle d'administrateur à l'utilisateur

Cette étape permet d'attribuer à l'utilisateur le rôle d'administrateur (admin).

Saisissez le nom d'utilisateur auquel vous souhaitez attribuer le rôle d'administrateur. Le rôle d'administrateur est requise pour gérer les paramètres de l'application et les paramètres des tâches via l'interface graphique et via la ligne de commande de l'application sans utiliser la commande `sudo`.

Vous pouvez attribuer un rôle d'administrateur à un utilisateur ultérieurement, après avoir terminé la configuration initiale de l'application.

Configuration du mécanisme d'interception des événements système

À cette étape, la possibilité d'utiliser divers mécanismes pour intercepter les événements système dans l'application est déterminée. Si le système d'exploitation de l'appareil prend en charge la technologie fanotify, vous pouvez sélectionner le mécanisme d'interception des événements système que l'application utilisera dans son fonctionnement :

- Saisissez `yes` si vous souhaitez utiliser le mécanisme d'interception basé sur le module de noyau mis à jour.
- Saisissez `no` si vous souhaitez utiliser le mécanisme d'interception système basé sur la technologie fanotify.

Une application peut utiliser le mécanisme de hook basé sur le module du noyau si le système d'exploitation répond aux exigences d'installation du module du noyau. Si le système d'exploitation de l'appareil prend en charge fanotify mais ne répond pas aux exigences d'installation du module de noyau mis à jour, l'application utilisera fanotify pour intercepter les événements système.

Si vous sélectionnez le mécanisme d'interception basé sur le module de noyau mis à jour, spécifiez les paramètres suivants :

- L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer :
  - Saisissez `yes` si vous souhaitez que l'application utilise la technologie fanotify pour intercepter les événements système si le module de noyau mis à jour ne parvient pas à démarrer.
  - Saisissez `no` si vous souhaitez que l'application continue de s'exécuter sans intercepter les événements système si le module de noyau mis à jour ne parvient pas à démarrer.

    Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

- Mode de redémarrage de l'application lors du passage à l'utilisation d'un module de noyau mis à jour. Pour exécuter le module, vous devez redémarrer l'application automatiquement ou manuellement.

  Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.

  Saisissez `yes` pour autoriser le redémarrage automatique de l'application pour exécuter le module.

Si le système d'exploitation de l'appareil ne prend pas en charge la technologie fanotify, l'application utilisera le module du noyau pour se protéger contre les fichiers malicieux afin d'intercepter les événements système. Si tous les paquets nécessaires sont présents, la compilation du module du noyau sera démarrée automatiquement lorsque la protection contre les fichiers malicieux sera lancée.

Si les paquets nécessaires ne sont pas détectés sur l'appareil, l'application Kaspersky Endpoint Security proposera de les installer. En cas d'échec du téléchargement des paquets, un message d'erreur s'affiche.

Activation de la configuration automatique de SELinux

Cette étape n'apparaît que si SELinux est installé sur votre système d'exploitation.

Lors de cette étape, vous pouvez activer la configuration automatique du système de contrôle d'accès SELinux pour qu'il fonctionne avec l'application Kaspersky Endpoint Security.

Entrez `yes` pour activer la configuration automatique du système SELinux. Si la configuration automatique du système SELinux a échoué (par exemple, dans ls cas d'absence de l'utilitaire semanage), l'application affiche un message d'erreur et invite l'utilisateur à configurer le système SELinux manuellement.

Saisissez `no` si vous ne souhaitez pas que l'application configure automatiquement le système SELinux.

Par défaut, l'application suggère `yes`.

Si nécessaire, vous pouvez configurer manuellement le système SELinux pour qu'il fonctionne ultérieurement avec l'application, après avoir terminé la configuration initiale de l'application.

Configuration de la source des mises à jour

Cette étape s'affiche uniquement si vous avez sélectionné d'utiliser Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent lors des premières étapes de l'Assistant. Si Kaspersky Endpoint Security est utilisé en mode Light Agent, Kaspersky Endpoint Security reçoit les mises à jour des bases de données Light Agent et des modules d'application du Serveur de protection.

Cette étape, vous pouvez configurer la source de mises à jour pour les bases de données et les modules de l'application. Les bases de l'application contiennent les descriptions des signatures des menaces et les méthodes de lutte contre celles-ci. L'application utilise ces enregistrements pour rechercher et neutraliser les menaces. Les experts antivirus de Kaspersky ajoutent régulièrement des enregistrements sur les menaces.

Saisissez une des valeurs suivantes :

- `KLServers` : l'application récupère les mises à jour depuis un des serveurs de mise à jour de Kaspersky.
- `SCServer` : l'application télécharge les mises à jour sur l'appareil protégé depuis le serveur d'administration de Kaspersky Security Center installé dans votre organisation. Vous pouvez sélectionner cette source de mise à jour si vous utilisez l'application Kaspersky Security Center pour l'administration centralisée de la protection des appareils au sein de votre entreprise.
- `Custom` : l'application télécharge les mises à jour depuis la source personnalisée. Vous pouvez d'indiquer l'adresse de la source de mise à jour personnalisée sur le réseau local ou sur Internet.

Configuration du serveur proxy

Cette étape s'affiche uniquement si vous avez sélectionné d'utiliser Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent lors des premières étapes de l'Assistant.

Dans le cadre de cette étape, vous devez définir les paramètres du serveur proxy si vous accédez à Internet via un tel serveur. Pour télécharger les bases de l'application à partir des serveurs de mise à jour, vous devez disposer d'une connexion Internet.

Pour configurer le serveur proxy, exécutez une des actions suivantes :

- Si la connexion à Internet s'opère via un serveur proxy, indiquez l'adresse de ce dernier dans un des formats suivants :
  - `<protocole de connexion>://<adresse IP du serveur proxy>:<numéro de port>`, si la connexion au serveur proxy ne nécessite pas d'authentification
  - `<protocole de connexion>://<nom d'utilisateur>:<mot de passe>@<adresse IP du serveur proxy>:<numéro de port>` si la connexion au serveur proxy nécessite une authentification

    La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.

Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.

- Si vous n'utilisez pas de serveur proxy pour vous connecter à Internet, saisissez `no` comme réponse.

Par défaut, l'application suggère `no`.

Vous pouvez configurer les paramètres du serveur proxy ultérieurement après avoir terminé la configuration initiale de l'application.

Démarrage d'une mise à jour de la base de données d'une application

Cette étape s'affiche uniquement si vous avez sélectionné d'utiliser Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent lors des premières étapes de l'Assistant. Si Kaspersky Endpoint Security est utilisé en mode Light Agent, Kaspersky Endpoint Security reçoit les mises à jour des bases de données Light Agent et des modules d'application du Serveur de protection.

À cette étape, vous pouvez exécuter la tâche de mise à jour de la base de données de l'application sur l'appareil client.

Saisissez `no` si vous souhaitez refuser d'exécuter une mise à jour de la base de données de l'application.

Si vous souhaitez exécuter la tâche de mise à jour de la base de données sur l'appareil, saisissez `yes`.

Par défaut, l'application suggère `yes`.

Si la valeur `yes` est sélectionnée, l'application sera automatiquement redémarrée après la mise à jour des bases de données.

L'application Kaspersky Endpoint Security assure la protection de l'appareil uniquement après la mise à jour des bases de l'application.

Vous pouvez exécuter la tâche de mise à jour ultérieurement après avoir terminé la configuration initiale de l'application.

Activation de la mise à jour automatique des bases de l'application

Cette étape s'affiche uniquement si vous avez sélectionné d'utiliser Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent lors des premières étapes de l'Assistant. Si Kaspersky Endpoint Security est utilisé en mode Light Agent, Kaspersky Endpoint Security reçoit les mises à jour des bases de données Light Agent et des modules d'application du Serveur de protection.

Cette étape correspond à l'activation de la mise à jour automatique des bases de l'application.

Saisissez `yes` pour activer la mise à jour automatique des bases de l'application. L'application recherche la présence éventuelle de mises à jour pour les bases toutes les 60 minutes par défaut. S'il existe des mises à jour, l'application télécharge les bases mises à jour.

Saisissez `no` si vous ne souhaitez pas que l'application mette à jour automatiquement les bases.

Vous pouvez activer les mises à jour automatiques de la base de données ultérieurement, après avoir terminé la configuration initiale de l'application, en planifiant la tâche de mise à jour.

Activation de l'application

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors des premières étapes. Si Kaspersky Endpoint Security est utilisé en mode Endpoint Detection and Response Agent, après avoir terminé la configuration initiale de l'application, vous devez ajouter une clé de licence conçue pour activer la fonctionnalité Kaspersky Endpoint Detection and Response Expert (n-premise). Si Kaspersky Endpoint Security est utilisé en mode Light Agent, Kaspersky Endpoint Security reçoit des informations sur la licence du Serveur de protection ; il n'est pas nécessaire d'activer Kaspersky Endpoint Security séparément.

Cette étape vous permet d'activer l'application à l'aide d'un code d'activation ou d'un fichier clé.

Pour activer l'application à l'aide d'un code d'activation, il faut saisir le code d'activation.

Pour activer l'application à l'aide d'un fichier clé, il faut indiquer le chemin d'accès complet au fichier clé.

Si vous n'avez pas indiqué de code d'activation ou de fichier clé, l'application sera activée avec une clé d'évaluation valide un mois.

Vous pouvez activer l'application ultérieurement après avoir terminé la configuration initiale de l'application.

Configuration initiale de l'application en mode automatique

Pour effectuer la configuration initiale de l'application en mode automatique, vous devez :

1. Préparer un fichier de configuration contenant les paramètres de configuration initiale. Vous pouvez créer ce fichier ou en copier la structure à partir du fichier de configuration autoinstall.ini utilisé pour installer l'application à distance à l'aide de Kaspersky Security Center.

2. Lancer l'Assistant de configuration initiale de l'application Kaspersky Endpoint Security en spécifiant le chemin d'accès au fichier de configuration.

   L'Assistant de configuration initiale doit être exécuté avec les privilèges root.

Pour démarrer la configuration initiale de l'application en mode automatique, exécutez la commande suivante :

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=< fichier de configuration initiale >
```

où < `fichier de configuration initiale` > est le chemin d'accès au fichier de configuration qui contient les paramètres de configuration initiale.

Lorsque l'Assistant de configuration initiale a terminé son exécution et que la console a été libérée, cela signifie que le processus de configuration initiale de l'application est terminé.

Pour vérifier le code retour, exécutez la commande suivante :

```
echo $?
```

Si la commande renvoie 0, la configuration post-installation de l'application est terminée avec succès.

L'application Kaspersky Endpoint Security assure la protection de l'appareil uniquement après la mise à jour des bases de l'application.

Pour mettre à jour correctement les modules de l'application après avoir terminé l'Assistant, vous devrez peut-être redémarrer l'application. Vérifiez l'état des mises à jour de l'application à l'aide de la commande `kesl-control --app-info`.

Paramètres du fichier de configuration de la configuration initiale de l'application

Dans le fichier de configuration d'installation initiale, vous pouvez définir les paramètres indiqués dans le tableau ci-dessous. L'ensemble des paramètres applicables dépend de la manière dont l'application est utilisée.

Les valeurs des paramètres sont sensibles à la casse.

Paramètres du fichier de configuration de la configuration initiale de l'application

Paramètre	Description	Valeurs
KSVLA_MODE	Utilisation de Kaspersky Endpoint Security est utilisé en mode Light Agent.	`Yes` : Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent). `No` : Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent (cf. le paramètre ENDPOINT_AGENT_MODE).
SERVER_MODE	Le rôle de la machine virtuelle protégée (serveur ou poste de travail). Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.	`Yes` : la machine virtuelle protégée est utilisée comme serveur. `No` : la machine virtuelle protégée est utilisée comme poste de travail.

Paramètre	Description	Valeurs
VDI_MODE	Activation du mode de protection de l'infrastructure VDI pour optimiser les performances des applications sur les machines virtuelles temporaires. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.	`Yes` : activer le mode de protection de l'infrastructure VDI. Recommandé lors de l'installation de Kaspersky Endpoint Security sur un modèle de machine virtuelle à partir duquel des machines virtuelles temporaires seront créées. `No` : ne pas activer le mode de protection de l'infrastructure VDI.
ENDPOINT_AGENT_MODE	Utilisation de Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent.	`Yes` : Kaspersky Endpoint Security est utilisé en mode Endpoint Detection and Response Agent pour assurer le fonctionnement conjoint des solutions Detection and Response de Kaspersky et des solutions antivirus tierces sur les appareils protégés. `No` : Kaspersky Endpoint Security est utilisé en mode standard ou en mode Light Agent (cf. le paramètre KSVLA_MODE).
EULA_AGREED	Paramètre obligatoire. Acceptation des dispositions du Contrat de licence Utilisateur final.	`Yes` : accepter les conditions du Contrat de licence utilisateur final. `No` : refuser les conditions du Contrat de licence utilisateur final. La configuration initiale de l'application sera interrompue.
PRIVACY_POLICY_AGREED	Paramètre obligatoire. Acceptation des dispositions de la Politique de confidentialité.	`Yes` : accepter la Politique de confidentialité pour poursuivre l'installation de l'application. `No` : ne pas accepter les conditions de la Politique de confidentialité. La configuration initiale de l'application sera interrompue.
USE_KSN	Paramètre obligatoire. Activation de l'utilisation de Kaspersky Security Network : Pour activer l'utilisation de KSN, vous devez accepter les termes de la Déclaration de Kaspersky Security Network. Si Kaspersky Endpoint Security est utilisé en mode standard et que vous avez activé l'utilisation de KSN, le mode cloud de l'application est automatiquement activé. Dans ce mode, Kaspersky Endpoint Security utilise une version allégée des bases de données des programmes malveillants.	`Yes` : accepter les conditions de la Déclaration de Kaspersky Security Network et activer l'utilisation de KSN. `No` : ne pas accepter les conditions de la Déclaration de Kaspersky Security Network. La désactivation du KSN n'interrompt pas le processus de configuration initiale de l'application.
GROUP_CLEAN	Paramètre obligatoire. Suppression d'utilisateurs des groupes privilégiés kesladmin et keslaudit avant l'installation de l'application.	`Yes` : supprimer les utilisateurs des groupes privilégiés. Si `Yes` est spécifié et qu'il n'y a pas de groupe, l'installation échouera et vous serez invité à supprimer manuellement les utilisateurs des groupes privilégiés. `No` : ne pas supprimer les utilisateurs des groupes privilégiés.

Paramètre	Description	Valeurs
LOCALE	Paramètre avancé. Paramètres régionaux du service pour la localisation des événements de l'application envoyés à Kaspersky Security Center. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.	Les paramètres régionaux au format défini dans la RFC 3066. Valeurs possibles : • `de_DE.UTF-8` : Allemand ; • `en_US.UTF-8` : Anglais ; • `fr_FR.UTF-8` : Français ; • `ja_JP.UTF-8` : Japonais ; • `ru_RU.UTF-8` : Russe ; • `zh_TW.UTF-8` : Chinois traditionnel. • `zh_CN.UTF-8` : Chinois simplifié ; Si le paramètre `LOCALE` n'est pas spécifié, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais (en_US.UTF-8 au format standard RFC 3066) est utilisé pour localiser les événements.
INSTALL_LICENSE	Code d'activation ou chemin d'accès au fichier clé pour ajouter la clé de licence à l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`<code d'activation>` : si vous devez activer l'application à l'aide d'un code d'activation lors de l'installation ; `<chemin complet vers le fichier clé>` : si vous devez activer l'application à l'aide d'un fichier clé lors de l'installation ; `None` : si vous n'avez pas besoin d'activer l'application lors de l'installation, par exemple, si l'application est installée dans un segment de réseau fermé sans accès à Internet.
UPDATER_SOURCE	Source des mises à jour des bases et des modules de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	`SCServer` : le serveur d'administration de Kaspersky Security Center est la source des mises à jour. `KLServers` : utilise les serveurs de Kaspersky comme source des mises à jour. `< adresse de la source de mise à jour >`.
PROXY_SERVER	Adresse du serveur proxy à utiliser pour la connexion à Internet. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	Adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<IP address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.

Paramètre	Description	Valeurs
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de l'application lors de la configuration initiale. Le paramètre s'applique uniquement si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent.	`Yes` : lancer la tâche de mise à jour. `No` : ne pas lancer la tâche de mise à jour.
KERNEL_SRCS_INSTALL	Démarrer automatiquement la compilation du module du noyau lorsque la tâche de protection contre les fichiers malicieux est démarrée (pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify).	`Yes` : compiler le module du noyau lors du démarrage de la tâche de protection contre les fichiers malicieux. `No` : ne pas compiler le module du noyau.
ADMIN_USER	Utilisateur auquel est attribué le rôle d'administrateur (admin).	
CONFIGURE_SELINUX	Configuration automatique de SELinux pour fonctionner avec l'application Kaspersky Endpoint Security.	`Yes` : configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security. `No` – ne pas effectuer de configuration automatique de SELinux.
DISABLE_PROTECTION	Désactivation des modules de protection et des tâches d'analyse des applications après leur installation. Une installation avec des modules de protection désactivés peut être pratique, par exemple, pour reproduire un problème dans l'application afin de créer un fichier de traçage. Si, après avoir installé l'application avec le paramètre `DISABLE_PROTECTION=Yes`, vous activez les modules et les tâches nécessaires, alors après le redémarrage de l'application, les modules et les tâches activés continueront de fonctionner.	`Yes` : désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation. `No` : ne pas désactiver les modules de protection et les tâches d'analyse lorsque l'application est lancée après l'installation.
INTERCEPTOR_MODE	Le mécanisme d'interception des événements système utilisé par l'application Kaspersky Endpoint Security dans son travail. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`UseFanotify` pour utiliser la technologie fanotify afin d'intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.
INTERCEPTOR_FALLBACK_STRATEGY	L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`FallbackToFanotify` : passer à l'utilisation de la technologie fanotify pour intercepter les événements système. `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système. Par conséquent, l'analyse des fichiers en temps réel n'est pas effectuée et le niveau de protection de l'appareil diminue.
ENABLE_TRACES_ON_FIRST_STARTUP	Créer un fichier de traçage de l'application lors du premier lancement après l'installation. Pour enregistrer la traçage, le fichier kesl_startup.log est automatiquement créé dans le répertoire /var/log/kaspersky/kesl/. Ce fichier n'est pas soumis à la limitation de taille fixée pour les fichiers de traçage classiques de l'application. L'enregistrement de traçage s'arrête après le démarrage de la tâche Protection contre les fichiers malicieux ou cinq minutes après le démarrage de l'enregistrement de traçage.	`Yes` : créer un fichier de traçage de l'application lors du premier lancement après l'installation. `No` : ne pas créer le fichier de traçage au premier démarrage de l'application.

Spécifiez les valeurs des paramètres au format <nom du paramètre>=<valeur du paramètre> sans espaces entre le nom du paramètre et sa valeur.

Configuration des règles d'autorisation dans le système SELinux

Configuration de SELinux pour travailler manuellement avec l'application

Si l'application n'a pas réussi à configurer automatiquement le système SELinux lors de la configuration initiale de l'application Kaspersky Endpoint Security ou si vous avez refusé la configuration automatique, vous pouvez configurer manuellement le système SELinux pour qu'il fonctionne avec l'application Kaspersky Endpoint Security.

Pour configurer manuellement le système SELinux pour qu'il fonctionne avec l'application :

1. Placez le système SELinux en mode non bloquant :
   - Si SELinux a été activé, exécutez la commande suivante :

     ```
     # setenforce Permissive
     ```

   - Si SELinux était désactivé, ouvrez le fichier de configuration /etc/selinux/config, attribuez la valeur suivante au paramètre `SELINUX=permissive` et redémarrez le système d'exploitation.
2. Assurez que l'utilitaire semanage est installé dans le système. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.
3. Si vous utilisez une stratégie SELinux personnalisée, c'est-à-dire différente de targeted policy par défaut, attribuez une étiquette à chaque fichier exécutable source de l'application Kaspersky Endpoint Security conformément à la stratégie SELinux utilisée en exécutant les commandes suivantes :

   ```
   # semanage fcontext -a -t bin_t < fichier exécutable >
   # restorecon -v < fichier exécutable >
   ```

   où `< fichier exécutable >` désigne :
   - /var/opt/kaspersky/kesl/12.4.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.4.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.4.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.4.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/shared/kesl

4. Lancez les tâches suivantes :

   - tâche Protection contre les fichiers malicieux :

     ```
     kesl-control --start-task 1
     ```

   - tâche d'analyse des zones critiques :

     ```
     kesl-control --start-task 4 -W
     ```

   Il est recommandé de lancer toutes les tâches que vous pensez utiliser pendant l'utilisation de l'application Kaspersky Endpoint Security.

5. Lancez l'interface utilisateur graphique si vous prévoyez de l'utiliser.

6. Assurez-vous que le fichier audit.log ne contient aucune erreur :

   ```
   # grep kesl /var/log/audit/audit.log
   ```

7. Si vous découvrez des erreurs dans le fichier audit.log, créez et chargez un nouveau module de règles sur la base des enregistrements de blocage pour éliminer les erreurs, puis exécutez toutes les tâches que vous avez l'intention d'exécuter pendant l'utilisation de l'application Kaspersky Endpoint Security en exécutant les commandes suivantes :

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

   En cas d'apparition de nouveaux messages audit relatifs à Kaspersky Endpoint Security, il faut mettre à jour le fichier du module des règles.

8. Placez le système SELinux en mode bloquant :

   ```
   # setenforce Enforcing
   ```

Si vous utilisez une stratégie SELinux personnalisée, après l'installation des mises à jour de l'application, vous devez attribuer manuellement une étiquette aux fichiers exécutables d'origine de l'application Kaspersky Endpoint Security (suivez les étapes 1 et de 3 à 8).

Pour obtenir de plus amples informations, consultez la documentation du système d'exploitation utilisé.

Configuration de SELinux pour exécuter la tâche Démarrer le processus

Si SELinux est installé sur votre système d'exploitation en mode `Enforcing`, l'exécution de la tâche Démarrer le processus nécessite une configuration supplémentaire de SELinux.

Pour configurer le système SELinux pour exécuter la tâche Démarrer le processus :

1. Placez le système SELinux en mode non bloquant :

   - Si SELinux a été activé, exécutez la commande suivante :

     ```
     # setenforce Permissive
     ```

   - Si SELinux était désactivé, ouvrez le fichier de configuration /etc/selinux/config, attribuez la valeur suivante au paramètre `SELINUX=permissive` et redémarrez le système d'exploitation.

2. Assurez que l'utilitaire semanage est installé dans le système. Si l'utilitaire n'est pas installé, installez le paquet policycoreutils-python ou policycoreutils-python-utils en fonction du type de gestionnaire de paquets.

3. Lancez la tâche Démarrer le processus.

4. Assurez-vous que le fichier audit.log ne contient aucune erreur :

   ```
   # grep kesl /var/log/audit/audit.log
   ```

5. S'il y a des erreurs dans le fichier audit.log, créez et chargez un nouveau module de règles basé sur les enregistrements de blocage pour résoudre les erreurs, puis exécutez à nouveau la tâche Démarrer le processus.

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

6. Placez le système SELinux en mode bloquant :

   ```
   # setenforce Enforcing
   ```

Lancement de l'application sous Astra Linux en mode environnement logiciel fermé

Cette section décrit les actions que vous devez effectuer pour lancer l'application sur le système d'exploitation Astra Linux Special Edition en mode environnement logiciel fermé.

Pour Astra Linux Special Edition (prochaines mises à jour 1.6, 1.7 et 1.8)

Pour lancer l'application dans le système d'exploitation Astra Linux Special Edition (prochaines mises à jour 1.6, 1.7 ou 1.8) :

1. Définir les paramètres suivants dans le fichier /etc/digsig/digsig_initramfs.conf :

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Installer le paquet de compatibilité :

   ```
   apt install astra-digsig-oldkeys
   ```

3. Créer un répertoire pour la clé de l'application :

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Placer la clé de l'application (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) dans le répertoire créé à l'étape précédente :

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Mettez à jour l'image initramfs :

   ```
   update-initramfs -u -k all
   ```

6. Redémarrez le système d'exploitation.

Pour Astra Linux Special Edition (operational update 1.5)

Pour lancer l'application dans le système d'exploitation Astra Linux Special Edition (operational update 1.5) :

1. Définir les paramètres suivants dans le fichier /etc/digsig/digsig_initramfs.conf :

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Créer un répertoire pour la clé de l'application :

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. Placer la clé de l'application (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) dans le répertoire créé à l'étape précédente :

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. Mettez à jour l'image initramfs :

   ```
   sudo update-initramfs -u -k all
   ```

5. Redémarrez le système d'exploitation.

L'interaction avec l'interface graphique utilisateur de l'application est supportée pour les sessions obligatoires.

Lancement de l'application sous ALT SP en mode environnement logiciel fermé

Cette section décrit les actions que vous devez effectuer dans la ligne de commande pour lancer l'application sur le système d'exploitation Alt SP en mode environnement logiciel fermé.

Pour exécuter une application sous le système d'exploitation ALT SP :

1. Désactivez le mode environnement logiciel fermé s'il est activé en exécutant la commande :

   ```
   integrity-remover
   ```

2. Créez le groupe kesl pour modifier la stratégie IMA en exécutant la commande :

   ```
   groupadd kesl
   ```

3. Trouvez l'identifiant unique (GUID) du groupe créé en exécutant la commande :

   ```
   cat /etc/group | grep kesl
   ```

4. Modifiez la stratégie IMA pour exclure le groupe kesl. Pour ce faire, procédez comme suit :

   a. Copiez le fichier /usr/share/integrity/policy en exécutant la commande :

      ```
      cp /usr/share/integrity/policy /etc/integrity/policy
      ```

   b. Modifiez le fichier /etc/integrity/policy avec un éditeur de texte (tel que vim) en exécutant la commande :

      ```
      vim /etc/integrity/policy
      ```

   c. Après la ligne `dont_measure fsmagic=0xf97cff8c` (il s'agit généralement de la dernière ligne de la section `dont_measure`), ajoutez la ligne `dont_measure fgroup=<GUID>`, où `<GUID>` est l'ID unique du groupe créé à l'étape 2 de ces instructions).

   d. Après la ligne `dont_appraise fsmagic=0x27e0eb` (il s'agit généralement de la dernière ligne de la section `dont_appraise`), ajoutez la ligne `dont_appraise fgroup=<GUID>`, où `<GUID>` est l'ID unique du groupe créé à l'étape 2 de ces instructions).

   e. Enregistrez vos modifications.

5. Dans le fichier /usr/sbin/integrity-sign, modifiez la fonction list_all_files pour inclure Kaspersky Endpoint Security dans la liste d'autorisation des applications autorisées à s'exécuter en mode environnement logiciel fermé. Pour ce faire, procédez comme suit :

   a. Modifiez le fichier /usr/sbin/integrity-sign à l'aide d'un éditeur de texte (par exemple, vim) en exécutant la commande :

      ```
      vim /usr/sbin/integrity-sign
      ```

   b. Recherchez la fonction list_all_files et dans le corps de la fonction, dans les lignes commençant par `find -P` à la fin de chaque liste de répertoire, ajoutez les répertoires de l'application Kaspersky Endpoint Security /var/opt et /opt.

   c. Enregistrez vos modifications.

6. Installez l'application Kaspersky Endpoint Security. Pour garantir le bon fonctionnement de la mise à jour des bases de données de l'application après l'installation, ne lancez pas cette mise à jour lors de la configuration initiale de l'application (pour cela, saisissez no à l'étape de lancement de la mise à jour des bases de l'application).

7. Attribuez l'héritage des droits du groupe et des répertoires kesl aux modules mis à jour de l'application Kaspersky Endpoint Security en exécutant les commandes suivantes :

   ```
   cd /var/opt/kaspersky/kesl/< numéro de build _*>/var/opt/kaspersky/kesl/private
   chown -R root:kesl updates/
   find updates -type d -exec chmod g+s {} \;
   cd /opt/kaspersky/kesl/lib64
   chown -R root:kesl updatable_modules/
   find updatable_modules -type d -exec chmod g+s {} \;
   cd /var/opt/kaspersky/kesl/common/
   chown -R root:kesl temp/
   find temp -type d -exec chmod g+s {} \;
   ```

8. Attribuez l'héritage des droits du groupe et des répertoires kesl aux modules mis à jour de l'Agent d'administration en exécutant les commandes suivantes :

   ```
   cd /var/opt/kaspersky/
   chown -R root:kesl klnagent/
   find klnagent/ -type d -exec chmod g+s {} \;
   cd /opt/kaspersky/
   chown -R root:kesl klnagent64/
   find klnagent64/ -type d -exec chmod g+s {} \;
   ```

9. Activez le mode d'environnement logiciel fermé en exécutant la signature système avec la commande :

   ```
   integrity-applier -i -A
   ```

10. Assurez-vous que le sous-système IMA est activé en exécutant la commande :

    ```
    cat /proc/cmdline
    ```

    L'affichage de la commande doit contenir les lignes `lsm=integrity ima_hash=sha512 ima_appraise=enforce.`

11. Exécutez la tâche de mise à jour des bases de données avec la commande :

    ```
    kesl-control --start 6 -W
    ```

    Si l'événement *EventType=BasesApplied* est présent dans l'affichage après la fin de la tâche de mise à jour des bases de données, les bases de données ont été correctement mises à jour.

12. Redémarrez l'application en exécutant la commande :

    ```
    systemctl restart kesl
    ```

Configuration du système d'exploitation OSnova pour que l'application fonctionne

Pour la version de OSnova 2.4

Pour préparer un appareil exécutant le système d'exploitation OSnova 2.4 pour l'installation à distance de l'Agent d'administration :

1. ouvrez le fichier /etc/systemd/logind.conf et commentez la ligne `#KillUserProcesses=yes` dans la section `[Login]`.

2. Ouvrez le fichier /usr/lib/NESS/pam-user-session et commentez la ligne `#loginctl terminate-session "$XDG_SESSION_ID"`.

Pour exécuter une application sous le système d'exploitation OSnova 2.4 :

1. Ouvrez le fichier /etc/NESS/systemd/kesl.service.config et définissez la valeur du paramètre `NESSCTX_MODIFY=t+ADDEQUSOCK,OMIT,70,SSUID_SAVE_CTX_PERMANENT"`.

2. Actualisez les paramètres du service en exécutant la commande `systemctl daemon-reload`.

3. Si vous souhaitez exécuter une analyse de la mémoire des processus et de la mémoire du noyau, vous devez désactiver le moyen de protection de la mémoire mprotect (ou PaX) dans le noyau, c'est-à-dire ajouter le paramètre `mprotect=off` dans la ligne de commande de démarrage du noyau. Pour plus de détails, consultez la documentation OSnova.

4. Redémarrez le système d'exploitation.

Après avoir installé l'interface graphique (paquet kesl-gui), exécutez les commandes suivantes dans le terminal de la ligne de commande en tant qu'utilisateur root :

```
rm /etc/xdg/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /etc/xdg/autostart/kaspersky-kesl.desktop

rm /usr/share/applications/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/app.desktop /usr/share/applications/kaspersky-kesl.desktop

rm /usr/share/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /usr/share/autostart/kaspersky-kesl.desktop

rm /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/Thunar/sendto/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/sendto.desktop /usr/share/Thunar/sendto/kaspersky-kesl.desktop
```

Pour les versions 2.5.1 et supérieures de OSnova

Pour préparer un appareil exécutant le système d'exploitation OSnova 2.5.1 ou suivant pour l'installation à distance de l'Agent d'administration :

1. Ouvrez le fichier /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf et dans la section `[Login]` commentez la ligne `#KillUserProcesses=yes`.

2. Ouvrez le fichier /usr/lib/NESS/pam-user-session et commentez la ligne `#loginctl terminate-session "$XDG_SESSION_ID"`.

Pour exécuter une application sous le système d'exploitation OSnova 2.5.1 ou suivant :

1. Ouvrez le fichier /etc/NESS/systemd/kesl.service.config et définissez la valeur du paramètre `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`.

2. Actualisez les paramètres du service en exécutant la commande `systemctl daemon-reload`.

3. Ouvrez le fichier /etc/sysctl.d/30-disable-ptrace.conf et définissez `kernel.yama.ptrace_scope=0.`

4. Si vous souhaitez exécuter une analyse de la mémoire des processus et de la mémoire du noyau, vous devez désactiver le moyen de protection de la mémoire mprotect (ou PaX) dans le noyau, c'est-à-dire ajouter le paramètre `mprotect=off` dans la ligne de commande de démarrage du noyau. Pour plus de détails, consultez la documentation OSnova.

5. Redémarrez le système d'exploitation.

Lors de l'installation de l'application Kaspersky Endpoint Security sur un appareil doté des versions OSnova 2.14 et supérieures, l'erreur `"dpkg: error processing package kesl (--install): installed kesl package post-installation script subprocess returned error exit status 1"` peut se produire en raison de la présence de deux lignes `SUPPORT_URL` dans le fichier /etc/os-release. Pour installer correctement l'application, vous devez supprimer l'une des deux lignes `SUPPORT_URL` dans le fichier /etc/os-release.

Optimisation de l'utilisation des ressources par l'application

Cette section contient des recommandations des experts de Kaspersky sur la configuration de l'application Kaspersky Endpoint Security pour optimiser la consommation des ressources système. Lorsque l'application s'exécute avec les paramètres par défaut, les performances du système peuvent diminuer sur certains appareils en raison de l'utilisation partagée des ressources système par les applications appliquées et l'application Kaspersky Endpoint Security. Pour éviter toute dégradation des performances, il est recommandé de suivre les procédures de cette section après l'installation et la configuration initiale de l'application.

Le scénario recommandé pour la configuration d'une application visant à optimiser la consommation des ressources système comprend les étapes suivantes :

1. **Répartition des appareils en groupes d'administration en fonction du rôle des appareils dans l'infrastructure**

   Effectuez un inventaire des appareils selon les fonctions qu'ils exécutent et placez-les dans différents groupes d'administration selon ces fonctions. Par exemple, placez les serveurs Web dans un groupe d'administration, placez les serveurs de base de données dans un autre groupe d'administration, placez les postes de travail des utilisateurs dans un troisième groupe d'administration, etc.

2. **Configuration de l'application pour les rôles de serveur typiques**

   Effectuez la configuration recommandée de l'application sur les appareils en fonction de leur rôle dans l'infrastructure.

3. **Analyse des performances sur les appareils pilotes**

   Attribuez 1 à 2 appareils pilotes dans chacun des groupes d'administration. Pour chaque appareil, analysez la manière dont l'application Kaspersky Endpoint Security utilise les ressources système et comment les performances des applications installées sur les appareils évoluent.

4. **Configuration des paramètres de l'application sur les appareils pilotes en fonction des résultats de l'analyse des performances**

   Si les performances des applications diminuent considérablement ou si la quantité de ressources système consommées par Kaspersky Endpoint Security est critique pour le fonctionnement du système d'exploitation et des applications, effectuez la configuration recommandée de la Protection contre les fichiers malicieux et les tâches d'analyse.

   Vous pouvez également optimiser les modules Protection contre les menaces Internet et Protection contre les menaces réseau.

5. **Configurer les paramètres de l'application sur tous les appareils**

   Si les étapes ci-dessus entraînent une amélioration des performances de votre appareil, veuillez effectuer une configuration similaire de l'application sur d'autres appareils du même type.

Recommandations pour les rôles de serveur typiques

Serveur Web

Lorsque vous travaillez sur le protocole HTTPS et sous une charge client élevée sur le serveur, les modules Protection contre les menaces Internet et Protection contre les menaces réseau peuvent augmenter considérablement la consommation des ressources système. Cela se produit parce que l'application décrypte et vérifie le trafic HTTPS.

Analysez la façon dont la charge sur le serveur change pendant l'exécution de ces modules. Veuillez contacter l'assistance technique de Kaspersky pour sélectionner les paramètres de fonctionnement optimaux et résoudre les problèmes de compatibilité.

Serveur Proxy

Il est recommandé de désactiver les modules Protection contre les menaces Internet et Protection contre les menaces réseau sur l'appareil qui agit comme serveur proxy ou équilibreur de charge.

Serveur avec conteneurisation

Il est recommandé de désactiver les modules Protection contre les menaces Internet et Protection contre les menaces réseau sur les serveurs utilisés pour les services de conteneurisation. Pour protéger les environnements de conteneurs, vous pouvez utiliser l'application Kaspersky Container Security.

Analyse du fonctionnement de l'application sur l'appareil

Pour analyser les objets, l'application Kaspersky Endpoint Security utilise les ressources du processeur, les entrées et sorties du sous-système de disque et la mémoire vive.

Pour afficher des informations sur la consommation des ressources par l'application, exécutez la commande suivante :

```
top -bn1|grep kesl
```

Il faut exécuter la commande lors du chargement dans le système.

La commande renvoie la quantité de mémoire utilisée et le temps de processeur :

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kesl
```

La colonne 6 reprend le volume de mémoire résidente – `2.302g`.

La colonne 9 reprend le pourcentage d'utilisation des cœurs du processeur – 120.0, où chaque cœur est utilisé à 100 %. Ainsi, 120 % signifie qu'un processeur est occupé à 100 % et le deuxième, à 20 %.

Si l'exécution de l'application Kaspersky Endpoint Security ralentit considérablement votre système, vous devez déterminer quels modules et tâches de l'application occupent des ressources système. Pour ce faire, effectuez les tests suivants sur l'appareil à l'aide de la ligne de commande :

1. Analysez la consommation de ressources de la tâche Protection contre les fichiers malicieux (tâche de type OAS). Par conséquent, vous serez en mesure de déterminer si les problèmes de performances sont liés à la tâche Protection contre les fichiers malicieux ou aux tâches d'analyse (tâches de type ODS et ContainerScan) et de mettre en œuvre des recommandations pour les tâches correspondantes.

2. Identifiez les objets les plus fréquemment vérifiés. Vous pouvez optimiser les performances de l'application en excluant les objets et fichiers non dangereux de l'analyse.

L'analyse des performances des tâches est effectuée à l'aide de la ligne de commande. Si l'appareil est administré par une stratégie de Kaspersky Security Center, il faut autoriser l'administration des tâches locales lors de l'étude.

Analyse de la consommation de ressources par la tâche Protection contre les fichiers malicieux

Pour analyser la consommation de ressources par la tâche Protection contre les fichiers malicieux :

1. Arrêtez toutes les tâches d'analyse et de surveillance.

2. Assurez-vous que les tâches d'analyse à la demande (tâches de types ODS et ContainerScan) ne sont pas planifiées pour s'exécuter pendant l'analyse :

   a. Pour obtenir la liste de toutes les applications en cours d'exécution, exécutez la commande suivante :

   ```
   kesl-control --get-task-list
   ```

   b. Obtenez les paramètres de planification pour toutes les tâches de types ODS et ContainerScan en exécutant la commande suivante :

   ```
   kesl-control --get-schedule <ID/nom de la tâche>
   ```

   Si la commande renvoie `RuleType=Manual`, la tâche est uniquement exécutée manuellement.

   c. Pour toutes les tâches dont la valeur du paramètre `RuleType` est autre que `Manual`, modifiez la planification de démarrage en exécutant la commande suivante :

   ```
   kesl-control --set-schedule <ID/nom de la tâche> RuleType=Manual
   ```

3. Pour activer la création d'un fichier de traçage de l'application au niveau de détail le plus élevé, exécutez la commande suivante :

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

4. Pour lancer la tâche Protection contre les fichiers malicieux, au besoin, exécutez la commande suivante :

   ```
   kesl-control --start-task 1
   ```

5. Créez une charge sur le système dans le mode qui a provoqué les problèmes de performance. Quelques heures suffisent.

6. Analysez les fichiers de traçage résultants. Par défaut, les fichiers de traçage sont enregistrés dans le répertoire /var/log/kaspersky/kesl.

   Quand elle est soumise à une charge, l'application enregistrer beaucoup d'information dans les fichiers de travail. Par défaut, le système conserver 10 fichiers de 500 Mo chacun. Pour cette raison, les informations les plus anciennes sont supprimées.

   Si les problèmes de performances et de consommation de ressources persistent, il peut être nécessaire d'optimiser la Protection contre les fichiers malicieux.

   Si les problèmes de performances et de consommation de ressources ne se produisent plus, les problèmes sont probablement causés par des tâches d'analyse à la demande (tâches de types ODS et ContainerScan). Il est nécessaire d'optimiser le travail de ces tâches.

7. Pour désactiver la création de fichiers de traçage de l'application, exécutez la commande suivante :

   ```
   kesl-control --set-app-settings TraceLevel=None
   ```

Identifier les objets les plus fréquemment vérifiés

Pour obtenir la liste des objets le plus souvent analysés, exécutez la commande suivante :

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c |
sort -k1 -n -r|less
```

Le résultat s'affiche dans le programme de visionnage de texte less. Les objets les plus souvent analysés apparaissent en début de fichier.

Si vous devez agréger des statistiques sur la vérification des objets dans les répertoires pour une certaine profondeur d'imbrication de répertoire, à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X est la profondeur d'imbrication spécifiée, par exemple :

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 |
sort | uniq -c | sort -k1 -n -r|less
```

Si divers services enregistrent souvent des fichiers, ces fichiers seront à nouveau analysés dans la fille d'attente. Pour obtenir la liste des chemins d'accès analysés le plus souvent dans la file d'attente, exécutez la commande suivante :

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk
'{print $10}' | sort | uniq -c | sort -k1 -n -r
```

Les fichiers analysés le plus souvent apparaissent en début de liste.

Si vous devez agréger des statistiques sur la vérification des objets dans les répertoires pour une certaine profondeur d'imbrication de répertoire, à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X est la profondeur d'imbrication spécifiée, par exemple :

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk
'{print $10}' | tr -d ',' | cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

Il est recommandé de déterminer si les objets et les fichiers qui ont été analysés le plus souvent sont dangereux. Vous pouvez ajouter des objets et des fichiers non dangereux aux exclusions pour optimiser la Protection contre les fichiers malicieux et les tâches d'analyse. Par exemple, les fichiers de base de données, les répertoires et les fichiers journaux peuvent être considérés comme sûrs s'ils sont écrits par un processus de confiance. En cas de difficultés, contactez le Support technique.

Recommandations pour la Protection contre les fichiers malicieux et les tâches d'analyse

Optimisation de la Protection contre les fichiers malicieux

Pour optimiser le fonctionnement du module Protection contre les fichiers malicieux, vous pouvez procéder comme suit :

- Configurer des exclusions d'analyse pour les objets qui sont analysés le plus fréquemment et qui ne sont pas dangereux.
- Configurer les exclusions à partir de l'interception des opérations de fichiers.
- Modifier le mode d'analyse des fichiers afin que l'analyse soit effectuée uniquement lorsqu'un fichier est ouvert. Par défaut, l'application vérifie le fichier lorsque vous essayez de l'ouvrir et à nouveau lorsque vous essayez de le fermer si le fichier a été modifié. Vous pouvez modifier le mode d'analyse des fichiers dans les paramètres de la Protection contre les fichiers malicieux :
  - Dans la stratégie utilisant Web Console ou la Console d'administration : définissez la valeur **À l'accès** pour le paramètre **Mode de la Protection contre les fichiers malicieux**.
  - Localement sur l'appareil à l'aide de la commande :

    ```
    kesl-control --set-set 1 ScanByAccessType=Open
    ```

  Les modifications introduites dans le fichier après l'ouverture ne seront pas analysées avant la prochaine consultation du fichier.
- Assurez-vous que l'analyse des archives est désactivée (valeur par défaut). L'analyse des archives réduit les performances du fait que l'accès au fichier d'archive est bloqué avant que le fichier ne soit décompressé dans un répertoire /tmp temporaire et analysé. Les archives comprennent à la fois des archives traditionnelles et des objets compactés de type .jar.

  Vous pouvez activer ou désactiver l'analyse des archives à l'aide de Web Console ou de la Console d'administration (paramètre **Analyser les archives**) ou localement sur l'appareil à l'aide de la ligne de commande (paramètre `ScanArchived`).
- Définissez une limite sur la quantité de RAM utilisée par une application.

Optimisation des tâches d'analyse

Pour optimiser les performances des tâches d'analyse (tâches de types ODS et ContainerScan), vous pouvez procéder comme suit :

- Configurez un calendrier d'exécution des tâches d'analyse afin que les tâches s'exécutent à des moments différents. L'application vous permet d'exécuter des tâches d'analyse simultanément, mais la consommation de ressources peut augmenter considérablement. Vérifiez la planification de toutes les tâches de types ODS et ContainerScan localement sur l'appareil ou via Kaspersky Security Center.
- Lancer l'analyse quand le serveur est soumis à la charge la moins importante.
- Assurez-vous que la zone des tâches d'analyse n'inclut pas les répertoires distants montés sur l'appareil via les protocoles SMB et NFS. Il est recommandé de vérifier ces répertoires directement sur l'appareil fournissant la ressource. Si cela n'est pas possible, n'effectuez pas l'analyse sur les serveurs avec des services critiques, car une telle tâche peut prendre beaucoup de temps (en fonction de la vitesse de connexion et du nombre de fichiers).
- Configurer des exclusions d'analyse pour les objets qui sont analysés le plus fréquemment et qui ne sont pas dangereux.
- Configurer les exclusions à partir de l'interception des opérations de fichiers.
- Définissez une limite sur la quantité de RAM utilisée par une application.

Configuration des exclusions de l'analyse

Les exclusions de vérification aident à maintenir un équilibre entre la sécurité et les performances du système. Selon les experts en virus de Kaspersky, vous pouvez ajouter en toute sécurité des fichiers de données et des fichiers d'index de base de données aux exclusions. Il est considéré qu'il n'y a aucun risque de pénétration de virus à travers de tels fichiers.

Vous pouvez exclure les objets non dangereux de la liste des objets les plus fréquemment analysés.

Les exclusions peuvent être configurées par chemin (y compris le type de montage), masque de fichier, type de menace et chemin d'accès au processus effectuant les opérations de fichier.

> L'application ne vérifie pas les objets exclus de l'analyse, mais des retards minimes dans les opérations sur les fichiers sont présents, car l'application intercepte et bloque toujours les opérations sur les fichiers. Si même des retards minimes dans le fonctionnement du système sont critiques, il est recommandé de configurer des exclusions à l'interception des opérations sur les fichiers.

Vous pouvez configurer des exclusions pour la Protection contre les fichiers malicieux dans une stratégie à l'aide de Web Console ou de la Console d'administration, ou localement sur l'appareil à l'aide de la ligne de commande.

Vous pouvez également configurer des exclusions pour les tâches d'analyse avec les ODS et ContainerScan. Les exclusions sont définies dans les paramètres des tâches dans Kaspersky Security Center ou localement sur l'appareil à l'aide de la ligne de commande.

> Les paramètres d'exclusion d'analyse pour une tâche d'analyse n'affectent pas les autres tâches d'analyse. Chaque tâche d'analyse nécessite que vous configuriez ses propres exclusions.

Vous trouverez ci-dessous des exemples de configuration des exclusions pour la Protection contre les fichiers malicieux à l'aide de la ligne de commande.

Pour exclure le répertoire /tmp/logs ainsi que tous les sous-dossiers et fichiers, saisissez la commande suivante :

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

Pour exclure un fichier en particulier ou des fichiers en fonction d'un masque situés dans le répertoire /tmp/logs, saisissez la commande :

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

Pour exclure selon un masque récursif tous les fichiers portant l'extension .log du répertoire /tmp/ et de ses sous-répertoires, exécutez la commande suivante :

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Configuration des exclusions à partir de l'interception des opérations de fichiers

Les fichiers exclus de l'analyse peuvent toujours être interceptés par l'application pendant la Protection contre les fichiers malicieux et les tâches d'analyse. L'application intercepte les événements d'opération de fichier et bloque les actions jusqu'à ce que les événements soient traités. Après analyse, l'application peut :

- enlever le blocage et laisser l'opération se dérouler ;
- bloquer l'opération et exécuter les actions spécifiées dans les paramètres de la protection ou d'analyse.

L'interception des événements prend du temps à traiter, ce qui affecte les performances d'autres applications et du système d'exploitation.

Vous pouvez obtenir des statistiques sur les fichiers interceptés par l'application en utilisant la commande :

```
kesl-control --get-statistic --files
```

La commande permet d'afficher des statistiques sur les opérations sur les fichiers interceptées au cours des dernières 24 heures.

Si nécessaire, vous pouvez effectuer une analyse plus détaillée à l'aide des fichiers de traçage de l'application. Par défaut, les fichiers de traçage ne sont pas créés. Vous pouvez activer la création de fichiers de traçage à l'aide de la commande :

```
kesl-control --set-app-settings TraceLevel=Detailed
```

L'activation du traçage peut avoir un impact négatif sur les performances globales du système. Il est recommandé de désactiver la création de fichiers de traçage lorsque le besoin d'enregistrer des traces disparaît.

Vous pouvez désactiver la création de fichiers de traçage à l'aide de la commande :

```
kesl-control --set-app-settings TraceLevel=None
```

En analysant les fichiers de traçage, vous pouvez obtenir une liste des fichiers interceptés par l'application et identifier les chemins où se produisent un grand nombre d'interceptions d'opérations de fichiers. Vous pouvez obtenir une liste des fichiers interceptés en exécutant la commande suivante :

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -
F':' '{print $2}'|sort | uniq -c | sort -k1 -n -r
```

Si vous devez agréger des statistiques sur l'interception des opération de fichiers dans les répertoires pour une certaine profondeur d'imbrication de répertoire, à partir du répertoire racine `/`, vous pouvez ajouter `cut -d/ -f 1-X` à la commande, où X est la profondeur d'imbrication spécifiée, par exemple :

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -
F':' '{print $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
```

Pour exclure les fichiers d'un répertoire particulier non seulement de l'analyse, mais également de l'interception, vous devez exclure le point de montage dans son ensemble. L'exclusion des points de montage (exclusion globale) vous permet d'exclure les répertoires locaux ou distants montés sur l'appareil de l'interception des opérations sur les fichiers.

Pour les chemins qui ne sont pas des points de montage, les exclusions globales n'ont aucun effet.

Les experts de Kaspersky recommandent d'utiliser des exclusions globales si :

- la connexion à une ressource distante montée, telle que NFS ou SMB, est lente ;
- Même les retards minimes dans le fonctionnement du système sont critiques.

Pour protéger les ressources réseau partagées, utilisez l'application Kaspersky Endpoint Security sur l'appareil sur lequel les ressources sont physiquement stockées.

Vous pouvez configurer des exclusions globales dans la stratégie à l'aide de Web Console ou de la Console d'administration, ou localement sur l'appareil à l'aide de la ligne de commande.

Vous trouverez ci-dessous un exemple de configuration d'une exclusion à l'interception d'opérations de fichiers à l'aide de la ligne de commande.

Pour exclure tous les fichiers du répertoire /tmp de l'interception :

1. Si le répertoire n'est pas un point de montage, il faut le transformer en point de montage. Par exemple pour transformer le répertoire /tmp en point de montage, exécutez la commande suivante :

   ```
   mount --bind /tmp/ /tmp
   ```

2. Pour conserver le point de montage après le redémarrage du serveur, ajoutez la ligne suivante au fichier /etc/fstab :

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Pour ajouter le répertoire /tmp aux exclusions globales, saisissez la commande suivante :

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. S'il faut ajouter plusieurs répertoires, augmentez le compteur item_0000 d'une unité (item_0001, item_0002 et ainsi de suite).

Spécification de la restriction d'utilisation de la mémoire par application

Vous pouvez limiter la quantité de la mémoire vive utilisée par Kaspersky Endpoint Security lors de l'analyse des fichiers avec le module Protection contre les fichiers malicieux et lors de l'exécution de tâches d'analyse de type ODS et ContainerScan.

Les limites d'utilisation de la mémoire peuvent être utiles pour les systèmes dotés de grandes quantités de la mémoire vive (plus de 5 Go).

Par défaut, la limite d'utilisation de la mémoire de l'application est de 8 192 Mo. Vous pouvez ajuster la quantité de RAM utilisée par l'application :

- Dans la stratégie, utilisez le paramètre **Limite d'utilisation de la mémoire pour les tâches d'analyse (Mo)**.
- Localement sur l'appareil à l'aide du paramètre `ScanMemoryLimit=<quantité de mémoire en mégaoctets>` dans le fichier de configuration kesl.ini.

Si la valeur spécifiée du paramètre est inférieure à 2 Mo, l'application utilise la valeur minimale (2 Mo). Si la valeur spécifiée du paramètre est supérieure à la quantité de mémoire vive de l'appareil, l'application utilisera au maximum 25 % de la mémoire vive. Vous ne pouvez pas modifier cette valeur.

Ce paramètre limite uniquement la quantité de mémoire utilisée lors de l'analyse des fichiers. Cela signifie que la quantité totale de mémoire requise par l'application peut être supérieure à la valeur de ce paramètre.

Recommandations pour la Protection contre les menaces Internet et la Protection contre les menaces réseau

Pour réduire l'impact des modules Protection contre les menaces Internet et Protection contre les menaces réseau sur le fonctionnement des applications, nous vous recommandons d'effectuer les étapes suivantes.

- Configurer le pare-feu du système d'exploitation. Si le système dispose de ses propres règles réseau (ou firewalld) avec des stratégies Drop, alors pour que l'application fonctionne correctement, vous devez ajouter une règle d'autorisation pour autoriser les connexions entrantes depuis l'appareil local (loopback).

Exemple de la commande pour iptables :

```
iptables -A INPUT -i lo -j ACCEPT
```

- Pour garantir la compatibilité d'une règle REDIRECT (par exemple, redirection du port 443 vers 8443) avec les règles d'interception du module Protection contre les menaces réseau :

  a. Supprimer la règle :

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
  ```

  b. Ajouter plutôt les règles suivantes :

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400
  -j REDIRECT --to-ports 8443
  ```

  ```
  iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype
  ! --src-type LOCAL -j DNAT --to-destination :8443
  ```

- Configurer la stratégie de vérification des certificats. Par défaut, le module Protection contre les menaces Internet décrypte et inspecte le trafic réseau transmis via des connexions chiffrées. Dans ce cas, le module peut utiliser Internet pour vérifier et télécharger les chaînes manquantes nécessaires à la vérification du certificat. Si l'appareil n'a pas d'accès direct à Internet, vous devez choisir une méthode locale de vérification des certificats par l'application (sans utiliser Internet) ou utiliser un serveur proxy pour accéder à Internet.

  Vous pouvez sélectionner une méthode locale pour vérifier les certificats dans les paramètres d'analyse du trafic réseau :

  - Dans la stratégie utilisant Web Console ou la Console d'administration : définissez la valeur **Vérification locale** pour le paramètre **Stratégie de vérification du certificat**.

  - Localement sur l'appareil à l'aide de la commande :

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  L'application n'utilisera pas Internet pour vérifier les certificats.

  Vous pouvez activer l'utilisation d'un serveur proxy et configurer ses paramètres dans une stratégie à l'aide de Web Console, de la Console d'administration ou localement à l'aide de la ligne de commande.

- Limiter la liste des ports réseau contrôlés par l'application. Par défaut, l'application surveille uniquement les ports réseau sélectionnés. Si l'appareil utilise une connexion SMB, assurez-vous que la valeur par défaut est utilisée :

  - Dans la stratégie de Web Console ou dans la Console d'administration : sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés** dans les paramètres d'analyse du trafic réseau.

  - Localement sur l'appareil : le paramètre d'analyse du trafic réseau `MonitorNetworkPort` est défini sur `Selected`.

Lorsque vous utilisez l'application avec l'équilibreur de charge HAProxy, il est recommandé d'effectuer les étapes suivantes :

1. Ouvrez le fichier de configuration /var/opt/kaspersky/kesl/common/kesl.ini, créez la section `[Environment]` et ajoutez-y le paramètre `TcpSynInterceptDisabled=1`.

2. Redémarrer l'application :

   ```
   systemctl restart kesl
   ```

Le fonctionnement conjoint des modules Protection contre les menaces Internet et Protection contre les menaces réseau et de la conteneurisation Kubernetes nécessite une configuration supplémentaire fine et laborieuse du pare-feu du système d'exploitation. La collaboration n'est pas possible lors de l'utilisation de Kubernetes avec Cillium CNI.

Mise à jour d'une ancienne version de l'application

Vous pouvez réaliser la mise à jour vers Kaspersky Endpoint Security 12.4 for Linux uniquement depuis Kaspersky Endpoint Security 12.3 for Linux.

Il n'est pas possible de mettre à jour Kaspersky Endpoint Security des versions antérieures vers la version 12.4. Si vous disposez d'une version antérieure de Kaspersky Endpoint Security, vous devez d'abord la désinstaller, puis installer Kaspersky Endpoint Security 12.4 for Linux.

Avant de lancer la mise à jour de l'application Kaspersky Endpoint Security, vous devez réaliser les préparatifs d'installation :

La procédure de mise à jour de l'application comprend les étapes suivantes :

1. **Mise à jour de l'Agent d'administration de Kaspersky Security Center**

   Si vous gérez l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, vous devez mettre à jour l'Agent d'administration sur les appareils protégés. La mise à jour s'effectue en installant une nouvelle version de l'Agent d'administration.

   > Sur un appareil exécutant le système d'exploitation Astra Linux Special Edition, il est recommandé de mettre à jour l'Agent d'administration à distance à l'aide de Kaspersky Security Center, car la mise à jour à l'aide de la ligne de commande dans la console d'administration de Kaspersky Security Center entraîne la création d'un nouvel exemplaire de cet appareil géré, et l'ancien n'est plus disponible.

   Pendant la mise à jour de l'Agent d'administration, l'application continue de fonctionner correctement.

2. **Mise à jour du plug-in d'administration de Kaspersky Endpoint Security**

   Si vous gérez l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, vous devrez mettre à jour le plug-in Internet d'administration ou le plug-in MMC d'administration de Kaspersky Endpoint Security, selon la Console d'administration de Kaspersky Security Center que vous utilisez.

3. **Mise à jour de l'application et de l'interface graphique sur les appareils protégés**

   Vous devez mettre à jour l'application installée sur les appareils protégés. Pour l'application mise à jour, le mode d'utilisation de l'application sélectionné lors de l'installation est conservé. Si vous souhaitez utiliser l'application dans un mode différent, vous devez désinstaller l'application, puis suivre la procédure d'installation et de configuration initiale de l'application.

   Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode Agent Endpoint Detection and Response et que vous utilisez l'interface graphique de l'application, vous devez également mettre à jour cette dernière.

Vous pouvez mettre à jour l'application et l'interface graphique de l'application des manières suivantes :

- À distance, à l'aide de Kaspersky Security Center.
- Localement, via la ligne de commande.

En cas d'erreur lors de la mise à jour de l'application, la mise à jour est annulée et la version antérieure de l'application est lancée. Dans ce cas, un message d'erreur s'affiche, mais la nouvelle version (rpm/dkpg) apparaît dans le gestionnaire de paquets.

Que l'application Kaspersky Endpoint Security ait été lancé avant le démarrage du processus de mise à jour ou non, si la mise à jour a réussi, une nouvelle version de l'application est lancée.

Lorsque vous mettez à jour une version d'une application, les fichiers de vidage de la version précédente sont supprimés.

Lors de la mise à jour d'une version de l'application, le fichier de la base de données des événements de la version précédente devient le premier fichier des événements dans l'ensemble de fichiers de la version actuelle. Ce fichier sera stocké jusqu'à ce que le nombre d'événements dans les fichiers restants atteigne le nombre maximal spécifié (spécifié dans le paramètre `MaxEventsNumber`). Par conséquent, une situation temporaire peut survenir dans laquelle l'application stocke deux fois plus d'événements que spécifié dans le paramètre `MaxEventsNumber`.

Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent, il est recommandé d'exécuter la tâche de mise à jour des bases de données après la mise à jour de l'application.

À propos de la mise à jour des plug-ins de gestion de Kaspersky Endpoint Security

La mise à jour du plug-in d'administration de Kaspersky Endpoint Security s'effectue en installant une nouvelle version du plug-in d'administration. En fonction de la Console d'administration de Kaspersky Security Center que vous utilisez, vous devrez installer :

- le plug-in Internet d'administration de Kaspersky Endpoint Security ;
- le plug-in MMC d'administration de Kaspersky Endpoint Security.

Les stratégies et les tâches configurées pour les versions précédentes de l'application Kaspersky Endpoint Security ne sont pas compatibles avec la version mise à jour de l'application. Si vous utilisez la Console d'administration de Kaspersky Security Center pour gérer l'application, après avoir mis à jour le plug-in MMC d'administration, vous pouvez convertir les stratégies et les tâches à l'aide de l'Assistant de conversion groupée des stratégies et des tâches de Kaspersky Security Center (pour plus de détails, consultez l'aide de Kaspersky Security Center).

Les stratégies et les tâches converties possèdent la valeur « <Nom de la stratégie ou de la tâche d'origine> (convertie) ».

Dans les stratégies et tâches converties, la plupart des paramètres utilisent les valeurs configurées pour la version précédente de l'application. Certains paramètres ont des valeurs spéciales. Les paramètres qui manquaient dans les stratégies et les tâches de la version précédente prennent des valeurs par défaut dans les stratégies et les tâches converties.

La procédure de conversion des stratégies et des tâches n'est pas disponible dans Kaspersky Security Center Web Console. Si vous utilisez Web Console pour gérer l'application, vous devez créer de nouvelles stratégies et tâches pour l'application dans Kaspersky Security Center. Vous pouvez transférer certaines valeurs des paramètres de stratégie et de tâche d'une version précédente d'une stratégie ou d'une tâche vers une nouvelle en exportant et en important les paramètres.

Les plug-ins d'administration de la version précédente continuent de fonctionner après l'installation d'une nouvelle version des plug-ins d'administration de Kaspersky Endpoint Security. Avec leur aide, vous pouvez gérer la version précédente de l'application Kaspersky Endpoint Security.

Si vous avez mis à jour l'application sur tous les appareils clients, vous pouvez supprimer les plug-ins d'administration de Kaspersky Endpoint Security de la version précédente.

Lors de l'installation d'une nouvelle version du plug-in MMC d'administration de la même version de l'application, vous devez d'abord supprimer le plug-in MMC déjà installé de cette version, puis installer le nouveau plug-in MMC de cette version.

Mise à jour de l'application via Kaspersky Security Center

La mise à jour de l'application et de l'interface graphique est effectuée en installant à distance une nouvelle version des paquets de l'application et de l'interface graphique sur l'appareil protégé.

L'interface utilisateur graphique n'est pas prise en charge si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

La mise à jour à l'aide de Kaspersky Security Center comprend les étapes suivantes :

1. Création d'un paquet d'installation.

   Le paquet d'installation de l'application de Kaspersky Endpoint Security est utilisé pour effectuer l'installation à distance. Vous pouvez créer un paquet d'installation à l'aide de Kaspersky Security Center Web Console ou à l'aide de la Console d'administration.

2. Déploiement de l'application Kaspersky Endpoint Security sur les appareils du réseau de l'organisation.

   Kaspersky Security Center Web Console prend en charge les principales méthodes de déploiement suivantes :

   - Installation de l'application à l'aide de l'assistant de déploiement de protection.
   - Installation de l'application à l'aide de la tâche d'installation à distance de l'application.

   La Console d'administration de Kaspersky Security Center prend en charge les principales méthodes de déploiement suivantes :

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

   Pour une description des procédures de déploiement, consultez l'aide de Kaspersky Security Center.

Mise à jour de l'application via la ligne de commande

La mise à jour d'une application en ligne de commande s'effectue en installant une nouvelle version de l'application sur l'appareil à partir d'un paquet RPM ou DEB selon le type de gestionnaire de paquets.

L'interface utilisateur graphique n'est pas prise en charge si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Si une nouvelle version de l'application modifie les termes du Contrat de licence et/ou de la Politique de confidentialité, vous devez accepter les nouveaux termes lors de la mise à jour de l'application. Veuillez consulter la nouvelle version du Contrat de licence et/ou de la Politique de confidentialité :

- la nouvelle version du Contrat de licence se trouve dans le répertoire ~/.kesl/<version de l'application>/license.<identifiant de la langue> ;
- la nouvelle version de la Politique de confidentialité se trouve dans le répertoire ~/.kesl/<version de l'application>/license.<identifiant de la langue>.

Si vous n'acceptez pas les termes du Contrat de licence et/ou de la Politique de confidentialité, l'application ne sera pas mise à jour.

Si les conditions de la déclaration de Kaspersky Security Network ont changé dans la nouvelle version de l'application, vous devez accepter ou refuser les nouvelles conditions d'utilisation de Kaspersky Security Network. Consultez la nouvelle version du document située dans le répertoire ~/.kesl/<version de l'application>/ksn_license.<ID de langue>. Le rejet de l'utilisation de Kaspersky Security Network n'entraîne pas l'arrêt de la mise à jour de l'application Kaspersky Endpoint Security. Vous pouvez activer, désactiver ou modifier le mode de Kaspersky Security Network ultérieurement.

Si vous avez utilisé KSN dans la version précédente de l'application et avez accepté les termes de la déclaration de Kaspersky Security Network, vous devez accepter les termes de la déclaration de Kaspersky Security Network lors de la mise à jour de la version de l'application. Dans le cas contraire, l'utilisation de KSN sera désactivée.

Pour accepter les termes des nouveaux accords lors de la mise à jour, utilisez les variables KESL_EULA_AGREED=yes, KESL_PRIVACY_POLICY_AGREED=yes et KESL_USE_KSN=yes/no.

Pour mettre à jour l'application :

1. Installez le paquet d'application à l'aide de la commande suivante en fonction du type de gestionnaire de paquets. Si une version précédente de l'interface graphique de l'application est installée, vous devez également installer le paquet contenant les fichiers de l'interface graphique de l'application.

   - Pour le paquet RPM :

     ```
     # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.4.0-<numéro de build>.<arch>.rpm [kesl-gui-12.4.0-<numéro de build>.<arch>.rpm]
     ```

où <arch> désigne le type d'architecture :

- i386, pour les systèmes d'exploitation 32 bits
- x86_64, pour les systèmes d'exploitation 64 bits
- aarch64, pour les systèmes d'exploitation 64 bits pour l'architecture Arm

Si vous disposez d'un paquet de l'application et d'un paquet de l'interface graphique installés sur un système d'exploitation avec le gestionnaire de paquets de type rpm, il n'est pas recommandé de mettre à jour un seul des paquets.

- Pour le paquet DEB :

  `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.4.0-<numéro de build>_<arch>.deb [./kesl-gui_12.4.0-<numéro de build>_<arch>.deb]`

  où <arch> désigne le type d'architecture :

  - i386, pour les systèmes d'exploitation 32 bits
  - amd64, pour les systèmes d'exploitation 64 bits
  - arm64, pour les systèmes d'exploitation 64 bits pour l'architecture Arm

  Si un paquet de l'application et un paquet de l'interface utillisateur graphique sont installés sur un système d'exploitation avec le gestionnaire de paquets de type dpkg, il n'est pas possible de mettre à jour un seul des paquets.

2. L'application Kaspersky Endpoint Security redémarre automatiquement.

Exemple :
Mettre à jour le paquet de l'application au format RPM avec un paquet de l'interface utilisateur graphique pour les systèmes d'exploitation 64 bits *:*

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.4.0-<numéro de build>.x86_64.rpm kesl-gui-12.4.0-<numéro de build>.x86_64.rpm
```

Si vous utilisez la ligne de commande pour gérer l'application, après la mise à niveau, la plupart des paramètres de l'application utilisent les valeurs configurées pour la version précédente de l'application. Certains paramètres ont des valeurs spéciales. Les paramètres qui manquaient dans la version précédente de l'application reprennent des valeurs par défaut dans la nouvelle version de l'application.

Les modifications apportées aux paramètres de l'application après la fin de la mise à jour et avant le redémarrage de l'application ne sont pas enregistrées.

Particularités de définition des valeurs des paramètres lors de la mise à jour de l'application

Si vous utilisez la Console d'administration de Kaspersky Security Center pour gérer l'application, vous pouvez convertir les stratégies et les tâches pour utiliser les valeurs des paramètres des stratégies et des tâches configurés pour la version précédente de l'application (pour plus de détails, consulter l'aide de Kaspersky Security Center). La procédure de conversion des stratégies et des tâches n'est pas disponible dans Kaspersky Security Center Web Console.

Lorsque vous mettez à jour une application à l'aide de la ligne de commande, la plupart des paramètres reprennent leurs valeurs de la version précédente de l'application. Vous pouvez également migrer les paramètres de l'application en exportant les paramètres vers un fichier et en les important à partir d'un fichier.

Les paramètres qui manquaient dans la version précédente de l'application prennent des valeurs par défaut. Certains paramètres ont des valeurs spéciales.

Sources de mise à jour des bases de données

Les modifications suivantes ont été apportées aux tâches de mise à jour des bases de données dans la nouvelle version de l'application :

- Le paramètre **Utiliser les serveurs de mises à jour Kaspersky si les autres sources sont inaccessibles** (`UseKLServersWhenUnavailable`) est supprimé. Vous pouvez configurer cette fonctionnalité à l'aide d'autres paramètres de la tâche.

- Vous pouvez spécifier plusieurs sources de mise à jour des bases de données simultanément. L'application utilise ces sources de mise à jour dans l'ordre dans lequel elles apparaissent dans la liste des sources.

Après la conversion des tâches dans le plug-in MMC, les sources de mises à jour sont configurées comme suit :

- Si l'option **Serveurs de mises à jour Kaspersky** était sélectionnée dans la version précédente, la case **Serveurs de mises à jour Kaspersky** sera cochée dans la liste des sources.

- Si l'option **Kaspersky Security Center** était sélectionnée dans la version précédente, la case **Kaspersky Security Center** sera cochée dans la liste des sources.

  Si la case **Utiliser les serveurs de mises à jour Kaspersky si les autres sources de mises à jour sont indisponibles** était cochée dans la version précédente, la case **Serveurs de mises à jour Kaspersky** sera également cochée dans la liste des sources, et la source **Kaspersky Security Center** sera déplacée en haut de la liste.

- Si une source personnalisée était configurée dans la version précédente (option **Autre sources sur le réseau local ou global**), cette source avec ses paramètres (chemin ou adresse Internet) sera ajoutée à la liste des sources et cette case sera cochée.

  Si la case **Utiliser les serveurs de mises à jour Kaspersky si les autres sources de mises à jour sont indisponibles** était cochée dans la version précédente, la case **Serveurs de mises à jour Kaspersky** sera également cochée dans la liste des sources, et la source utilisateur sera déplacée en haut de la liste.

La conversion des stratégies n'est pas prise en charge dans le plug-in Web.

Après la mise à jour de l'application à l'aide de la ligne de commande, les sources de mises à jour sont configurées comme suit :

- Si la valeur `KLServers` était sélectionnée pour le paramètre `SourceType` dans la version précédente, la source de mise à jour est créée dans la section **[Sources]** : `SourceType=KLServers`, `Enabled=Yes`.

- Si la valeur `SCServer` était sélectionnée pour le paramètre `SourceType` dans la version précédente, la source de mise à jour est créée dans la section **[Sources]** : `SourceType=SCServer`, `Enabled=Yes`.

  Dans ce cas, si la valeur du paramètre `UseKLServersWhenUnavailable=Yes` a été définie dans la version précédente, une deuxième source de mise à jour est créée dans la section **[Sources]** : `SourceType=KLServers`, `Enabled=Yes`.

- Si, dans la version précédente, `SourceType` était défini sur `Custom` et que la source personnalisée était configurée dans la section **[CustomSources.item_#]**, une source de mise à jour personnalisée est créée dans la section **[Sources]** : `SourceType=Custom`, `URL=<chemin d'accès ou adresse Internet de la source>`, `Enabled=Yes`.

  Dans ce cas, si la valeur du paramètre `UseKLServersWhenUnavailable=Yes` a été définie dans la version précédente, une deuxième source de mise à jour est créée dans la section **[Sources]** : `SourceType=KLServers`, `Enabled=Yes`.

Paramètres d'interception des événements système

Si le mécanisme d'interception des événements système basé sur le module de noyau mis à jour était sélectionné dans la version précédente de l'application, après la mise à jour, l'application utilise la technologie fanotify pour intercepter les événements système. Ensuite, après la mise à jour des bases et des modules de l'application et un redémarrage automatique, l'application revient à l'utilisation du module de noyau mis à jour.

Paramètres de Kaspersky Security Network

Après la conversion d'une stratégie dans le plugin MMC, les paramètres d'utilisation de Kaspersky Security Network dans les propriétés de la stratégie dépendent de si vous avez accepté ou refusé les conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion des stratégies et des tâches :

- Si vous avez accepté les conditions de la Déclaration, l'option **Mode étendu de KSN** est sélectionnée.

- Si vous avez rejeté les conditions de la Déclaration, l'option **Ne pas utiliser KSN** est sélectionnée.

La conversion des stratégies n'est pas prise en charge dans le plug-in Web.

Après la mise à jour d'une application à l'aide de la ligne de commande, le paramètre `UseKSN` est défini sur `No` si lors de la mise à jour vous avez défini la valeur du paramètre `KESL_USE_KSN=No`, et est défini sur `UseKSN=Extended` si vous avez défini la valeur du paramètre `KESL_USE_KSN=Yes`. Dans d'autres cas, la valeur du paramètre `UseKSN` ne change pas après la mise à jour.

Paramètres d'utilisation du mode cloud

Après la conversion d'une stratégie dans le plug-in MMC, les paramètres d'utilisation du mode cloud peuvent changer selon le fait que vous avez accepté ou refusé les conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion des stratégies et des tâches :

- Si vous avez accepté les conditions de la Déclaration, la case **Activer le mode cloud** sera cochée.
- Si vous refusez les conditions de la Déclaration, la case **Activer le mode cloud** sera décochée.

La conversion des stratégies n'est pas prise en charge dans le plug-in Web.

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `CloudMode` est défini sur les valeurs suivantes :

- `CloudMode=No`, si le paramètre `UseKSN=No` après la mise à jour ;
- `CloudMode=Yes` si `UseKSN=Basic/Extended` a été défini après la mise à jour et `CloudMode=Yes` a été défini avant la mise à jour.

Le mode Cloud est disponible si l'utilisation de KSN est activée. Pour activer le mode cloud, vous avez besoin de :

- sélectionner l'option **Mode étendu de KSN** et cocher la case **Activer le mode cloud** lorsque vous utilisez le plug-in MMC ou Internet ;
- lors de l'utilisation de la ligne de commande, définir la valeur `Basic` ou `Extended` pour le paramètre `UseKSN` et la valeur `Yes` pour le paramètre `CloudMode`.

Paramètres d'intégration avec Kaspersky Managed Detection and Response

Si le module MDR a été activé, après la conversion de la stratégie dans le plug-in MMC, l'état du module MDR dépend de votre acceptation ou de votre rejet des conditions de la Déclaration de Kaspersky Security Network dans l'Assistant de conversion de stratégie et de tâche :

- Si vous avez accepté les conditions de la Déclaration, le module MDR restera activé (la case **Activer Managed Detection and Response** est cochée).
- Si vous avez rejeté les conditions de la Déclaration, la case **Activer Managed Detection and Response** sera décochée.

La conversion des stratégies n'est pas prise en charge dans le plug-in Web.

Après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `UseMDR` est défini sur les valeurs suivantes :

- `UseMDR=No`, si le paramètre `UseKSN=No` après la mise à jour ;
- `UseMDR=Yes` si `UseKSN=Basic/Extended` a été défini après la mise à jour et `UseMDR=Yes` a été défini avant la mise à jour.

Si vous souhaitez utiliser la fonctionnalité Kaspersky Managed Detection and Response, vous devez activer l'utilisation de Kaspersky Security Network en mode avancé.

Suppression d'une application

La procédure de désinstallation de l'application Kaspersky Endpoint Security comprend les étapes suivantes :

1. **Suppression de l'application et de l'interface graphique de l'application**

   Vous devez supprimer les paquets de l'application et les paquets de l'interface graphique de l'application depuis les appareils protégés, si vous avez utilisé une interface graphique.

   Vous pouvez supprimer le paquet de l'application et le paquet de l'interface graphique en même temps, ou vous pouvez désinstaller uniquement le paquet de l'interface graphique. Il est impossible de supprimer uniquement le paquet de l'application si le paquet de l'interface graphique est installé.

   Vous pouvez supprimer l'application et l'interface graphique de l'application des manières suivantes :

   - À distance, à l'aide de Kaspersky Security Center.
   - Localement, via la ligne de commande.

   > Pendant le processus de désinstallation de l'application, toutes les tâches de Kaspersky Endpoint Security sur l'appareil seront arrêtées.

2. **Suppression de l'Agent d'administration**

   Si vous avez utilisé Kaspersky Security Center pour gérer l'application Kaspersky Endpoint Security, vous devez supprimer l'Agent d'administration des appareils protégés.

   Vous pouvez désinstaller l'Agent d'administration des manières suivantes :

   - À distance, à l'aide de Kaspersky Security Center.
   - Localement, via la ligne de commande.

3. **Suppression du plug-in d'administration de Kaspersky Endpoint Security**

   Si vous avez utilisé Kaspersky Security Center pour gérer l'application Kaspersky Endpoint Security, vous devez supprimer le plug-in Web d'administration ou le plug-in MMC d'administration de Kaspersky Endpoint Security, selon la Console d'administration de Kaspersky Security Center que vous avez utilisée.

> Après la désinstallation de l'application, toutes les informations enregistrées pendant son exécution sont supprimées, à l'exception de la base de données des licences. Les certificats installés de l'application sont également supprimés. La base de données de licences est conservée et vous pouvez l'utiliser pour réinstaller l'application. L'ID unique de l'installation de l'application (SensorID) est également enregistré.

Si l'application a été installée sur un système systemd, une fois l'application désinstallée, les paramètres systemd reprennent leur valeur d'origine.

À propos de la désinstallation d'une application et de l'Agent d'administration à l'aide de Kaspersky Security Center

Vous pouvez supprimer à distance l'application Kaspersky Endpoint Security et l'Agent d'administration des appareils clients.

La désinstallation s'effectue à l'aide de la tâche de désinstallation de l'application à distance dans Kaspersky Security Center Web Console ou dans la Console d'administration. Pour en savoir plus, consultez l'Aide de Kaspersky Security Center.

Si vous souhaitez supprimer uniquement l'interface utilisateur graphique sans supprimer l'application, vous devez utiliser le paramètre `USE_GUI=No` dans le fichier de configuration autoinstall.ini et lancer la tâche d'installation à distance de l'application.

La suppression s'effectue en arrière-plan. Une fois la suppression terminée, vous serez invité à redémarrer l'appareil client.

Suppression de l'application via la ligne de commande

Suppression du paquet de l'application et du paquet de l'interface utilisateur graphique

Pour supprimer Kaspersky Endpoint Security et l'interface utilisateur graphique, installés à l'aide d'un paquet au format RPM, exécutez la commande suivante :

```
# rpm -e kesl kesl-gui
```

Pour supprimer Kaspersky Endpoint Security et l'interface utilisateur graphique, installés à l'aide d'un paquet au format DEB, exécutez la commande suivante :

```
# apt-get purge kesl kesl-gui
```

Suppression du paquet de l'application sans supprimer le paquet de l'interface utilisateur graphique

Pour supprimer l'application installée à l'aide d'un paquet au format RPM, sans supprimer l'interface graphique de l'application, exécutez la commande suivante :

```
# rpm -e kesl
```

Pour supprimer l'application installée à l'aide d'un paquet au format DEB, sans supprimer l'interface graphique de l'application, exécutez la commande suivante :

```
# apt-get purge kesl
```

Suppression du paquet de l'interface utilisateur graphique

Pour supprimer l'interface graphique de l'application installée à l'aide d'un paquet au format RPM, exécutez la commande suivante :

```
# rpm -e kesl-gui
```

Pour supprimer l'interface graphique de l'application installée à l'aide d'un paquet au format DEB, exécutez la commande suivante :

```
# apt-get purge kesl-gui
```

Une fois la procédure de suppression terminée, un message sur les résultats de la suppression s'affiche.

Suppression de l'Agent d'administration à l'aide de la ligne de commande

Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# rpm -e klnagent
```

Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# rpm -e klnagent64
```

Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :

```
# apt-get purge klnagent
```

Pour supprimer l'Agent d'administration installé à l'aide d'un paquet au format DEB sur un système d'exploitation 64 bits, exécutez la commande suivante :

```
# apt-get purge klnagent64
```

Une fois la procédure de suppression terminée, un message sur les résultats de la suppression s'affiche.

Suppression des plug-ins d'administration de Kaspersky Endpoint Security

Le plug-in Internet d'administration de Kaspersky Endpoint Security est supprimé dans Kaspersky Security Center Web Console dans la liste des plug-ins installés (**Paramètres** → **Plug-ins Internet**).

Pour supprimer le plug-in MMC d'administration de Kaspersky Endpoint Security :

1. Fermez la Console d'administration de Kaspersky Security Center.
2. Sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée, ouvrez l'éditeur du registre Windows et accédez à :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   Cette branche contient des données sur tous les plug-ins d'administration installés dans la Console d'administration. Le nom de l'application gérée se trouve dans le paramètre **DisplayName**.
3. Sélectionnez la section qui correspond au plug-in de l'application Kaspersky Endpoint Security de la version requise.
4. Ouvrez le paramètre **UninstallString** et copiez sa valeur.
5. Ouvrez la ligne de commande avec les droits d'administrateur, collez la valeur copiée et appuyez sur la touche **Enter**.

Licence de l'application

Cette section contient des informations sur les concepts de base associés à l'octroi de licences aux applications de Kaspersky, ainsi que des informations sur les fonctionnalités d'activation de l'application Kaspersky Endpoint Security.

Après avoir activé l'application, il est recommandé de surveiller la période de validité de la licence utilisée par l'application afin de renouveler la licence dans les meilleurs délais. Vous pouvez afficher des informations sur les clés de licence utilisées par Kaspersky Endpoint Security à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande sur un appareil protégé.

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 de l'application que vous avez achetée.

Veuillez lire attentivement les termes du Contrat de licence avant d'utiliser l'application.

Vous pouvez prendre connaissance du Contrat de licence utilisateur final et de la Politique de confidentialité, qui décrit le traitement et la mise à disposition des données :

- Avant d'installer l'application, dans le fichier license.<identifiant de langue>. Ce fichier est fourni dans le kit de distribution de l'application.
- Pendant l'installation de l'application Kaspersky Endpoint Security.

  En confirmant votre consentement au texte du Contrat de licence utilisateur final et de la Politique de confidentialité lors de la création du paquet d'installation de l'application (si l'installation est effectuée à l'aide de Kaspersky Security Center) ou pendant la configuration initiale de l'application (si l'installation est effectuée à l'aide de la ligne de commande), vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous n'acceptez pas les conditions du Contrat de licence utilisateur final ou de la Politique de confidentialité, vous devez annuler l'installation de l'application et ne pouvez pas utiliser l'application.

- Après l'installation de l'application, les fichiers contenant les textes du Contrat de licence utilisateur final de l'application Kaspersky et de la Politique de confidentialité se trouvent sur l'appareil protégé dans le répertoire /opt/kaspersky/kesl/doc/license.<identifiant de langue>.

À propos de la licence

Licence est un droit d'utilisation limité dans le temps de Kaspersky Endpoint Security, qui vous est accordé selon les termes du contrat de licence conclu (Contrat de licence).

La liste des fonctions disponibles et la durée d'utilisation de l'application dépendent de la licence sous laquelle l'application est utilisée.

Les types de licence suivants sont proposés :

- *Évaluation*

  Licence gratuite destinée à tester l'application. La licence d'évaluation a une courte durée.

  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, il faut acheter une licence commerciale.

  Vous ne pouvez utiliser l'application sous une licence d'essai que pour une seule période d'essai.

- *Commercial*

  Licence payante.

  Après l'expiration de la licence commerciale, l'application cesse d'exercer ses fonctions principales. Pour continuer à utiliser Kaspersky Endpoint Security, vous devez renouveler la licence commerciale. Une fois votre licence expirée, vous ne pouvez plus utiliser l'application et devez la supprimer de votre appareil.

  Il est conseillé de renouveler la période de validité de la licence avant sa date d'expiration afin de garantir une protection continue des appareils contre les menaces de sécurité informatique.

Pour activer l'application Kaspersky Endpoint Security, une licence est requise, qui inclut les fonctionnalités de base de l'application. La licence de base peut également inclure des fonctionnalités supplémentaires de l'application (par exemple, des fonctionnalités d'intégration avec les solutions Detection and Response de Kaspersky). Si la licence de base sous laquelle vous utilisez l'application n'inclut pas les fonctionnalités supplémentaires dont vous avez besoin, vous devrez acheter une licence distincte pour activer les fonctionnalités supplémentaires.

Veuillez vérifier auprès du partenaire de Kaspersky auprès duquel vous achetez la licence l'étendue des fonctionnalités incluses dans la licence de base et dans la licence pour les fonctionnalités supplémentaires.

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 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. La clé de licence est créée par les spécialistes de Kaspersky.

Pour activer l'application, vous avez besoin d'une clé de licence de base. Si la licence de base sous laquelle vous utilisez l'application n'inclut pas les fonctionnalités supplémentaires dont vous avez besoin (par exemple, la fonctionnalité Kaspersky Endpoint Detection and Response Optimum), vous avez également besoin d'une clé de licence pour les fonctionnalités supplémentaires.

Vous pouvez ajouter une clé de licence à un appareil protégé de l'une des manières suivantes : appliquer un *fichier clé* ou saisissez un *code d'activation*. La clé de licence s'affiche dans l'interface de l'application sous la forme d'une séquence alphanumérique unique une fois que vous l'avez ajoutée à l'appareil protégé.

La clé de licence peut être bloquée par Kaspersky en cas de non-respect des termes du contrat de licence utilisateur final. Si la clé de licence est verrouillée, une autre clé de licence doit être ajoutée pour que l'application fonctionne.

La clé de licence peut être ajoutée comme active ou de réserve.

- Une *clé de licence active* est une clé de licence utilisée actuellement par l'application. Une clé de licence pour une licence d'évaluation, une clé pour une licence commerciale (clé commerciale) ou une clé d'abonnement peuvent être ajoutées comme actives. Vous ne pouvez ajouter qu'une seule clé de licence de base en tant que clé active. Il peut y avoir plusieurs clés de licence actives pour des fonctionnalités supplémentaires.

- Une *clé de licence de réserve* est une clé de licence qui permet à l'utilisateur d'utiliser l'application mais qui n'est pas actuellement en cours d'utilisation. La clé de licence de réserve s'active automatiquement lorsque la période de validité de la licence associée à la clé de licence active expire.

  Pour prolonger la période de validité de la licence de base de l'application, vous pouvez ajouter une clé de réserve pour la fonctionnalité de base. Si vous avez activé des fonctionnalités supplémentaires sous une licence distincte, vous pouvez également ajouter une clé de réserve pour les fonctionnalités supplémentaires.

  Une clé de licence de réserve ne peut être ajoutée que s'il existe une clé de licence active du même type.

  > Une clé de licence d'évaluation peut être ajoutée en tant que clé de licence active. Il est impossible d'ajouter la clé de la licence d'évaluation et la clé d'abonnement en guise de clé de réserve.

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. Le code d'activation est envoyé à l'adresse email que vous avez indiquée à l'achat de Kaspersky Endpoint Security ou lors de la commande de la version d'évaluation de Kaspersky Endpoint Security.

Pour activer l'application avec un code d'activation, vous avez besoin d'un accès Internet en vue de vous connecter aux serveurs d'activation Kaspersky.

Si le code d'activation a été perdu après l'activation du programme, contactez le partenaire de 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.

Si un fichier clé a été supprimé par accident, vous pouvez le restaurer. Vous aurez besoin du fichier clé pour ouvrir un Kaspersky CompanyAccount par exemple.

Pour restaurer votre fichier clé, effectuez l'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.

À propos de l'abonnement

L'abonnement à l'application Kaspersky Endpoint Security est un bon de commande pour l'application avec des paramètres définis (date d'expiration de l'abonnement, nombre d'appareils protégés). Vous pouvez commander un abonnement pour l'application Kaspersky Endpoint Security auprès de votre prestataire de services (par exemple, votre FAI). Vous pouvez renouveler l'abonnement ou le résilier. Vous pouvez administrer l'abonnement sur le site du prestataire de services.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour prolonger le fonctionnement de l'application après la date d'expiration d'un abonnement limité, il est nécessaire de renouveler ce dernier. L'abonnement illimité se renouvelle automatiquement si le montant dû au prestataire de services est versé dans les délais.

À l'expiration d'un abonnement limité, une période de grâce peut vous être proposée pour renouveler l'abonnement. Pendant cette période, l'application conserve ses fonctionnalités. C'est le prestataire de services qui décide d'octroyer ou non une période de grâce et en cas d'octroi, il détermine la durée.

Les actions disponibles pour l'administration de l'abonnement peuvent varier en fonction du prestataire de services. Celui-ci peut ne pas offrir de période de grâce pendant laquelle l'application conserve ses fonctions jusqu'au renouvellement de l'abonnement.

Pour utiliser l'application Kaspersky Endpoint Security selon un abonnement, vous devez saisir le code d'activation fourni par le prestataire de services. Une fois que vous avez appliqué un code d'activation à l'application, celle-ci reçoit une clé active qui correspond à la licence d'utilisation de l'application selon l'abonnement. Il est possible d'ajouter une clé de réserve uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé ou d'un abonnement.

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

Comparaison des fonctions de l'application selon la licence

L'ensemble des fonctions disponibles de l'application Kaspersky Endpoint Security dépend du type de licence de base.

La licence de base sous laquelle l'application est utilisée peut inclure à la fois des fonctionnalités de base et supplémentaires de l'application. Par exemple, la licence « Kaspersky Optimum Security » permet d'activer les modules de base de protection et de contrôle, ainsi que la fonctionnalité d'intégration avec Kaspersky Endpoint Detection and Response Optimum.

Pour activer des fonctionnalités supplémentaires de l'application, des licences distinctes peuvent également être utilisées, par exemple une licence pour activer la fonctionnalité Kaspersky Unified Monitoring and Analysis Platform.

Veuillez vérifier auprès du partenaire de Kaspersky auprès duquel vous achetez la licence l'étendue des fonctionnalités incluses dans la licence de base et dans la licence pour les fonctionnalités supplémentaires.

Ouvrir la liste des fonctions de la solution disponibles sous les licences primaires de l'application

Activation des applications et gestion des clés de licence

L'*activation* est une procédure qui permet d'activer une licence qui vous autorise à utiliser une version entièrement fonctionnelle de l'application jusqu'à l'expiration de la licence.

Pour activer l'application Kaspersky Endpoint Security sur un appareil protégé, vous devez ajouter une clé de licence de base à l'application. Si la licence de base sous laquelle vous utilisez l'application n'inclut pas les fonctionnalités supplémentaires de l'application Kaspersky Endpoint Security dont vous avez besoin, vous devrez également ajouter une clé de licence à l'application pour les fonctionnalités supplémentaires :

- une clé de licence distincte de « Kaspersky Endpoint Detection and Response Optimum Add-on » (ci-après également dénommée « clé EDR Optimum ») : pour activer le module EDR Optimum ;
- une clé de licence distincte « Kaspersky Unified Monitoring and Analysis Platform Add-on » (ci-après également dénommée « clé KUMA ») : pour activer la fonctionnalité de Kaspersky Unified Monitoring and Analysis Platform ;

- une clé de licence distincte pour « Kaspersky Managed Detection and Response Optimum/Expert Add-on » (ci-après également dénommée « clé MDR ») : pour activer le module MDR ;
- une clé de licence distincte de Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on (ci-après également dénommée clé EDR Expert (on-premise)) afin d'activer le module EDR Expert (on-premise).

La clé EDR Expert (on-premise) est également utilisée pour activer l'application Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent. Dans ce mode, vous n'avez pas besoin d'ajouter la clé de licence primaire à l'application.

Vous pouvez ajouter des clés de licence à l'application de l'une des manières suivantes :

- en utilisant un fichier clé ;
- en utilisant le code d'activation.

Si l'application Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, il n'est pas nécessaire d'activer l'application. Vous activez la solution Kaspersky Security for Virtualization Light Agent. L'activation s'effectue du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant une clé de licence à la SVM. Une clé de licence pour activer des fonctionnalités supplémentaires est également ajoutée à la SVM si nécessaire.

Si vous n'avez pas activé l'application Kaspersky Endpoint Security lors de l'installation (en ajoutant une clé au paquet d'installation ou lors de l'exécution de la configuration initiale), vous devez activer l'application installée de l'une des manières suivantes :

- À distance via Kaspersky Security Center :
  - Utilisation de la tâche d'ajout d'une clé à l'application.
  - En distribuant une clé de licence située sur le Serveur d'administration aux appareils clients.
- Sur la ligne de commande à l'aide des commandes de gestion.

Pour ajouter une clé de licence à une application pour bénéficier de fonctionnalités supplémentaires, vous pouvez également utiliser la tâche d'ajout d'une clé, la procédure de distribution de clé aux appareils clients ou les commandes de gestion des clés de licence. L'ajout d'une clé pour des fonctionnalités supplémentaires n'est pas différent de l'ajout de la clé de licence de base de l'application.

Si Kaspersky Endpoint Security est utilisé en mode standard, une clé pour des fonctionnalités supplémentaires ne peut être ajoutée qu'après l'ajout de la clé de licence primaire de l'application.

Vous pouvez également ajouter une clé de réserve à l'application pour la fonctionnalité de base de l'application et une clé de réserve pour des fonctionnalités supplémentaires. Une clé de réserve devient active lorsque la licence associée à la clé active expire ou lorsque la clé active est supprimée. La disponibilité d'une clé de réserve permet d'éviter la restriction des fonctionnalités de l'application à l'expiration d'une licence.

La clé de réserve ne peut être ajoutée qu'après l'ajout de la clé de licence active.

Vous pouvez consulter à distance les informations sur les clés de licence ajoutées à l'application à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande sur un appareil protégé.

Vous pouvez également activer l'application et gérer les clés de licence via l'interface utilisateur graphique.

Activation de l'application via Kaspersky Security Center

Vous pouvez ajouter des clés de licence à une application via Kaspersky Security Center des manières suivantes :

- Utilisation de la tâche d'ajout d'une clé à l'application.

  Cette méthode permet d'ajouter une clé de licence à un appareil spécifique ou à des appareils faisant partie d'un groupe d'administration. Lors de la création d'une tâche, la clé ajoutée au stockage des clés de Kaspersky Security Center est utilisée. Vous pouvez ajouter une clé de licence stockage des clés au préalable ou lors de la création d'une tâche d'activation.

- En distribuant aux appareils clients une clé de licence stockée sur le Serveur d'administration de Kaspersky Security Center.

  Cette méthode permet d'ajouter automatiquement une clé aux appareils client déjà connectés à Kaspersky Security Center et aux nouveaux appareils clients. Pour utiliser cette méthode, vous devez d'abord ajouter la clé au stockage des clés de Kaspersky Security Center.

Pour créer une tâche permettant d'ajouter une clé à une application, une tâche permettant d'ajouter une clé à un stockage des clés et une tâche permettant de distribuer une clé aux appareils clients, vous pouvez utiliser Kaspersky Security Center Web Console ou la Console d'administration de Kaspersky Security Center.

Ajout des clés à l'aide de Kaspersky Security Center Web Console

Pour ajouter une clé au stockage des clés de Kaspersky Security Center à l'aide de Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Licences Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, sélectionnez la méthode d'ajout de la clé au stockage :
   - **Saisissez un code d'activation** si vous souhaitez ajouter une clé à l'aide d'un code d'activation.
   - **Ajouter un fichier clé** si vous souhaitez ajouter une clé à l'aide d'un fichier clé.
4. Selon le mode d'ajout de la clé que vous avez sélectionné à l'étape précédente, effectuez l'une des actions ci-dessous :
   - Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.
   - Cliquez sur le bouton **Sélectionner le fichier de clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension .key.
5. Cliquez sur le bouton **Fermer**.

La clé ajoutée apparaîtra dans la liste de clés.

Pour ajouter une clé à l'application via Web Console à l'aide de la tâche Ajouter une clé :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

   b. Dans la liste déroulante **Type de tâche**, sélectionnez **Ajout d'une clé**.

   c. Dans le champ **Nom de la tâche**, saisissez une brève description, telle que `Activation de Kaspersky Endpoint Security`.

   d. Dans la section **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Cliquez sur le bouton **Suivant**.

   La fenêtre **Stockage des clés du Kaspersky Security Center** s'ouvre.

5. Si vous aviez préalablement ajouté la clé dans le stockage des clés de Kaspersky Security Center, choisissez dans la liste la clé et cliquez sur le bouton **Suivant**.

6. Si la clé souhaitée ne se trouve pas dans le stockage de clés, cliquez sur le bouton **Ajouter une clé**.

   a. Dans la fenêtre qui s'ouvre, sélectionnez la méthode d'ajout de la clé au stockage :

      - **Saisissez un code d'activation** si vous souhaitez ajouter une clé à l'aide d'un code d'activation.
      - **Ajouter un fichier clé** si vous souhaitez ajouter une clé à l'aide d'un fichier clé.

   b. Selon le mode d'ajout de la clé que vous avez sélectionné à l'étape précédente, effectuez l'une des actions ci-dessous :

      - Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.
      - Cliquez sur le bouton **Sélectionner le fichier de clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension .key.

   c. Lisez les informations relatives à la clé et cliquez sur le bouton **Fermer**.

   d. La clé ajoutée apparaîtra dans la liste de clés. Sélectionnez-la dans la liste, puis cliquez sur le bouton **Suivant**.

7. Lisez les informations sur la licence et cliquez sur le bouton **Suivant**.

8. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

9. Cochez la case en regard de la tâche. Cliquez sur le bouton **Exécuter**.

Dans les propriétés de la tâche *Ajouter une clé*, vous pouvez ajouter une *clé de réserve* à l'application. Une clé de réserve devient active lorsque la licence associée à la clé active expire ou lorsque la clé active est supprimée. La disponibilité d'une clé de réserve permet d'éviter la restriction des fonctionnalités de l'application à l'expiration d'une licence.

Si vous ajoutez une clé de réserve mais que la clé active n'a pas encore été ajoutée à l'application, la tâche échoue.

Pour ajouter une clé via Web Console en distribuant aux appareils une clé située sur le Serveur d'administration :

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Licences Kaspersky**.
2. Ouvrez les propriétés de la clé en cliquant sur le lien portant le nom de l'application que la clé est censée activer.
3. Dans l'onglet **Général**, cochez la case **Distribuer automatiquement la clé de licence aux appareils administrés**.
4. Cliquez sur le bouton **Enregistrer**.

   La clé de licence est alors distribuée automatiquement aux appareils clients appropriés.

Une nouvelle clé de licence ne sera ajoutée à l'appareil que si l'application sur cet appareil n'est pas encore activée ou si la licence expire dans moins de 14 jours.

Lors de la distribution automatique d'une clé en tant que clé active ou de réserve, la restriction de licence sur le nombre d'appareil (définie dans les propriétés de la clé) est prise en compte. Une fois la restriction de licence atteinte, la distribution de cette clé aux appareils cesse automatiquement. Vous pouvez afficher le nombre d'appareils auxquels la clé a été ajoutée ainsi que d'autres données dans les propriétés de la clé sous l'onglet **Appareils**.

Particularités de l'activation dans Kaspersky Security Center Cloud Console

Une version d'essai est disponible 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 fonctionnalités de Cloud Console. Dans cette version, vous pouvez réaliser des opérations dans l'espace de travail pendant 30 jours. Tous les applications administrées, y compris l'application Kaspersky Endpoint Security, sont automatiquement activés sous la licence d'évaluation de Kaspersky Security Center Cloud Console. Vous ne pouvez pas activer l'application Kaspersky Endpoint Security avec votre propre licence d'évaluation après l'expiration de votre licence d'évaluation pour Cloud Console. Pour en savoir plus sur Cloud Console, consultez la documentation 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.

Gestion des clés de licence en ligne de commande

Pour gérer les clés de licence sur un appareil, vous pouvez utiliser les commandes de gestion des clés de licence.

Les commandes d'administration des clés de licence ne peuvent être exécutées que si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent. Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, les commandes de gestion des clés de licence échouent avec une erreur. Vous activez l'application dans le cadre de la solution Kaspersky Security for Virtualization Light Agent ; vous n'avez pas besoin d'activer l'application séparément.

Pour ajouter une clé de licence active à l'application, exécutez la commande suivante :

```
kesl-control [-L] --add-active-key <chemin d'accès au fichier clé/code d'activation>
```

où :

- `chemin d'accès au fichier clé` : chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.
- `code d'activation` : code d'activation.

Pour ajouter une clé de licence de réserve à votre application, exécutez la commande suivante :

```
kesl-control [-L] --add-reserve-key <chemin d'accès au fichier clé/code d'activation>
```

Si la clé active n'a pas encore été ajoutée à l'application sur l'appareil, la commande échoue.

À l'aide de la commande d'ajout d'une clé, vous pouvez ajouter à la fois des clés de licence de base de l'application et des clés de licence pour des fonctionnalités supplémentaires. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

Il existe différentes commandes pour supprimer les clés de licence de base et les clés pour des fonctionnalités supplémentaires.

Pour supprimer la clé active de base, exécutez la commande :

```
kesl-control [-L] --remove-active-key
```

Pour supprimer la clé de réserve de base, exécutez la commande :

```
kesl-control [-L] --remove-reserve-key
```

Pour supprimer une clé EDR Optimum active, exécutez la commande suivante :

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Pour supprimer la clé de réserve EDR Optimum, exécutez la commande suivante :

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Pour supprimer une clé active de KUMA, exécutez la commande :

```
kesl-control [-L] --remove-active-key --kuma
```

Pour supprimer la clé de réserve de KUMA, exécutez la commande :

```
kesl-control [-L] --remove-reserve-key --kuma
```

Pour supprimer une clé active de MDR, exécutez la commande :

```
kesl-control [-L] --remove-active-key --mdr
```

Pour supprimer la clé de réserve de MDR, exécutez la commande :

```
kesl-control [-L] --remove-reserve-key --mdr
```

Pour supprimer une clé active EDR Expert (on-premise), exécutez la commande :

```
kesl-control [-L] --remove-active-key --edr-kata
```

Pour supprimer la clé de réserve EDR Expert (on-premise), exécutez la commande :

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Afficher les informations sur les clés de licence utilisées

Vous pouvez afficher des informations sur les clés de licence utilisées par Kaspersky Endpoint Security des manières suivantes :

- Dans Kaspersky Security Center, dans les propriétés de la tâche d'ajout d'une clé.

  Les propriétés de la tâche *Ajouter une clé* affichent des informations sur la clé ajoutée à l'application à la suite de cette tâche.

- Dans Kaspersky Security Center, dans les propriétés de l'application de Kaspersky installée sur l'appareil client.

  Les propriétés de l'application Kaspersky Endpoint Security sur l'appareil protégé affichent des informations sur les clés actives et de réserve ajoutées à l'application sur cet appareil. Vous pouvez afficher les propriétés de l'application à l'aide de Web Console ainsi que de la Console d'administration.

- Dans Kaspersky Security Center, dans le rapport sur l'utilisation de la clé de licence.

  Vous pouvez afficher le rapport d'utilisation des clés à l'aide de Web Console (**Surveillance et rapports** → **Rapports**), ainsi qu'à l'aide de la Console d'administration (onglet **Rapports**). Pour afficher le rapport, vous devez sélectionner le modèle « Rapport d'utilisation de la clé de licence » dans la liste des rapports et commencer à générer le rapport.

- Dans Kaspersky Security Center, dans le stockage des clés de licence de Kaspersky Security Center.

  Vous pouvez ouvrir le stockage des clés à l'aide de Web Console (**Opérations → Licences de Kaspersky**), ainsi qu'à l'aide de la Console d'administration (dossier **Licences de Kaspersky**). Le stockage affiche des informations sur toutes les clés ajoutées au Serveur d'administration de Kaspersky Security Center.

- Sur un appareil sur lequel l'application Kaspersky Endpoint Security est installée. Vous pouvez afficher des informations sur la licence utilisée par Kaspersky Endpoint Security à l'aide de la ligne de commande.

Vous pouvez également recevoir des informations sur les clés de licence utilisées et les licences qui leur sont associées à l'aide des notifications d'événements de Kaspersky Security Center. L'application envoie des informations sur l'expiration de la licence et la violation des restrictions de licence au Serveur d'administration de Kaspersky Security Center.

Si vous utilisez l'application Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent et utilisez Kaspersky Security Center pour gérer l'application, les informations sur l'ajout et la suppression de clés de licence et sur l'expiration de la licence sont enregistrées par défaut dans le journal du système d'exploitation.

Afficher les informations sur les clés d'un appareil via Web Console

Pour afficher des informations sur les clés de licence ajoutées à un appareil dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils) → Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez afficher les informations et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application ouverte, ouvrez l'onglet **Général**, la section **Licences**.

   La section affiche des informations sur les clés de licence ajoutées à l'application et les licences associées à ces clés :

   - **État de la clé de licence** : état de la clé : active ou de réserve.
   - **Nom de l'application** : nom de la licence associée à la clé et les informations sur cette licence.
   - **Clé de licence** : clé de licence, une séquence alphanumérique unique.
   - **Type de licence** : type de licence : essai, commerciale ou abonnement.

- **Date d'activation** : date à laquelle cette clé a été ajoutée.
- **Date d'expiration** : date d'expiration de l'application activée à l'aide de cette clé.

Afficher les informations sur les clés de l'appareil via la Console d'administration

Pour afficher les informations sur les clés de licence ajoutées à l'appareil dans la Console d'administration de Kaspersky Security Center :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.
6. Dans la fenêtre qui s'ouvre, accédez à la section **Clés de licence**.

   La section affiche des informations sur les clés de licence actives et de réserve :

   - **Numéro de série** : succession unique de caractères alphanumériques.
   - **État** :état de la clé de licence, par exemple, actif ou de réserve.
   - **Type** : le type de licence, commerciale ou évaluation.
   - **Période de validité de la licence** : nombre de jours pendant lesquels il est possible d'utiliser l'application qui a été activée à l'aide de l'ajout de cette clé.
   - **Limite** : le nombre d'ordinateurs sur lesquels vous pouvez utiliser la clé.
   - **Date d'activation** (le champ est disponible uniquement pour la clé active) : la date d'ajout de la clé active.
   - **Date d'expiration** (le champ est accessible seulement pour la clé active) : la date d'expiration de la durée d'utilisation de l'application activée via l'ajout d'une clé active.

Afficher les informations sur la licence et la clé dans la ligne de commande

Sur la ligne de commande, à l'aide de la commande `-L --query`, vous pouvez afficher des informations sur les clés de licence actives et de sauvegarde ajoutées à l'application, ainsi que la licence sous laquelle l'application est activée. Si une clé distincte est ajoutée à l'application pour activer les fonctionnalités supplémentaires, les informations sur les clés de licence actives et de sauvegarde ajoutées pour des fonctionnalités supplémentaires sont également affichées.

Pour afficher des informations sur les clés de licence et les licences sur un appareil, exécutez la commande suivante :

```
kesl-control -L --query [--json]
```

où `--json` : afficher les données au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

À la suite de l'exécution de la commande, les informations suivantes seront affichées sur la console :

- Informations sur la clé de licence principale active, si la clé a été ajoutée :
  - La date et l'heure de la durée de validité de la licence sous laquelle l'application est utilisée.
  - Le nombre de jours avant l'expiration de la durée de validité de la licence.
  - Informations sur les limitations des fonctions de protection.
  - Informations sur les limitations de la fonction de mise à jour de la base de données de l'application.
  - Informations sur l'état de la clé de licence.
  - Le type de licence associé à la clé.
  - Limitation de la clé de licence (nombre d'unités de licence).
  - Le nom de l'application que la clé est censée activer.
  - Clé de licence active (séquence alphanumérique unique).
  - Date d'activation.
- Informations sur la clé de licence principale de réserve. Affiché si l'application est utilisée en mode standard et qu'une clé de réserve a été ajoutée. Si l'application est utilisée en mode Light Agent pour la protection des environnements virtuels, les informations relatives à la clé de réserve ne sont pas affichées ; la clé de réserve est ajoutée à la SVM.
  - La date et l'heure de la durée de validité de la licence sous laquelle l'application est utilisée.
  - Informations sur les limitations des fonctions de protection.
  - Informations sur les limitations de la fonction de mise à jour de la base de données de l'application.

- Informations sur l'état de la clé de licence.
- Le type de licence associé à la clé.
- Limitation de la clé de licence (nombre d'unités de licence).
- Le nom de l'application que la clé est censée activer.
- Clé de licence de réserve (séquence alphanumérique unique).
- La date et l'heure d'expiration de la licence associée à la clé active.

- Informations sur la clé active pour des fonctionnalités supplémentaires si une clé distincte est ajoutée :
  - La date et l'heure d'expiration de la durée de validité de la licence pour activer des fonctionnalités supplémentaires.
  - Le nombre de jours avant l'expiration de la durée de validité de la licence.
  - Informations sur les limitations de la fonction de mise à jour de la base de données de l'application.
  - Informations sur l'état de la clé de licence.
  - Le type de licence associé à la clé.
  - Limitation de la clé de licence (nombre d'unités de licence).
  - Le nom de l'application que la clé est censée activer.
  - Clé de licence active (séquence alphanumérique unique).
  - Date d'activation.
- Informations sur la clé pour des fonctionnalités supplémentaires. Affiché lorsque l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent et qu'une clé de réserve a été ajoutée pour des fonctionnalités supplémentaires. Si l'application est utilisée en mode Light Agent pour la protection des environnements virtuels, les informations relatives à la clé de réserve ne sont pas affichées ; la clé de réserve est ajoutée à la SVM.
  - La date et l'heure d'expiration de la durée de validité de la licence pour activer des fonctionnalités supplémentaires.
  - Informations sur les limitations de la fonction de mise à jour de la base de données de l'application.
  - Informations sur l'état de la clé de licence.
  - Le type de licence associé à la clé.
  - Limitation de la clé de licence (nombre d'unités de licence).
  - Le nom de l'application que la clé est censée activer.
  - Clé de licence de réserve (séquence alphanumérique unique).
  - La date et l'heure d'expiration de la licence associée à la clé active.

Vous pouvez également obtenir des informations sur la licence sous laquelle l'application est utilisée en affichant les informations sur l'application à l'aide de la commande `kesl-control --app-info`.

À propos des données

Cette section contient des informations sur les données que Kaspersky Endpoint Security peut enregistrer sur l'appareil et transférer automatiquement à Kaspersky au cours de son fonctionnement.

Kaspersky protège toutes les informations ainsi reçues conformément à la loi et aux règles applicables de Kaspersky Les données sont transmises via des canaux de communication chiffrés.

Pour en savoir plus sur le traitement, le stockage et la destruction des informations obtenues pendant l'utilisation de l'application et transmises à Kaspersky, lisez le Contrat de licence utilisateur final, la Déclaration de Kaspersky Security Network et consultez la Politique de confidentialité sur le site de Kaspersky. Les fichiers license.<identifiant de la langue> et ksn_license.<identifiant de la langue> contiennent le Contrat de licence utilisateur final et la Déclaration de Kaspersky Security Network et font partie du kit de distribution de l'application.

Données fournies lors de l'utilisation d'un code d'activation

Si l'application Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent et a été activée à l'aide du code d'activation, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes afin de vérifier la légitimité de l'utilisation de l'application et de recevoir des informations statistiques concernant la distribution et l'utilisation de l'application :

- type, version et localisation de l'application installée ;
- versions des mises à jour installées de l'application ;
- identifiant de l'appareil et identifiant de l'installation de l'application sur l'appareil ;
- code d'activation avec lequel l'application est activée ;
- identifiant de la licence valide ;
- date et heure de création de la clé de licence de l'application ;
- date et heure sur l'appareil de l'utilisateur ;
- date et heure d'expiration de la licence d'utilisation de l'application ;
- type, version et nombre de bits du système d'exploitation.

Données fournies lors du téléchargement des mises à jour depuis les serveurs de mise à jour de Kaspersky

Si l'application Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent et que vous utilisez les serveurs de mise à jour de Kaspersky pour télécharger les mises à jour, dans le but d'augmenter l'efficacité de la procédure de mise à jour et de recevoir des informations statistiques concernant la distribution et l'utilisation de l'application, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes :

- ID de l'application provenant de la licence ;
- version complète de l'application ;
- ID de licence de l'application ;
- type de licence utilisé ;
- ID de l'installation de l'application (PCID) ;
- ID du démarrage de la mise à jour de l'application ;
- adresse Internet en cours de traitement.

Données transférées lors de l'utilisation de l'application en mode Light Agent

Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels dans le cadre de la solution Kaspersky Security for Virtualization Light Agent, pendant le fonctionnement, l'application enregistre et transmet aux autres modules de la solution les informations suivantes, qui peuvent contenir des informations personnelles et données confidentielles :

- Pour l'activer, l'application Kaspersky Endpoint Security transfère les données suivantes au Serveur de protection : la période de validité de la confirmation de l'état de la clé de licence, l'identifiant (BIOS ID) de la machine virtuelle protégée, les informations sur la licence requise par le Light Agent pour fonctionner.
- Pour mettre à jour les bases de données du Light Agent, l'application Kaspersky Endpoint Security transfère les données suivantes au Serveur de protection : identifiant du logiciel obtenu grâce à la licence ; version complète du logiciel ; identifiant de licence de logiciel ; identifiant d'installation du logiciel (PCID) ; adresse Internet traitée ; type de licence installée ; identifiant de lancement d'une mise à jour.
- Pour assurer la protection et pendant les tâches d'analyse, l'application Kaspersky Endpoint Security transfère au Serveur de protection les informations nécessaires à l'analyse des objets. Cela inclut les noms de fichiers et leurs chemins d'accès dans le système de fichiers, les hachages de fichiers, les adresses Web, ainsi que les objets analysés ou leurs fragments.
- Dans une infrastructure gérée par VMware vCenter Server et VMware NSX Manager, l'application Kaspersky Endpoint Security peut transmettre au Serveur d'intégration des informations sur les tags de sécurité attribuées à une machine virtuelle protégée lorsque des virus, des logiciels malveillants et des activités typiques d'attaques réseau sont détectés. Cela inclut le transfert des identifiants des machines virtuelles protégées.

- Pour obtenir les informations utilisées lors de la sélection d'une SVM pour la connexion, l'application Kaspersky Endpoint Security transmet l'identifiant de la machine virtuelle protégée au Serveur d'intégration et au Serveur de protection.

- Lors de l'utilisation de la solution Kaspersky Security for Virtual Environments Light Agent en mode multi-tenant, les informations nécessaires à la génération des rapports sur la protection des locataires peuvent être transférées de l'application Kaspersky Endpoint Security vers le Serveur de protection. Peuvent être transmis : l'identifiant de la machine virtuelle protégée ; type et version du système d'exploitation invité sur la machine virtuelle protégée ; périodes pendant lesquelles l'application Kaspersky Endpoint Security était connectée à la SVM.

- Pour obtenir des statistiques, l'application Kaspersky Endpoint Security transmet les informations suivantes au Serveur de protection : des informations sur la version du système d'exploitation de la machine virtuelle protégée ; localisation de l'application Kaspersky Endpoint Security ; noms des modules actifs de l'application Kaspersky Endpoint Security ; identifiant (BIOS ID) de la machine virtuelle protégée.

Les informations spécifiées, en plus des informations nécessaires pour effectuer la vérification de l'objet et des informations utilisées lors de la sélection d'un SVM, sont transmises sur des canaux de données cryptés. La connexion entre l'application Kaspersky Endpoint Security et les Serveurs de protection n'est pas sécurisée par défaut. Vous pouvez activer le chiffrement du canal de transmission des données entre les Light Agents et les Serveurs de protection dans les paramètres de l'application Kaspersky Endpoint Security.

Données transmises à l'application Kaspersky Security Center

Pendant son fonctionnement, l'application Kaspersky Endpoint Security enregistre des informations et les transmet à l'application Kaspersky Security Center. Ces informations peuvent contenir des données personnelles et confidentielles :

- Informations relatives aux bases que l'application utilise :
  - liste des catégories de bases indispensables à l'application ;
  - date et heure de la publication et du chargement des bases que l'application utilise ;
  - date d'édition des mises à jour des bases de l'application téléchargées ;
  - date et heure de la dernière publication des bases de l'application ;
  - le nombre d'enregistrements dans les bases de données d'application actuellement utilisées.
- Informations sur la licence d'utilisation de l'application :
  - numéro de série et type de la licence ;
  - durée de validité de la licence en jours ;
  - nombre d'appareils couverts par la licence ;
  - date de début et de fin de validité de la licence ;
  - état de la clé de licence ;

- date et heure de la dernière synchronisation réussie avec les serveurs d'activation, si l'application a été activée à l'aide d'un code d'activation ;
- ID de l'application dont la licence est prévue pour l'activation ;
- fonctionnalités disponibles sous la licence ;
- nom de l'organisation à laquelle la licence a été octroyée ;
- informations complémentaires en cas d'utilisation de l'application selon un abonnement (empreinte de l'abonnement, date de fin d'abonnement et nombre de jours disponibles pour renouveler l'abonnement, adresse Internet du fournisseur de l'abonnement, état actuel et raison du passage à cet état), date et heure d'activation de l'application sur l'appareil ;
- Date et heure de fin de validité de la licence sur l'appareil

- Informations relatives aux mises à jour de l'application :
  - liste des mises à jour à installer ou à supprimer ;
  - date d'édition de la mise à jour et présence de l'état *Critique* ;
  - nom, version et brève description de la mise à jour ;
  - lien vers l'article contenant la description complète de la mise à jour ;
  - ID et texte du Contrat de licence utilisateur final et de la Politique de confidentialité pour la mise à jour de l'application ;
  - ID et texte de la Déclaration de Kaspersky Security Network pour la mise à jour de l'application ;
  - indice de la possibilité de supprimer la mise à jour ;
  - version de la stratégie et du plug-in d'administration de l'application ;
  - adresse Internet pour le téléchargement du plug-in d'administration de l'application ;
  - nom des mises à jour de l'application installées, versions et dates d'installation ;
  - code et description de l'erreur si l'installation ou la suppression de la mise à jour s'est soldée sur une erreur ;
  - indice et raison de la nécessité de redémarrer le appareils ou l'application à cause de la mise à jour de l'application
- Acceptation ou refus des conditions de la Déclaration de Kaspersky Security Network, du Contrat de licence utilisateur final et de la Politique de confidentialité.
- Liste des tags attribués aux appareils.
- Liste des états des appareils et raison de leur attribution.
- État général de l'application et état de tous ses modules ; informations sur la conformité à la stratégie, état de protection en temps réel de l'appareil, état de stabilité de l'application, informations sur l'arrêt de l'application.

- Date et heure de la dernière analyse de l'appareil ; nombre d'objets analysés ; nombre d'objets malveillants détectés ; nombres d'objets bloqués, supprimés ou désinfectés ; nombre d'objets dont la réparation était impossible ; nombre d'erreurs d'analyse ; nombre d'attaques de réseau détectées.
- Données relatives aux valeurs actuelles des paramètres de l'application.
- État actuel et résultats d'exécution des tâches de groupe et des tâches locales, ainsi que paramètres des tâches.
- Informations relatives aux appareils externes connectés à l'appareil client (ID, nom, type, fabricant, description, numéro de série et VID/PID).
- Informations relatives aux copies de sauvegarde placés dans la sauvegarde (nom, chemin d'accès, taille et type de l'objet, description de l'objet, nom de la menace détectée, version des bases de l'application qui ont détecté la menace, date et heure de l'enregistrement de l'objet dans la sauvegarde, action réalisée sur l'objet dans la sauvegarde (suppression, restauration)) ainsi que les fichiers à la demande de l'administrateur.
- Informations relatives au fonctionnement de chaque module de l'application ou à l'exécution de chaque tâche sous la forme d'un événement :
  - date et heure de l'événement ;
  - nom et type de l'événement ;
  - gravité de l'événement ;
  - nom de la tâche ou du module de l'application au cours du fonctionnement duquel s'est produit l'événement ;
  - informations relatives à l'application qui a provoqué l'événement : nom de l'application, chemin d'accès au fichier sur le disque, ID de processus, valeurs des paramètres en cas de publication de l'événement du lancement ou de modification des paramètres de fonctionnement de l'application ;
  - ID de l'utilisateur
  - nom de l'initiateur (planificateur de tâche, application, Kaspersky Security Center ou nom d'utilisateur) dont l'action a provoqué l'événement ;
  - nom et identificateur de l'utilisateur qui a initialisé l'accès au fichier ;
  - résultat du traitement de l'objet ou de l'action (description, type, nom, niveau de danger et précision, nom du fichier et type d'opération sur l'appareil, décision de l'application suite à cette opération) ;
  - informations relatives à l'objet (nom et type d'objet, chemin d'accès à l'objet sur le disque, version de l'objet, taille, informations relatives à l'action exécutée, description de la raison de l'événement, description de la raison du non-traitement et du laisser-passer de l'objet) ;
  - des informations sur l'appareil (nom du fabricant, nom de l'appareil, chemin d'accès, type d'appareil, type de bus, identifiant, VID/PID, attribut de l'appareil système, nom de la planification des règles d'accès à l'appareil) ;
  - informations relatives au blocage et au déblocage de l'appareil ; informations relatives aux connexions bloquées (nom, description, nom de l'appareil, protocole, adresse distante et port, adresse locale et port, règles pour les paquets, actions) ;
  - informations relatives à l'adresse Internet sollicitée ;

- informations relatives aux objets détectés ;
- type de détection, méthode et identifiant ;
- informations relatives à l'action exécutée ;
- informations relatives aux bases de l'application (date d'édition des mises à jour des bases téléchargées, informations relatives à l'application des bases, erreurs d'application des bases, informations relatives à l'annulation des mises à jour des bases installées) ;
- informations relatives à la détection d'un chiffrement malveillant (nom du chiffreur ; nom de l'appareil sur lequel le chiffrement malveillant a été détecté, informations relatives au blocage ou au déblocage de l'appareil) ;
- paramètres de l'application et paramètres de réseau ;
- informations relatives à la règle du Contrôle des applications appliquée (nom et type) et le résultat de son application ;
- informations relatives aux conteneurs et aux images de conteneur (noms des conteneurs ou des images de conteneurs, chemin d'accès aux conteneurs ou aux images de conteneur, adresse Internet du référentiel) ;
- informations relatives aux connexions actives et bloquées (nom, description et type) ;
- informations relatives au blocage et au déblocage de l'accès aux appareils douteux
- des informations sur l'utilisation du KSN (état de connexion au KSN, infrastructure du KSN, identifiant de la déclaration KSN en mode avancé, acceptation de la Déclaration KSN en mode avancé, identifiant de la Déclaration KSN, acceptation de la Déclaration KSN) ;
- informations relatives aux certificats (nom de domaine, nom du sujet, nom de l'émetteur, date d'expiration, état du certificat, type de certificat, heure d'ajout du certificat, date d'émission, numéro de série, empreinte SHA256) ;
- informations sur les systèmes externes faisant partie des solutions logicielles de l'entreprise (adresse du serveur d'intégration) ;
- des informations sur l'activation et la désactivation de l'isolement du réseau pour l'appareil ;
- des informations sur le travail en mode Light Agent : nom du modèle de machine virtuelle, adresse du Serveur d'intégration ;
- le nom de l'appareil pour lequel l'isolation réseau est activée ou désactivée ;
- statistiques d'exécution des tâches d'analyse : nombre d'objets analysés ; nombre de menaces trouvées ; nombre d'objets infectés ; nombre d'objets éventuellement infectés ; nombre d'objets désinfectés ; nombre d'objets ajoutés à la sauvegarde ; nombre d'objets supprimés ; nombre d'objets non réparés ; nombre d'erreurs de vérification ; nombre d'objets protégés par un mot de passe ; nombre d'objets manqués ; nombre de conteneurs et d'images vérifiés ;
- informations sur la version du module EDR Optimum utilisé dans l'application ;
- informations sur les chaînes de développement des menaces : nom de la liste réseau des chaînes de développement des menaces, identifiant de la chaîne de développement des menaces.

- Informations relatives au fonction de la tâche de vérification de l'intégrité du système (nom, type, chemin) et informations relatives à la capture de l'état du système.
- Informations relatives à l'activité réseau, aux règles pour les paquets et aux attaques réseau.
- Informations relatives au rôle de l'utilisateur :
  - nom et identificateur de l'utilisateur qui a lancé la modification du rôle utilisateur ;
  - rôle utilisateur ;
  - nom d'utilisateur auquel le rôle a été attribué ou retiré.
- Informations relatives aux fichiers d'application exécutables détectés sur l'appareil client (nom, chemin, type de fichier et hachage ; liste des catégories auxquelles l'application est affectée ; catégorie KL à laquelle l'application est affectée ; groupe de confiance auquel l'application est affectée ; premier lancement du fichier ; nom et version du demande ; nom du fabricant de l'application ; informations sur le certificat qui a signé la demande : numéro de série, empreinte digitale, émetteur, objet, date d'émission, date d'expiration et clé publique).
- Informations sur la liste réseau des chaînes de développement des menaces : identifiant de la chaîne de développement des menaces, heure de création de la chaîne de développement des menaces sous forme d'horodatage, format de la chaîne de développement des menaces (texte ou archive), taille du corps de la chaîne de développement des menaces en octets.

Données fournies lorsque vous cliquez sur des liens depuis l'interface de l'application

Lorsque vous cliquez sur des liens à partir de l'interface de l'application Kaspersky Endpoint Security, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes :

- version complète de l'application ;
- localisation de l'application ;
- ID de l'application (PID) ;
- nom du lien.

Données fournies lors de l'utilisation de Kaspersky Security Network

L'ensemble des données que Kaspersky Security Network transfère à Kaspersky dépend du mode d'utilisation de Kaspersky Security Network.

Le fichier ksn_license.<ID de la langue> qui contient le texte de la Déclaration de Kaspersky Security Network se trouve dans le kit de distribution de l'application.

Fourniture de données lors de l'utilisation de KSN en mode standard

Si vous utilisez Kaspersky Security Network en mode KSN de base (le commutateur **« Utilisation de Kaspersky Security Network (KSN) »** est activé et la case **« Utiliser le mode étendu de KSN »** est décochée dans la Web Console, l'option **« Mode KSN de base »** est sélectionnée dans la Console d'administration), en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement les informations suivantes à Kaspersky.

Fourniture de données lors de l'utilisation de KSN en mode étendu

Si vous utilisez Kaspersky Security Network en mode étendu de KSN (le commutateur **« Utilisation de Kaspersky Security Network (KSN) »** est activé et la case **« Utiliser le mode étendu de KSN »** est cochée dans la Web Console, l'option **« Mode étendu de KSN »** est sélectionnée dans la Console d'administration), en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement les informations suivantes à Kaspersky en plus des informations indiquées ci-dessus.

Fourniture de données lors de l'utilisation de KSN en mode étendu pendant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)

Si vous utilisez Kaspersky Endpoint Security dans le cadre de Kaspersky Endpoint Detection and Response Expert (on-premise), ainsi que Kaspersky Security Network en mode étendu, en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes, en plus de celles indiquées ci-dessus.

Fourniture de données lors de l'utilisation de Kaspersky Endpoint Security en mode standard et en mode Agent de Endpoint Detection and Response

Si vous utilisez Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent, ainsi que Kaspersky Security Network en mode étendu, en acceptant les conditions de la Déclaration de Kaspersky Security Network, vous acceptez de fournir automatiquement à Kaspersky les informations suivantes, en plus de celles indiquées ci-dessus.

Données fournies lors de l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum

Données transmises avec les résultats d'exécution des tâches *Analyse IOC*

Kaspersky Endpoint Security transfère automatiquement les données sur les résultats d'exécution des tâches *Analyse IOC* vers Kaspersky Security Center.

Les données des résultats d'exécution des tâches *Analyse IOC* peuvent contenir les informations suivantes :

- Informations réseau :
  - Adresse IP du tableau du protocole de résolution d'adresse (Address Resolution Protocol) ;
  - adresse MAC du tableau du protocole de résolution d'adresse ;
  - type et nom de l'enregistrement DNS ;
  - Adresse IP de l'appareil protégé
  - Adresse MAC de l'appareil protégé
  - adresse IP et port de connexion à distance ;
  - adresse IP de la carte réseau locale ;
  - numéro du port ouvert sur l'adaptateur local ;
  - numéro du protocole selon la norme IANA (Internet Assigned Numbers Authority).
- Informations relatives aux processus :
  - Nom du processus
  - Arguments du processus
  - chemin d'accès au fichier exécutable du processus ;
  - identifiant de processus (PID) ;
  - ID du processus parent ;
  - le nom de l'utilisateur qui a démarré le processus ;
  - Date et heure de démarrage du processus
- Informations sur les services :
  - Nom du service
  - Description du service
  - Chemin et nom du fichier exécutable du service
  - identifiant de service ;
  - type de service (pilote du noyau, adaptateur, etc.) ;
  - État du service
  - mode de démarrage du service ;
  - nom de l'utilisateur sous lequel le service est exécuté.

- Informations sur le système de fichiers :
  - Nom du volume
  - Lettre du volume
  - Type de volume
- Informations sur le système d'exploitation :
  - nom et version du système d'exploitation ;
  - Nom du réseau de l'appareil protégé
  - domaine ou groupe auquel appartient l'appareil.
- Informations sur l'activité Web :
  - Nom du navigateur
  - Version du navigateur
  - heure du dernier accès à la ressource Web ;
  - adresse Web de la requête HTTP ;
  - nom de l'utilisateur qui a effectué la requête HTTP ;
  - nom du processus qui a effectué la requête HTTP ;
  - chemin d'accès au fichier exécutable du processus qui a effectué la requête HTTP ;
  - ID du processus qui a effectué la requête HTTP ;
  - adresse Web de la source de la requête HTTP ;
  - adresse Web de la ressource demandée ;
  - agent utilisateur de la requête web traitée (HTTP User-Agent) ;
  - 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 peuvent contenir les informations suivantes :

- Informations générales sur l'alerte :
  - date et heure de l'alerte ;
  - Nom de l'objet
  - Mode d'analyse
  - état de la dernière activité associée à l'alerte ;
  - raison de l'échec du traitement de l'alerte.
- Informations concernant l'objet traité :
  - ID de processus ;
  - ID du processus parent ;
  - identifiant du fichier du processus ;
  - ligne de commande du processus ;
  - le nom de l'utilisateur qui a démarré le processus ;
  - identifiant de la session dans laquelle le processus s'exécute ;
  - type de session dans laquelle le processus s'exécute ;
  - niveau d'intégrité du processus traité ;
  - appartenance de l'utilisateur à des groupes privilégiés ;
  - identifiant de l'objet traité ;
  - Nom complet de l'objet traité
  - identifiant de l'appareil protégé ;
  - nom complet de l'objet (fichier local ou adresse Web) ;
  - hachages MD5 et SHA256 de l'objet traité ;
  - Type d'objet traité
  - date de création et dernière modification de l'objet ;
  - taille de l'objet en cours de traitement ;

- attributs de fichier d'un objet en cours de traitement ;
- informations sur l'organisation qui a signé l'objet ;
- résultat de la vérification du certificat numérique de l'objet ;
- Identifiant de sécurité (SID) de l'objet
- identifiant de fuseau horaire de l'objet ;
- adresse Web de téléchargement de l'objet (fichiers uniquement) ;
- Nom de l'application qui a téléchargé le fichier
- sommes de hachage 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 en dernier lieu ;
- nombre de démarrages de l'objet traité ;
- date et heure du premier lancement de l'objet ;
- identifiant unique du fichier ;
- nom complet du fichier (fichier local ou adresse Web) ;
- Adresse Web de la demande Web traitée
- Source des liens de la requête web traitée (référent HTTP)
- Agent utilisateur de la demande Web traitée
- type de requête 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
- ID du processus dans lequel le code malveillant a été injecté.

Données fournies lors de l'intégration avec le module Kaspersky Endpoint Detection and Response (KATA)

Lorsque Kaspersky Endpoint Security est intégré avec Kaspersky Endpoint Detection and Response (KATA), un module de la solution Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security stocke les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs dotés du module Central Node qui assurent l'interaction avec Kaspersky Endpoint Detection and Response (KATA) (ci-après également *serveurs KATA*) .
- clé publique du certificat du serveur pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA) ;
- Certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
- Identifiants d'authentification sur le serveur proxy.
- paramètres de fréquence de synchronisation avec le serveur KATA et paramètres de transfert de données vers le serveur KATA ;
- État de la connexion avec le serveur KATA et informations sur les erreurs de certificat client et de certificat serveur.
- Paramètres des tâches reçues des serveurs KATA :
  - Paramètres de la programmation du lancement d'une tâche
  - Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
  - Versions des paramètres
  - Type de lancement des services.
  - Noms des services.
  - Ligne de commande de lancement des processus avec les arguments.
  - Hachages MD5 et SHA256 des objets.
  - Chemins d'accès aux objets.
  - Fichiers IOC
- Paramètres d'isolation qui empêcheront l'appareil de communiquer avec d'autres appareils autres que ceux spécifiés dans les exclusions.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA), l'application Kaspersky Endpoint Security enregistre et peut transférer les données suivantes vers le serveur KATA :

- Données des requêtes de synchronisation vers le module EDR Expert (on-premises) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
- Données extraites des requêtes au module EDR Expert (on-premises) dans les rapports sur les résultats de tâche :
  - Adresse IP de l'appareil.
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Adresse MAC de l'appareil.
  - Erreurs d'exécution de tâche et codes de retour
  - États d'achèvement des tâches
  - Temps d'exécution de la tâche
  - Versions des paramètres d'exécution de la tâche.
  - Informations sur les processus lancés ou arrêtés sur l'appareil à la demande du serveur : PID et UniquePID, code d'erreur, hash MD5 et SHA-256 des objets
  - Fichiers demandés par le serveur
  - Données sur les erreurs d'obtention d'informations sur les objets : le nom complet de l'objet lors du traitement duquel une erreur s'est produite ; code d'erreur.
  - État de l'application d'isolement du réseau.

- Pour les indicateurs IOC, les résultats de la recherche sont renvoyés (si chaque indicateur a fonctionné ou non ; objets trouvés et informations sur la branche de l'indicateur qui a fonctionné).
- Pour les objets qui déclenchent des indicateurs IOC, différentes valeurs sont renvoyées selon le type d'indicateurs :
  - ArpEntry : adresse IP de la table ARP (y compris ipv6), adresse physique de la table ARP.
  - Fichier : hachage MD5 du fichier, hachage SHA-256 du fichier, nom complet du fichier (y compris le chemin), taille du fichier.
  - Port : adresse IP distante et port avec lequel une connexion a été établie au moment de la vérification ; Adresse IP et port de l'adaptateur local ; type de protocole (TCP, UDP, IP, RAWIP).
  - Processus : nom du processus ; arguments de processus ; chemin d'accès au fichier de processus ; PID système du processus ; PID système du processus parent ; le nom de l'utilisateur au nom duquel le processus est exécuté ; date et heure de début du processus.
  - SystemInfo : nom du système d'exploitation, version du système d'exploitation, nom réseau d'un appareil sans domaine, domaine ou groupe de travail.
  - User : nom d'utilisateur.
- Pour les objets mis en quarantaine :
  - Chemin du fichier
  - Taille du fichier
  - ID du fichier qui lui est attribué lors de la mise en quarantaine.
  - Indicateur concernant la suppression du fichier d'origine.
- Pour les fichiers reçus depuis la quarantaine :
  - ID du fichier qui lui est attribué lors de la mise en quarantaine.
- Pour les lancements interdits des fichiers exécutables ou des scripts :
  - ID du processus.
  - ID du processus parent ;
  - ID système.
  - ID de session de connexion au système.
  - État du processus
  - Date et heure de l'interception du lancement.

- Pour l'ouverture interdite de documents à l'aide des applications Office :
  - Identifiant du processus
  - ID du fichier.
  - Date et heure de l'interception du lancement.
- Données sur les fichiers :
  - identifiant unique du fichier ;
  - Hachage MD5 de l'objet
  - Contenu du fichier.
- Données dans les paquets de télémétrie :
  - Données sur les fichiers :
    - identifiant unique du fichier ;
    - 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.
    - Hachages MD5 et SHA256 de l'objet
    - Informations sur l'utilisateur et le groupe propriétaire du fichier (nom et identifiant).
  - Données sur les processus en cours :
    - identifiant du fichier du processus ;
    - Identifiant du processus
    - Paramètres de lancement du processus.
    - Identifiant de la session.
    - Date et heure de démarrage du processus
    - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).

- Informations sur le processus accédant à la mémoire d'un autre processus :
  - Identifiant du processus
  - Méthode et adresse d'injection (injection).
  - Ligne de commande de modification des processus avec les arguments.
  - Arguments de l'appel système du processus
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Version des bases de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.
  - Identifiant unique du fichier de menace.
- Données de modification des fichiers :
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur les modifications apportées au système :
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur la connexion de l'utilisateur :
  - Identifiant de la session.
  - Informations sur l'utilisateur (nom et identifiant).
  - Adresse IP de l'appareil à partir duquel la session a été établie.
- Données sur la fin des processus : identifiant unique du processus.
- Informations sur le chargement de la bibliothèque dans l'espace d'adressage du processus : identifiant de la bibliothèque chargée.

- Informations sur l'établissement d'une connexion réseau :
  - Adresse IP locale.
  - Adresse IP à distance.
  - Sens de connexion.
  - Protocole
- Informations sur le processus qui « écoute » les connexions réseau externes sur un port spécifique :
  - Adresse locale (port et adresse IP).
  - Protocole
- Informations sur l'accès au serveur DNS :
  - Le nom de domaine de la ressource demandée.
  - Adresse IP de la ressource demandée.
  - Adresse IP du serveur DNS
  - Type de demande.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises), l'application Kaspersky Endpoint Security enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs qui assurent l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- La clé publique du certificat serveur qui permet l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- Certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises).
- Identifiants d'authentification sur le serveur proxy.
- Paramètres de fréquence de synchronisation avec le serveur assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), et paramètres de transfert des données vers le serveur.

- L'état de la connexion avec le Serveur d'intégration qui assure l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), et des informations sur les erreurs de certificat client et de certificat serveur.
- Paramètres des tâches reçues des serveurs assurant l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) :
  - Paramètres de la programmation du lancement d'une tâche
  - Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
  - Versions des paramètres
  - Type de lancement des services.
  - Noms des services.
  - Ligne de commande de lancement des processus avec les arguments.
  - Hachages MD5 et SHA256 des objets.
  - Chemins d'accès aux objets.
  - Fichiers IOC
- Paramètres d'isolation qui empêcheront l'appareil de communiquer avec d'autres appareils autres que ceux spécifiés dans les exclusions.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises), l'application enregistre et peut transmettre les données suivantes au serveur assurant l'intégration :

- Données des requêtes de synchronisation vers le module EDR Expert (on-premises) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;

- Données extraites des requêtes au module EDR Expert (on-premises) dans les rapports sur les résultats de tâche :
  - Adresse IP de l'appareil.
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Adresse MAC de l'appareil.
  - Erreurs d'exécution de tâche et codes de retour
  - États d'achèvement des tâches
  - Temps d'exécution de la tâche
  - Versions des paramètres d'exécution de la tâche.
  - Informations sur les processus lancés ou arrêtés sur l'appareil à la demande du serveur : PID et UniquePID, code d'erreur, hash MD5 et SHA-256 des objets
  - Fichiers demandés par le serveur
  - Données sur les erreurs d'obtention d'informations sur les objets : le nom complet de l'objet lors du traitement duquel une erreur s'est produite ; code d'erreur.
  - État de l'application d'isolement du réseau.
  - Pour les indicateurs IOC, les résultats de la recherche sont renvoyés (si chaque indicateur a fonctionné ou non ; objets trouvés et informations sur la branche de l'indicateur qui a fonctionné).
  - Pour les règles YARA, les résultats de recherche sont renvoyés (déclenchement ou non de la règle, objets trouvés et informations sur la règle déclenchée).
  - Les objets qui ont déclenché les indicateurs IoC, les règles Yara, renvoient des valeurs différentes selon le type :
    - ArpEntry : adresse IP de la table ARP (y compris ipv6), adresse physique de la table ARP.
    - Fichier : hachage MD5 du fichier, hachage SHA-256 du fichier, nom complet du fichier (y compris le chemin), taille du fichier.
    - Port : adresse IP distante et port avec lequel une connexion a été établie au moment de la vérification ; Adresse IP et port de l'adaptateur local ; type de protocole (TCP, UDP, IP, RAWIP).
    - Processus : nom du processus ; arguments de processus ; chemin d'accès au fichier de processus ; PID système du processus ; PID système du processus parent ; le nom de l'utilisateur au nom duquel le processus est exécuté ; date et heure de début du processus.
    - SystemInfo : nom du système d'exploitation, version du système d'exploitation, nom réseau d'un appareil sans domaine, domaine ou groupe de travail.
    - User : nom d'utilisateur.

- Pour les objets mis en quarantaine :
  - Chemin du fichier
  - Taille du fichier
  - Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.
  - Indicateur concernant la suppression du fichier d'origine.
- Pour les fichiers reçus, restaurés ou supprimés de la quarantaine :
  - Identifiants du fichier qui lui sont attribués lors de la mise en quarantaine.
- Pour les lancements interdits des fichiers exécutables ou des scripts :
  - ID du processus.
  - ID du processus parent ;
  - ID système.
  - ID de session de connexion au système.
  - État du processus
  - Date et heure de l'interception du lancement.
- Pour l'ouverture interdite de documents à l'aide des applications Office :
  - Identifiant du processus
  - ID du fichier.
  - Date et heure de l'interception du lancement.
- Liste des fichiers dans le répertoire spécifié :
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Taille du fichier
  - Type de fichiers
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Métadonnées des fichiers.

- Nombre de liens physiques vers le fichier.
- Dates de création, de modification et de dernier accès aux fichiers.

- Liste des processus en cours d'exécution sur l'appareil :
  - Nom du processus
  - Heure de début du processus.
  - État du processus
  - Identifiant du processus (PID) et identifiant du processus parent.
  - Répertoire de travail actuel.
  - Paramètres de lancement du processus.
  - Variables d'environnement.
  - chemin d'accès au fichier exécutable du processus ;
  - Identifiant de session de l'utilisateur ayant lancé le processus.
  - Identifiant de l'utilisateur et du groupe ayant lancé le processus.
  - Identifiant de l'utilisateur et du groupe avec lesquels le processus a accès aux fichiers et aux ressources du système.
- Liste des points d'auto-démarrage :
  - Type de point d'auto-démarrage.
  - Nom du fichier
  - Chemin d'accès absolu du fichier.
  - Droits d'accès aux fichiers.
  - Indicateurs spéciaux du système de fichiers appliqués à chaque fichier.
  - Nom et identifiant du propriétaire et du groupe propriétaire.
  - Dates de création, de modification et de dernier accès aux fichiers.
- Image mémoire du processus :
  - Nom du processus
  - Chemin d'accès complet au fichier.
  - fichier de vidage du processus.
  - Taille du fichier de vidage du processus.

- Image mémoire de l'appareil : fichier de vidage de la mémoire vive de l'appareil.
- Image disque de l'appareil.

- Données sur les fichiers :
  - identifiant unique du fichier ;
  - Hachage MD5 de l'objet
  - Contenu du fichier.

- Données dans les paquets de télémétrie :
  - Données d'événements de télémétrie :
    - ID de l'événement.
    - Numéro de séquence de l'événement dans la séquence des paquets de télémétrie envoyés.
    - Type d'événement.
    - Heure de l'événement.
  - Les informations sur l'appareil protégé :
    - Nom de l'appareil protégé.
    - Identifiant de l'appareil protégé dans Kaspersky Security Center.
    - Identifiant de l'appareil protégé dans Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Nom, version et famille du système d'exploitation installé sur l'appareil protégé.
    - Heures de démarrage et d'arrêt du système d'exploitation installé sur l'appareil protégé.
  - Données sur les fichiers :
    - identifiant unique du fichier ;
    - 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.
    - Hachages MD5 et SHA256 de l'objet
    - Informations sur l'utilisateur et le groupe propriétaire du fichier (nom et identifiant).

- Données sur les processus en cours :
  - identifiant du fichier du processus ;
  - Identifiant du processus
  - Paramètres de lancement du processus.
  - Identifiant de la session.
  - Date et heure de démarrage du processus
  - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).
- Informations sur le processus accédant à la mémoire d'un autre processus :
  - Identifiant du processus
  - Méthode et adresse d'injection (injection).
  - Ligne de commande de modification des processus avec les arguments.
  - Arguments de l'appel système du processus
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Date de publication et version des bases de données de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.
  - Identifiant unique du fichier de menace.
- Données de modification des fichiers :
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.
- Informations sur les modifications apportées au système :
  - Identifiant unique du processus qui a effectué les modifications.
  - Informations sur le changement survenu.

- Informations sur la connexion de l'utilisateur :
  - Identifiant de la session.
  - Informations sur l'utilisateur (nom et identifiant).
  - Adresse IP de l'appareil à partir duquel la session a été établie.
- Données sur la fin des processus : identifiant unique du processus.
- Informations sur le chargement de la bibliothèque dans l'espace d'adressage du processus : identifiant de la bibliothèque chargée.
- Informations sur l'établissement d'une connexion réseau :
  - Adresse IP locale.
  - Adresse IP à distance.
  - Sens de connexion.
  - Protocole
- Informations sur le processus qui « écoute » les connexions réseau externes sur un port spécifique :
  - Adresse locale (port et adresse IP).
  - Protocole
- Informations sur l'accès au serveur DNS :
  - Le nom de domaine de la ressource demandée.
  - Adresse IP de la ressource demandée.
  - Adresse IP du serveur DNS
  - Type de demande.
- Informations sur les appareils externes connectés :
  - Type d'opération (connexion de l'appareil).
  - Type d'appareil.
  - Identifiant unique de l'appareil.
  - Nom de l'appareil
  - Chemin d'accès à l'appareil.

- Informations sur l'application et ses modules :
  - Version de l'application.
  - Heures d'installation, de démarrage, d'arrêt et de suppression de l'application.
  - Initiateur de l'action de l'application.
  - Motif de l'arrêt de l'application en cas d'arrêt anormal.
  - Codes de retour en cas d'arrêt anormal.
- Informations sur l'interaction avec les planificateurs de tâches (création et suppression des tâches) :
  - Nom de la tâche.
  - Chemin d'accès à la commande exécutée conformément à la planification.
  - Planifier l'exécution de la tâche.
  - Nom du compte utilisateur ayant créé la tâche.
  - Nom du compte sous lequel la tâche est exécutée.
  - Nom du compte utilisateur ayant supprimé la tâche.
- Informations sur la création, la suppression et la modification des services :
  - Nom du service (y compris le précédent s'il a été modifié).
  - Type de service (y compris le précédent s'il a été modifié).
  - Chemin d'accès au fichier exécutable (y compris le précédent s'il a été modifié).
  - Dépendance du service (y compris les précédentes s'il a été modifié).
  - Nom du compte sous lequel le service s'exécute (y compris le précédent s'il a été modifié).
  - Nom d'affichage du service (y compris le nom précédent s'il a été modifié).
  - Nom du compte utilisateur ayant créé, supprimé ou modifié le service.
  - Indicateur de suppression différée.
- Informations de saisie dans la console :
  - Identifiant et type du processus ayant initié la saisie dans la console.
  - Contenu de saisie dans la console.
- Informations sur les appareils montés :
  - Nom de système du volume.
  - Points de montage.

- Informations sur les modifications de la mémoire du processus :
  - Arguments de l'appel système du processus
  - Informations sur le processus ayant effectué l'injection de code et son processus parent.
    - Identifiant du processus et identifiant unique du processus et du processus parent.
    - Ligne de commande à partir de laquelle le processus et le processus parent ont été lancés.
    - Variables d'environnement de processus.
    - Type de compte utilisateur sous lequel le processus et le processus parent ont été lancés.
    - Appel système utilisé pour créer le processus.
    - Identifiant de l'utilisateur et du groupe ayant lancé le processus.
    - Nom et nom complet du processus et du processus parent.
    - Chemin complet du processus et du processus parent.
    - Hachages MD5 et SHA256 du processus et du processus parent.
    - Identifiant de la session.
    - Nom, nom de domaine et identifiant de l'utilisateur ayant lancé le processus et le processus parent.
  - Informations sur le processus par lequel le processus ayant injecté le code a été chargé.
    - Identifiant unique du processus ayant servi à charger le processus.
    - Nom et chemin complet du fichier ayant servi à charger le processus.
    - Chemin complet du processus ayant servi à charger le processus.
    - Hachage MD5 du processus ayant lancé le processus.
  - Informations sur le processus initiateur.
    - Identifiant et identifiant unique du processus initiateur.
    - Ligne de commande du processus initiateur.
    - Nom et nom de domaine de l'utilisateur ayant lancé le processus initiateur.
    - Nom et nom complet du processus initiateur.
    - Chemin d'accès complet au processus initiateur.
    - Hachages MD5 et SHA256 du processus initiateur.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec Kaspersky Network Detection and Response (KATA)

Lorsque Kaspersky Endpoint Security est intégré avec le module Kaspersky Network Detection and Response (KATA), un module de la solution Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security stocke les informations de service suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs NDR.
- Clé publique du certificat du serveur pour l'intégration avec Kaspersky Network Detection and Response (KATA).
- Certificat client pour l'intégration avec Kaspersky Network Detection and Response (KATA).
- Identifiants d'authentification sur le serveur proxy.
- paramètres de fréquence de synchronisation avec le serveur NDR et paramètres de transfert de données vers le serveur NDR ;
- État de la connexion avec le serveur NDR et informations sur les erreurs de certificat client et de certificat serveur.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Network Detection and Response (KATA), l'application Kaspersky Endpoint Security enregistre et transmet les données suivantes au serveur NDR :

- Données des demandes de synchronisation vers le serveur NDR :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom de l'appareil
  - Adresse IP de l'appareil.
  - Adresse MAC de l'appareil.
  - Heure locale sur l'appareil
  - Nom, famille et version du système d'exploitation installé sur l'appareil.
  - Version de Kaspersky Endpoint Security
  - Date d'édition des bases de données utilisées de l'application.
  - état de la clé de licence ;
  - Modèle et fabricant de l'appareil de l'utilisateur.

- Données dans les paquets de télémétrie :
  - Informations sur l'appareil et les utilisateurs :
    - Nom de l'appareil et heure sur l'appareil.
    - Nom, famille et version du système d'exploitation
    - Informations sur les interfaces réseau (description, liste des adresses IP avec masque de sous-réseau, adresse MAC, numéro de métrique, nom de domaine DNS, informations de routage, numéros de port d'écoute).
    - Identifiant interne unique de l'appareil
    - Noms d'utilisateur et identifiants.
    - Noms et identifiants des groupes d'utilisateurs.
  - Informations sur l'application Kaspersky Endpoint Security :
    - nom et version de l'application.
    - La date à laquelle l'application a été mise à jour pour la dernière fois.
    - Informations sur les clés de licence (numéro de série, type, période de validité de la licence, état de la clé)
    - Version des bases de l'application.
    - Liste des versions d'API prises en charge
  - Informations sur les connexions établies :
    - Adresse IP locale, port et adresse MAC
    - Adresse IP à distance, port et adresse MAC.
    - Adresse IP de la passerelle.
    - Type de protocole (par IANA), numéro de protocole et EtherType.
    - Nombre de paquets reçus et transmis.
  - Informations sur les fichiers traités :
    - Le nom et l'identifiant unique du fichier.
    - Type et taille du fichier.
    - Chemin d'accès complet à l'image du fichier.
    - Masque d'attributs du système de fichiers.
    - Heure à laquelle le fichier a été créé et modifié

- hash MD5 et SHA-256 de l'objet.
- Privilèges du fichier, y compris hérités et effectifs.

- Informations sur les processus en cours d'exécution et de fin :
  - UID et PID du processus.
  - Type de processus.
  - Identifiant de la session.
  - La commande à exécuter.
  - Variables d'environnement.
- Informations sur les menaces détectées et traitées :
  - Le nom de la menace détectée et la technologie qui a détecté la menace, selon la classification de Kaspersky.
  - Version des bases de l'application.
  - L'adresse Internet à partir de laquelle l'objet infecté a été téléchargé.
  - État du traitement des menaces
  - La raison de l'impossibilité d'éliminer la menace.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de traçage et les fichiers de vidage.

Données fournies lors de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Unified Monitoring and Analysis Platform, l'application Kaspersky Endpoint Security enregistre les informations suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs KUMA.
- Clé publique du certificat du serveur pour l'intégration avec Kaspersky Unified Monitoring and Analysis Platform (sauf dans le cas où le protocole UDP est utilisé pour se connecter au serveur KUMA).
- Certificat client pour l'intégration avec Kaspersky Unified Monitoring and Analysis Platform.
- Identifiants d'authentification sur le serveur proxy.

- paramètres de fréquence de synchronisation avec le serveur KUMA et paramètres de transfert de données vers le serveur KUMA ;
- État de la connexion avec le serveur KUMA et informations sur les erreurs de certificat client et de certificat serveur.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform, l'application Kaspersky Endpoint Security enregistre et transmet les données suivantes au serveur KUMA dans des paquets de télémétrie :

- Informations sur la modification des fichiers :
  - ID unique du fichier avant modification.
  - Identifiant unique du fichier modifié.
  - Identifiant unique du processus qui a effectué les modifications.
  - Type et indicateur de l'opération sur le fichier.
  - Date et heure de la modification du fichier.
- Informations sur les processus en cours d'exécution et de fin :
  - identifiant du fichier du processus ;
  - UID et PID du processus.
  - Paramètres de lancement du processus.
  - Identifiant de la session.
  - Date et heure de démarrage du processus
  - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).
- Informations sur les événements dans le journal des événements :
  - date et heure de l'événement ;
  - UID du processus associé à l'événement.
  - Type d'événement et description.
  - Résultat d'exécution de l'opération.

Concept d'administration de l'application

Pour gérer l'application Kaspersky Endpoint Security, vous pouvez utiliser :

- Kaspersky Security Center
- ligne de commande ;
- l'interface graphique de l'application a été améliorée.

> Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, l'application ne peut pas être administrée à l'aide de Kaspersky Security Center Cloud Console et de l'interface graphique de l'application.

L'ensemble d'actions que vous pouvez effectuer à l'aide de l'interface graphique de l'application Kaspersky Endpoint Security est limité.

Cette section décrit les fonctionnalités de gestion de l'application via Kaspersky Security Center et la ligne de commande ainsi que les techniques de base pour travailler dans les consoles d'administration de Kaspersky Security Center et dans la ligne de commande.

Administration de l'application via Kaspersky Security Center

Kaspersky Security Center vous permet de gérer à distance et de manière centralisée le fonctionnement de l'application Kaspersky Endpoint Security sur les appareils clients. Vous pouvez installer et désinstaller, démarrer et arrêter à distance l'application Kaspersky Endpoint Security ; configurer les paramètres de fonctionnement de l'application, des modules individuels et des tâches de l'application ; démarrer et arrêter des tâches sur les appareils gérés.

Pour gérer l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez utiliser les Consoles d'administration de Kaspersky Security Center suivantes :

- Console d'administration de Kaspersky Security Center (ci-après également, « Console d'administration »). Il s'agit d'un module logiciel enfichable pour Microsoft Management Console (MMC), qui est installé sur le poste de travail de l'administrateur et fournit une interface utilisateur aux services d'administration du Serveur d'administration et de l'Agent d'administration.

  L'interface de gestion de l'application Kaspersky Endpoint Security via la Console d'administration de Kaspersky Security Center est fournie par le plug-in MMC d'administration pour la Console d'administration basée sur MMC (ci-après également, « plug-in MMC »).

- Kaspersky Security Center Web Console (ci-après également, « Web Console »). Il s'agit d'une interface Web permettant de gérer un système de protection basé sur les applications de Kaspersky. Vous pouvez travailler dans la Kaspersky Security Center Web Console via un navigateur sur n'importe quel appareil ayant accès au Serveur d'administration.

  L'interface de gestion de l'application Kaspersky Endpoint Security via Kaspersky Security Center Web Console est fournie par un plug-in Web d'administration (ci-après également, « plug-in Web »).

- Kaspersky Security Center Cloud Console. Il s'agit d'une Console d'administration cloud faisant partie de la version cloud de l'application Kaspersky Security Center, également appelée Kaspersky Security Center Cloud Console. La console cloud présente une interface similaire à celle de Kaspersky Security Center Web Console. L'interface de gestion de l'application Kaspersky Endpoint Security via Kaspersky Security Center Cloud Console est également assurée par un plug-in Internet.

  La gestion des applications à l'aide de Kaspersky Security Center Cloud Console n'est pas disponible si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Kaspersky Endpoint Security fait partie de la solution Kaspersky Next Pro View. Pour plus d'informations sur les fonctionnalités de l'application disponibles dans cette solution, veuillez consulter l'aide de Kaspersky Next.

Le plug-in MMC et le plug-in Web vous permettent de créer des stratégies et des tâches dans Kaspersky Security Center pour gérer le fonctionnement de l'application Kaspersky Endpoint Security :

- Une *stratégie* est un ensemble de paramètres appliqués à tous les appareils du groupe d'administration. À l'aide de stratégies, vous pouvez définir les mêmes valeurs des paramètres de l'application pour tous les appareils clients faisant partie du groupe d'administration.

  La stratégie de Kaspersky Endpoint Security définit les paramètres généraux de fonctionnement de l'application Kaspersky Endpoint Security et les paramètres de fonctionnement des modules fonctionnels individuels de l'application sur les appareils sur lesquels la stratégie est appliquée.

- Les *tâches* de Kaspersky Endpoint Security créées dans Kaspersky Security Center sont exécutées sur les appareils protégés et mettent en œuvre les fonctions de Kaspersky Endpoint Security telles que l'analyse à la demande, l'activation des applications, la mise à jour des bases de données et des modules de l'application.

  Dans Kaspersky Security Center, vous pouvez créer des tâches à exécuter sur un appareil individuel (tâches locales), ainsi que des tâches pour tous les appareils d'un groupe d'administration (tâches de groupe) ou des tâches pour une sélection aléatoire d'appareils (tâches pour des ensembles d'appareils).

Si l'application est utilisée en mode EDR Agent, seul un sous-ensemble limité des modules et des tâches de l'application est disponible. Vous pouvez gérer certains modules de protection, activer l'application et mettre à jour les bases de données. Pour en savoir plus sur les particularités du mode EDR Agent, consultez l'article Problèmes connus et limitations.

Quelle que soit la Console d'administration de Kaspersky Security Center que vous utilisez pour gérer le fonctionnement de l'application Kaspersky Endpoint Security installée sur les appareils via Kaspersky Security Center, vous devez placer ces appareils dans des groupes d'administration. Vous pouvez créer des groupes d'administration dans Kaspersky Security Center avant de commencer à installer Kaspersky Endpoint Security et configurer des règles visant à déplacer automatiquement les appareils vers les groupes d'administration. Vous pouvez également déplacer manuellement les appareils vers les groupes d'administration après avoir installé l'application Kaspersky Endpoint Security (consultez la documentation de Kaspersky Security Center pour en savoir plus).

À propos des plug-ins d'administration de Kaspersky Endpoint Security

Pour administrer l'application Kaspersky Endpoint Security via Kaspersky Security Center, les plug-ins d'administration suivants sont requis :

- Le plug-in Internet d'administration de Kaspersky Endpoint Security (ci-après, *plug-in Web*) permet à l'application Kaspersky Endpoint Security d'interagir avec l'application Kaspersky Security Center via Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console.

  Le plug-in Internet doit être installé sur un appareil sur lequel l'application Kaspersky Security Center Web Console est installée. La gestion de l'application Kaspersky Endpoint Security à l'aide d'un plug-in Internet est disponible pour tous les administrateurs ayant accès à Kaspersky Security Center Web Console dans un navigateur.

- Le plug-in MMC d'administration de Kaspersky Endpoint Security (ci-après« *plug-in MMC* ») facilite l'interaction entre l'application Kaspersky Endpoint Security et Kaspersky Security Center via la Console d'administration.

  Le plug-in MMC doit être installé sur un appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

Les plug-ins d'administration de Kaspersky Endpoint Security vous permettent de gérer l'application Kaspersky Endpoint Security à l'aide des stratégies et des tâches.

Pour en savoir plus sur les plug-ins d'administration, consultez la documentation de Kaspersky Security Center.

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 Web Console 16.0 ou Kaspersky Security Center Web Console 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. Dans ce cas, accédez à la fenêtre **Paramètres** → **Plug-ins Internet** 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.

À propos des politiques de Kaspersky Security Center

Une *stratégie* est un ensemble de paramètres de l'application Kaspersky Endpoint Security appliqués à tous les appareils clients faisant partie du groupe d'administration.

Plusieurs stratégies avec des valeurs différentes peuvent être configurées pour une seule application. Cependant, il ne peut y avoir qu'une seule stratégie active pour une application à la fois au sein d'un groupe d'administration. Lorsque vous créez une stratégie, toutes les autres stratégies au sein d'un groupe d'administration deviennent inactives. Vous pouvez modifier l'état de la stratégie ultérieurement.

Les stratégies, comme les groupes d'administration, présentent une hiérarchie. Par défaut, une stratégie enfant hérite des paramètres de la stratégie parent. *Stratégie enfant* : il s'agit d'une stratégie de niveau hiérarchique imbriquée, c'est-à-dire une stratégie pour des groupes d'administration imbriqués et des Serveurs d'administration secondaires. Vous pouvez désactiver l'héritage des paramètres de la stratégie parent.

Vous pouvez modifier à distance les paramètres spécifiés par la stratégie pour des appareils distincts dans le groupe d'administration si la modification de ces paramètres n'est pas interdite par la stratégie.

Chaque paramètre de la stratégie présente un « cadenas » , qui indique si la modification des paramètres des stratégies enfants et des paramètres locaux de l'application est interdite. La possibilité de modifier le paramètre de l'application sur un appareil client est défini par l'état du « cadenas » du paramètre dans les propriétés de la stratégie :

- Si le paramètre est verrouillé avec un "cadenas" (), cela signifie que vous ne pouvez pas modifier la valeur du paramètre localement ou dans les stratégies à un niveau imbriqué de la hiérarchie. Pour tous les appareils clients du groupe d'administration et des groupes imbriqués, la valeur du paramètre spécifié par cette stratégie est utilisée.

- Si le paramètre n'est pas verrouillé avec un "cadenas" (), cela signifie que vous pouvez modifier la valeur du paramètre localement ou dans des stratégies à un niveau imbriqué de la hiérarchie. Si pour les appareils clients d'un groupe d'administration, les valeurs des paramètres sont spécifiées localement ou dans des stratégies à un niveau hiérarchique imbriqué, alors la valeur du paramètre spécifiée dans les propriétés de la stratégie n'est pas appliquée.

Dans le plug-in Web et le plug-in MMC, le nombre de paramètres avec « cadenas » est différent. Le plug-in Web contient des « cadenas » qui ne sont pas présents dans le plug-in MMC.

Pour certaines listes, vous pouvez activer la fusion des éléments de liste. Pour fusionner des éléments de la liste, vous devez procéder comme suit :

- Dans les propriétés de la stratégie enfant, sous l'onglet **Général**, activer le paramètre **Hériter des paramètres de la stratégie parent**.

- Dans les propriétés de la stratégie parent, fermer la liste avec un « cadenas » ().

- Dans les propriétés de la stratégie parent, activer la fusion des paramètres en cochant la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents de Kaspersky Security Center sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités.

Vous ne pouvez pas supprimer ou modifier les éléments de liste hérités dans une stratégie enfant. Les éléments de la liste fusionnés par héritage ne peuvent être supprimés ou modifiés que dans la stratégie parent. L'ajout, la modification et la suppression des éléments de la liste sont possibles à des niveaux inférieurs. De cette façon, vous pouvez configurer une liste dans une stratégie parent qui s'appliquera à toutes les stratégies enfants, et vous pouvez également ajouter des éléments à la liste dans la stratégie enfant.

Un *profil de stratégie* peut contenir des paramètres distincts des paramètres de la stratégie de base et qui s'appliquent aux appareils clients lorsque les conditions que vous avez définies sont remplies (règles d'activation). L'utilisation des profils de stratégie permet une configuration plus souple des paramètres de fonctionnement de l'application sur différents appareils. Vous pouvez créer et configurer les profils dans la section **Profils de stratégies** des propriétés d'une stratégie.

Les paramètres du profil verrouillés remplacent les paramètres de la stratégie. Autrement dit, si le paramètre du profil verrouillé est différent du paramètre de la stratégie, l'application appliquera le paramètre du profil. Dans ce cas, les paramètres présentés sous forme de listes sont regroupés et se complètent. Autrement dit, si les paramètres de la liste de profils ne sont pas présents dans la stratégie « de base », ils compléteront la liste de paramètres résultante.

Certaines listes ne sont pas fusionnées. Dans ce cas, les paramètres du profil prévalent sur les paramètres de la stratégie « de base » :

- excluions dans les modules Protection contre les fichiers malicieux et Détection comportementale
- l'exclusion s'applique au fonctionnement des modules Protection contre les fichiers malicieux et Protection contre le chiffrement
- zones de surveillance dans le module Contrôle de l'intégrité du système
- liste des règles (dans la fenêtre **Règles du Contrôle des applications**) dans le module Contrôle des applications
- liste des règles dans le Contrôle Internet
- exclusions de la mémoire de processus de l'analyse des paramètres de l'application
- domaines de confiance dans les paramètres réseau
- certificats racines de confiance dans les paramètres réseau
- ports surveillés dans les paramètres réseau
- liste des adresses SVM dans les paramètres de découverte SVM

Les paramètres de fonctionnement de l'application changent conformément aux paramètres de la stratégie après la première application de la stratégie.

Si l'application n'est pas en cours d'exécution lorsque la stratégie est supprimée, une fois l'application lancée, la stratégie continue d'être appliquée sur l'appareil et l'application continue de fonctionner avec les paramètres spécifiés par la stratégie.

Pour plus d'informations sur les stratégies et les profils de stratégie, ainsi que sur le mécanisme d'héritage des paramètres, consultez l'aide de Kaspersky Security Center.

À propos des tâches de Kaspersky Endpoint Security créées dans Kaspersky Security Center

Vous pouvez créer les types de tâches suivants pour l'application Kaspersky Endpoint Security dans Kaspersky Security Center :

- tâches locales à exécuter sur des appareils individuels
- tâches de groupe à exécuter sur les appareils inclus dans le groupe d'administration

- Tâches pour des ensembles d'appareils à exécuter sur plusieurs appareils, quelle que soit leur appartenance à des groupes d'administration

  Les tâches pour une sélection d'appareils sont exécutées uniquement sur les appareils sélectionnés dans les paramètres de la tâche. En cas d'ajout de nouveaux appareils à un ensemble d'appareils pour lequel une tâche a été créée, cette tâche ne s'applique pas à ceux-ci. Dans ce cas, il faut créer une autre tâche ou modifier les paramètres de la tâche existante.

Vous pouvez créer un nombre illimité de tâches de groupe, de tâches pour des sélections des appareils ou de tâches locales.

Les tâches sont exécutées uniquement si l'application Kaspersky Endpoint Security est en cours d'exécution sur l'appareil.

Des informations générales sur les tâches créées dans Kaspersky Security Center sont fournies dans l'Aide de Kaspersky Security Center.

Pour administrer l'application Kaspersky Endpoint Security, Kaspersky Security Center propose les tâches suivantes :

- *Analyse des logiciels malveillants*. Lors de l'exécution de la tâche, l'application vérifie les zones de l'appareil indiquées dans les paramètres de la tâche pour détecter les virus et les autres applications malveillantes.
- *Analyse des zones critiques*. Lors de l'exécution de la tâche, l'application analyse les secteurs d'amorçage, les objets de démarrage automatique, la mémoire des processus et la mémoire du noyau.
- *Analyse du conteneur*. Lors de l'exécution de cette tâche, l'application analyse les conteneurs et les images à la recherche de virus et d'autres applications malveillantes.
- *Inventaire*. Lors de l'exécution de la tâche, l'application obtient des informations sur tous les fichiers exécutables d'applications conservés sur les appareils.
- *Vérification de l'intégrité du système*. Lors de l'exécution de la tâche, l'application confirme chaque modification d'objet via la comparaison de l'état actuel des objets surveillés à l'état d'origine, défini au préalable comme référence.
- *Ajout d'une clé*. Lors de l'exécution de la tâche, l'application ajoute la clé, y compris la clé de réserve, pour activer l'application.
- *Mise à jour*. Lors de l'exécution de la tâche, l'application met à jour les bases de données en fonction des paramètres de mise à jour configurés.
- *Annulation de la mise à jour des bases*. Lors de l'exécution de la tâche, l'application annule la dernière mise à jour des bases de données.

L'ensemble des paramètres et les valeurs par défaut des paramètres de tâche dépendent du type de licence. Les tâches *Ajouter une clé, Mise à jour* et *Annulation de la mise à jour des bases* ne sont pas applicables si l'application est utilisée en mode Light Agent.

Connexion et déconnexion de Web Console et de Cloud Console

Kaspersky Security Center Web Console

Pour entrer dans Web Console, vous devez connaître l'adresse Internet du Serveur d'administration et le numéro de port. Ces deux éléments sont définis lors de l'installation de Web Console, (le port 8080 est utilisé par défaut). Il faut également activer JavaScript dans le navigateur.

Vous pouvez vous connecter à Kaspersky Security Center Web Console à l'aide de l'une des méthodes suivantes :

- Authentification de domaine (Single Sign-On)
- Nom d'utilisateur et mot de passe d'un utilisateur du domaine
- Nom d'utilisateur et mot de passe d'un utilisateur interne

Pour en savoir plus sur la connexion à Kaspersky Security Center Web Console et la déconnexion de celle-ci, consultez l'Aide de Kaspersky Security Center.

Pour vous connecter à Web Console en indiquant un nom d'utilisateur et un mot de passe :

1. Dans votre navigateur, accédez à :

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   La page de sélection du Serveur d'administration s'ouvre.

2. Si vous avez ajouté plusieurs serveurs d'administration de confiance, sélectionnez dans la liste le Serveur d'administration auquel vous souhaitez vous connecter.

   Si vous n'avez ajouté qu'un seul Serveur d'administration, la liste des Serveurs d'administration ne s'affiche pas.

   Le navigateur est redirigé vers `https://<Administration Server address>:4444`.

3. Saisissez le nom d'utilisateur et le mot de passe de votre compte.

   Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois.

4. Cliquez sur le bouton **Entrer**.

   Si le Serveur d'administration ne répond pas ou si vous avez saisi des identifiants incorrects, un message d'erreur s'affiche.

5. Saisissez le code de sécurité à usage unique généré dans l'application d'authentification sur votre appareil mobile.

   Si vous vous connectez pour la première fois, configurez l'authentification en deux étapes pour votre compte.

Une fois connecté, un tableau de bord s'affiche avec la dernière langue et le dernier thème utilisés.

Pour en savoir plus sur l'interface de Web Console, consultez l'aide de Kaspersky Security Center.

Pour quitter Web Console :

dans le coin inférieur gauche de l'écran, sélectionnez **<Nom du compte 'utilisateur>** → **Quitter**.

Web Console se ferme et la page de connexion s'affiche.

Kaspersky Security Center Cloud Console

Pour Kaspersky Security Center Cloud Console, utilisez un jeton web pour vous connecter à votre compte dans le portail Cloud Console.

Pour en savoir plus sur Kaspersky Security Center Cloud Console, consultez la documentation de Kaspersky Security Center Cloud Console.

Administration des stratégies dans Web Console

Vous pouvez effectuer les actions suivantes avec les stratégies dans Web Console :

- Créer une stratégie.
- Modifier les paramètres d'une stratégie. Vous pouvez configurer les paramètres de la stratégie sous l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la stratégie. Les paramètres de la stratégie dans Web Console sont décrits dans l'Annexe 5.

  Si le compte utilisateur sous lequel vous avez accédé au Serveur d'administration n'est pas autorisé à modifier les paramètres de certaines zones fonctionnelles, les paramètres de ces zones ne peuvent pas être modifiés.

- Exporter et importer les paramètres d'une stratégie.

  L'exportation et l'importation des paramètres de la stratégie de Kaspersky Endpoint Security 12.3 for Linux vers Kaspersky Endpoint Security 12.4 for Linux ne sont pas prises en charge.

- Copier et déplacer une stratégie.
- Supprimer une stratégie.
- Modifier l'état d'une stratégie.
- Créer des profils de stratégie.

Pour obtenir des informations générales sur l'utilisation des stratégies, consultez l'aide de Kaspersky Security Center.

Création d'une stratégie dans Web Console

Pour créer une stratégie dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Stratégies et profils de stratégies**.

   Une liste de stratégies et de profils de stratégie s'ouvre.

2. Sélectionnez le groupe d'administration qui contient les appareils sur lesquels la stratégie doit être appliquée. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des stratégies et profils de stratégie, et sélectionnez le groupe d'administration dans la fenêtre qui s'ouvre.

3. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de la stratégie démarre.

4. Dans la fenêtre qui s'ouvre, sélectionnez le nom de l'application Kaspersky Endpoint Security dans la liste.

   Passez à l'étape suivante de l'Assistant.

5. Précisez dans quel mode vous utilisez l'application Kaspersky Endpoint Security :

   - **Mode standard ou mode Endpoint Detection and Response Agent** : l'application est utilisée pour protéger les appareils fonctionnant sous systèmes d'exploitation Linux en tant qu'application autonome ou en tant qu'application assurant la collaboration des solutions Detection and Response de Kaspersky et des solutions antivirus de fournisseurs tiers.

   - **Mode Light Agent pour la protection des environnements virtuels** : l'application est utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent pour la protection des machines virtuelles exécutant des systèmes d'exploitation invités Linux.

6. Si vous utilisez une application en mode Light Agent pour protéger les environnements virtuels, configurez les paramètres de détection des SVM :

   a. Sélectionnez la méthode utilisée par les Light Agents pour détecter les SVM disponibles pour la connexion :

      - **Utiliser le Serveur d'intégration**

        Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant.

      - **Utiliser une liste d'adresses SVM définie manuellement**

        Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

   Si vous avez sélectionné l'option **Utiliser la liste d'adresses des SVM définie manuellement** et pour Light Agent, un algorithme de sélection des SVM étendu est utilisé et le mode de protection SVM pour les grandes infrastructures est activé (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez spécifier la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

b. Si vous avez sélectionné le Serveur d'intégration, la fenêtre de l'Assistant affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. Si nécessaire, spécifiez de nouveaux paramètres de connexion :

a. Cliquez sur le bouton **Configurer** et spécifiez les nouveaux paramètres de connexion dans la fenêtre qui s'ouvre :

- **Adresse**

  L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.

- **Port**

  Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

> Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

b. Cliquez sur **Analyser**.

c. Le plug-in Web vérifie le certificat SSL reçu du Serveur d'intégration. Si le certificat contient une erreur ou n'est pas approuvé, un message à ce sujet s'affiche dans la fenêtre **Connexion au serveur d'intégration**.

Vous pouvez visualiser les informations sur le certificat reçu du Serveur d'intégration en cliquant sur la ligne **Afficher le certificat reçu**. Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

Pour enregistrer le certificat reçu et continuer la connexion au Serveur d'intégration, dans le groupe **Sélection de l'action**, sélectionnez l'option **Ignorer**.

d. Spécifiez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **Vérifier**.

L'Assistant de création de la stratégie se connecte au Serveur d'intégration. Si la connexion échoue, un message d'erreur apparaît dans la fenêtre. Si la connexion est établie, la fenêtre **Connexion au serveur d'intégration** se ferme et l'état **Installé** s'affiche dans le champ **Connexion au serveur d'intégration** de la fenêtre de l'Assistant de création d'une stratégie.

c. Si vous avez sélectionné une liste d'adresses SVM définie manuellement, la fenêtre affiche une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Pour ajouter une SVM à la liste, cliquez sur le bouton **Ajouter** et précisez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM dans la fenêtre qui s'ouvre. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

> Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application.

Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**.

Passez à l'étape suivante de l'Assistant.

7. Indiquez si vous avez l'intention d'utiliser Kaspersky Security Network. Pour ce faire, lisez attentivement la Déclaration de Kaspersky Security Network, puis effectuez l'une des opérations suivantes :

   - Si vous acceptez l'intégralité des dispositions de la Déclaration et que vous souhaitez consulter le Kaspersky Security Network dans le cadre de l'utilisation de l'application, sélectionnez l'option **Je confirme avoir entièrement lu et compris les conditions de la Déclaration de Kaspersky Security Network, et je l'accepte**.

   - Si vous ne souhaitez pas utiliser Kaspersky Security Network, sélectionnez l'option **Je refuse d'utiliser Kaspersky Security Network** et confirmez votre choix dans la fenêtre qui s'ouvre.

   Le refus d'utiliser Kaspersky Security Network n'entraîne pas l'arrêt de la création de la stratégie. Vous pouvez à tout moment activer ou désactiver l'utilisation de Kaspersky Security Network ou modifier le mode Kaspersky Security Network pour les appareils administrés dans les paramètres de la stratégie.

   Passez à l'étape suivante de l'Assistant.

8. La fenêtre des paramètres de la nouvelle stratégie s'ouvre à l'onglet **Général**. Donnez un nom à la nouvelle stratégie.

   Vous pouvez également configurer les paramètres de stratégie suivants :

   - L'état de la stratégie.

     - **Active**. La stratégie est actuellement appliquée à l'appareil. Si cette option est sélectionnée, lors de la prochaine synchronisation de l'appareil avec le Serveur d'administration, cette stratégie deviendra active sur l'appareil. Cette option est sélectionnée par défaut.

     - **Inactive**. Si cette option est sélectionnée, la stratégie ne s'applique pas à l'appareil mais reste dans le dossier **Stratégies**. Vous pouvez activer une stratégie inactive.

     - **Pour les utilisateurs itinérants**. Si cette option est sélectionnée, la stratégie entre en vigueur lorsque l'appareil quitte le réseau de l'entreprise.

       Dans la stratégie de l'Agent d'administration actuellement active sur l'appareil, dans la section **Réseau → Profils de connexion**, le paramètre **Activer le mode hors-ligne lorsque le Serveur d'administration est indisponible** doit être activé.

   - Héritage des paramètres de la stratégie :

     - **Hériter les paramètres de la stratégie parent**. Si le commutateur est activé, les valeurs des paramètres de la stratégie sont héritées de la stratégie de groupe de niveau supérieur. Les paramètres verrouillées (🔒) dans la stratégie parent, ne sont pas accessibles à la modification. Le commutateur est activé par défaut.

     - **Imposer l'héritage des paramètres aux stratégies enfants**. Si le commutateur est activé, les valeurs des paramètres de la stratégie seront propagés aux stratégies enfants. Dans les propriétés de la stratégie enfant, le commutateur **Hériter les 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 pour lesquels le "cadenas" (🔓) est ouvert. Le bouton bascule est désactivé par défaut.

   Pour obtenir des informations générales sur les paramètres de stratégie, reportez-vous à l'aide de Kaspersky Security Center.

9. Si vous souhaitez configurer d'autres paramètres de stratégie, accédez à l'onglet **Paramètres de l'application** et apportez les modifications nécessaires.

   Vous pouvez aussi modifier les paramètres de la stratégie ultérieurement.

10. Cliquez sur le bouton **Enregistrer**.

    La stratégie créée s'affiche dans la liste des stratégies.

Pour des informations générales sur l'administration des stratégies, consultez l'aide de Kaspersky Security Center.

Modification des paramètres de stratégie dans Web Console

Pour modifier les paramètres de stratégie dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Stratégies et profils de stratégies**.

   La liste des stratégies s'ouvre.

2. Sélectionnez le groupe d'administration contenant les appareils sur lesquels la stratégie est appliquée. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** dans la partie supérieure de la fenêtre et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   La liste affichera les stratégies configurées pour le groupe d'administration sélectionné.

3. Cliquez sur le nom de la stratégie souhaitée dans la liste.

   La fenêtre des propriétés de la stratégie s'ouvre.

4. Modifiez les paramètres de la stratégie sous l'onglet **Paramètres de l'application**.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

   La stratégie est enregistrée avec les paramètres mis à jour.

Paramètres d'une stratégie dans Web Console

L'ensemble des paramètres et des valeurs par défaut pour les paramètres de la stratégie dépendent de la licence sous laquelle l'application est activée. Certains paramètres de stratégie peuvent ou non être appliqués à l'application en fonction du mode dans lequel l'application est utilisée.

Vous pouvez configurer les paramètres de stratégie dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la stratégie.

Les paramètres de la stratégie dans Web Console sont décrits dans l'Annexe 5.

Section	Sous-sections
Protection contre les menaces de l'hôte	**Protection contre les fichiers malicieux**. Dans cette section, vous pouvez gérer la Protection contre les fichiers malicieux. **Protection BadUSB**. Dans cette section, vous pouvez configurer les paramètres de la protection BadUSB. **Analyse des disques amovibles**. Dans cette sous-section, vous pouvez configurer les paramètres d'analyse des disques amovibles lorsqu'ils sont connectés à l'appareil protégé. **Détection comportementale**. Dans cette section, vous pouvez configurer les paramètres de détection comportementale des applications. **Protection contre le chiffrement**. Dans cette section, vous pouvez configurer les paramètres de la protection contre le chiffrement malveillant à distance. **Protection contre les Exploits**. Dans cette section, vous pouvez configurer les paramètres de protection contre les Exploits.
Communication et protection Internet	**Protection contre les menaces par emails**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces par emails. **Protection contre les menaces Internet**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces Internet. **Protection contre les menaces réseau**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces réseau. **Pare-feu**. Dans cette section, vous pouvez configurer les paramètres de gestion du pare-feu.
Contrôles de sécurité	**Contrôle des appareils**. Dans cette section, vous pouvez configurer les paramètres de contrôle des appareils. **Contrôle Internet**. Dans cette section, vous pouvez configurer les paramètres de contrôle Internet. **Contrôle des applications**. Dans cette section, vous pouvez configurer les paramètres de contrôle des applications. **Contrôle de l'intégrité du système**. Dans cette section, vous pouvez configurer les paramètres de contrôle de l'intégrité du système.
Zone de confiance	Dans cette section, vous pouvez configurer les paramètres suivants : • Les exclusions qui s'appliquent au module Protection contre les fichiers malicieux. • Les exclusions qui s'appliquent au module Protection contre les menaces Internet. • Les exclusions qui s'appliquent au module Protection contre les menaces réseau. • Exclusions de l'analyse du trafic réseau. • Exclusion des points de montage de l'interception des opérations sur les fichiers. • Appareils de confiance utilisés dans le fonctionnement du module Contrôle des appareils.

Section	Sous-sections
Paramètres généraux	**Paramètres de détection**. Dans cette sous-section, vous pouvez configurer les paramètres suivants : • Détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données. • Mode d'interception des opérations sur les fichiers. **Kaspersky Security Network**. Dans cette section, vous pouvez configurer l'utilisation de Kaspersky Security Network dans Kaspersky Endpoint Security. **Interaction avec l'utilisateur**. Dans cette sous-section, vous pouvez configurer les paramètres suivants : • Paramètres de démarrage de l'application. • Autorisations permettant aux utilisateurs de gérer les tâches. **Performance**. Dans cette sous-section, vous pouvez configurer les paramètres suivants : • Annulation de l'exécution des tâches planifiées sur un appareil fonctionnant sur batterie. • Exclusion de la mémoire d'un processus de l'analyse • Limite d'utilisation de la mémoire et du processeur pour les tâches d'analyse. • Limite d'utilisation de la mémoire résidente par une application. • Surveillance de la stabilité de l'application. **Paramètres du réseau**. Dans cette sous-section, vous pouvez : • Les paramètres du serveur proxy si les utilisateurs des appareils clients accèdent à Internet via un serveur proxy. • Paramètres d'analyse du trafic réseau. **Analyse du conteneur**. Dans cette sous-section, vous pouvez gérer le fonctionnement du module Surveillance des conteneurs. **Assistance technique**. Dans cette sous-section, vous pouvez configurer les options de traçage et d'enregistrement de vidage. **Reports and Storage**. Dans cette sous-section, vous pouvez configurer les paramètres de la sauvegarde et de la quarantaine. **Intégration KSC**. Dans cette sous-section, vous pouvez configurer les paramètres d'envoi d'informations vers le stockage du Kaspersky Security Center. **Paramètres d'interaction avec le système d'exploitation**. Dans cette sous-section, vous pouvez : • Sélectionnez le mécanisme que l'application doit utiliser pour **intercepter les événements système**. Dans la Web Console, vous pouvez configurer l'interception des événements système dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Paramètres d'interaction du système d'exploitation**). Ces paramètres ne s'appliquent qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify. • Configurez les paramètres de collecte de télémétrie supplémentaires. **Paramètres de notifications d'événements**. Dans cette section, vous pouvez configurer les paramètres de notifications sur les événements.
Configuration des agents intégrés	**Managed Detection and Response**. Dans cette section, vous pouvez activer ou désactiver l'intégration avec Kaspersky Managed Detection and Response et charger le fichier BLOB MDR requis pour l'intégration. **Network Detection and Response (KATA)**. Dans cette section, vous pouvez activer ou désactiver l'intégration avec Kaspersky Network Detection and Response (KATA). **Endpoint Detection and Response**. Cette sous-section vous permet d'activer ou de désactiver l'intégration avec Kaspersky Detection and Response Optimum et de configurer les paramètres d'intégration. **Endpoint Detection and Response Expert (on-premise)**. Cette sous-section vous permet d'activer ou de désactiver l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou Kaspersky Endpoint Detection and Response (KATA) et configurer les paramètres d'intégration. **Sandbox**. Cette section vous permet d'activer ou de désactiver l'intégration avec Sandbox et configurer les paramètres d'intégration. **Intégration KUMA**. Dans cette sous-section, vous pouvez activer et désactiver l'intégration de Kaspersky Unified Monitoring and Analysis Platform et configurer les paramètres d'intégration.

Section	Sous-sections
Mode Light Agent Les paramètres de cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.	**SVM discovery settings**. Dans cette sous-section, vous pouvez sélectionner le mode utilisé par les Light Agents pour détecter les SVM disponibles pour la connexion. **Paramètres de connexion au Serveur d'intégration**. Cette section vous permet de configurer la connexion des Light Agents au Serveur d'intégration, au module Kaspersky Security for Virtualization Light Agent. **SVM connection tag**. Dans cette fenêtre, vous pouvez permettre au Light Agent d'utiliser des tags et attribuer un tag que le Light Agent utilisera pour se connecter. **SVM selection algorithm**. Cette sous-section vous permet de spécifier l'algorithme de sélection de la SVM que les Light Agents doivent utiliser. **Connection protection**. Dans cette sous-section, vous pouvez activer le chiffrement du canal de transmission des données entre le Light Agent et le Serveur de protection.

Gestion des stratégies dans la Console d'administration

Vous pouvez exécuter les actions suivantes avec les stratégies dans la Console d'administration de Kaspersky Security Center :

- Créer une stratégie.
- Modifier les paramètres d'une stratégie. Vous pouvez configurer les paramètres de stratégie dans la fenêtre des propriétés de la stratégie.

  Si le compte utilisateur sous lequel vous avez accédé au Serveur d'administration n'est pas autorisé à modifier les paramètres de certaines zones fonctionnelles, les paramètres de ces zones ne peuvent pas être modifiés.

- Exporter et importer les paramètres d'une stratégie.
- Supprimer une stratégie.
- Modifier l'état d'une stratégie.
- Créer des profils de stratégie.

Pour des informations générales sur l'administration des stratégies, consultez l'aide de Kaspersky Security Center.

Création de la stratégie à l'aide de Console d'administration

Pour créer une stratégie dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant les appareils sur lesquels la stratégie doit être appliquée.

   Dans l'onglet **Appareils** du dossier portant le nom du groupe d'administration, vous pouvez consulter la liste des appareils faisant partie de ce groupe d'administration.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Cliquez sur le bouton **Nouvelle stratégie** pour lancer l'Assistant de création de stratégie.

   Vous pouvez également lancer l'Assistant à l'aide de l'élément **Créer → Stratégie** du menu contextuel de la liste des stratégies.

4. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security dans la liste.

   Passez à l'étape suivante de l'Assistant.

5. Saisissez le nom de la nouvelle stratégie.

6. Si vous souhaitez transférer les paramètres de la stratégie d'une version antérieure de Kaspersky Endpoint Security dans la stratégie en cours de création, cochez la case **Utiliser les paramètres de la stratégie de la version antérieure de l'application**.

   Passez à l'étape suivante de l'Assistant.

7. Indiquez si vous avez l'intention d'utiliser Kaspersky Security Network. Pour ce faire, lisez attentivement la Déclaration de Kaspersky Security Network, puis effectuez l'une des opérations suivantes :

   - Si vous acceptez l'intégralité des dispositions de la Déclaration et que vous souhaitez consulter le Kaspersky Security Network dans le cadre de l'utilisation de l'application, sélectionnez l'option **Je confirme avoir entièrement lu et compris les conditions de la Déclaration de Kaspersky Security Network, et je l'accepte**.

   - Si vous ne souhaitez pas utiliser Kaspersky Security Network, sélectionnez l'option **Je refuse d'utiliser Kaspersky Security Network** et confirmez votre choix dans la fenêtre qui s'ouvre.

   Le refus d'utiliser Kaspersky Security Network n'entraîne pas l'arrêt de la création de la stratégie. Vous pouvez à tout moment activer ou désactiver l'utilisation de Kaspersky Security Network ou modifier le mode Kaspersky Security Network pour les appareils administrés dans les paramètres de la stratégie.

   Passez à l'étape suivante de l'Assistant.

8. Précisez dans quel mode vous utilisez l'application Kaspersky Endpoint Security :

   - **Mode standard ou mode Endpoint Detection and Response Agent** : l'application est utilisée pour protéger les appareils fonctionnant sous systèmes d'exploitation Linux en tant qu'application autonome ou en tant qu'application assurant la collaboration des solutions Detection and Response de Kaspersky et des solutions antivirus de fournisseurs tiers.

   - **Mode Light Agent pour la protection des environnements virtuels** : l'application est utilisée dans le cadre de la solution Kaspersky Security for Virtualization Light Agent pour la protection des machines virtuelles exécutant des systèmes d'exploitation invités Linux.

   Passez à l'étape suivante de l'Assistant.

9. Si vous utilisez une application en mode Light Agent pour protéger les environnements virtuels, configurez les paramètres de détection des SVM :

   a. Sélectionnez la méthode utilisée par les Light Agents pour détecter les SVM disponibles pour la connexion :

      - **Utiliser le Serveur d'intégration**

        Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant.

- **Utiliser une liste d'adresses SVM définie manuellement**

  Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.

Si vous avez sélectionné l'option **Utiliser la liste d'adresses des SVM définie manuellement** et pour Light Agent, un algorithme de sélection des SVM étendu est utilisé et le mode de protection SVM pour les grandes infrastructures est activé (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez spécifier la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

b. Si vous avez sélectionné le Serveur d'intégration, la fenêtre de l'Assistant affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. Si nécessaire, spécifiez de nouveaux paramètres de connexion :

   a. Cliquez sur le bouton **Modifier** et spécifiez les nouveaux paramètres de connexion dans la fenêtre qui s'ouvre :

      - **Adresse**

        L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration.

        Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center fait partie d'un domaine, le champ par défaut indique le nom de domaine de cet appareil.

        Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center ne fait pas partie d'un domaine ou si le Serveur d'intégration est installé sur un autre appareil, le champ doit être rempli manuellement.

        Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.

      - **Port**

        Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

      Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

   b. Cliquez sur le bouton **OK**.

   c. Si l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée ne fait pas partie d'un domaine ou si votre compte n'est pas membre du groupe KLAdmins local ou du domaine ou du groupe des administrateurs locaux, le compte administrateur du Serveur d'intégration est utilisé pour l'authentification sur le Serveur d'intégration.

      Dans la fenêtre qui s'ouvre, saisissez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **OK**.

d. Le plug-in MMC vérifie le certificat SSL reçu du Serveur d'intégration. Si le certificat contient une erreur ou n'est pas fiable, la fenêtre **Vérification du certificat du Serveur d'intégration** s'ouvrira. À l'aide du lien dans la fenêtre, vous pouvez afficher des informations sur le certificat reçu.

> Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

Pour continuer à vous connecter au Serveur d'intégration, cliquez sur le bouton **Ignorer**. Le certificat reçu sera installé en tant que certificat de confiance sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

c. Si vous avez sélectionné une liste d'adresses SVM définie manuellement, la fenêtre affiche une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Pour ajouter une SVM à la liste, cliquez sur le bouton **Ajouter** et précisez l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM dans la fenêtre qui s'ouvre. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne.

> Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application.

Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**.

Passez à l'étape suivante de l'Assistant.

10. Le cas échéant, configurez les paramètres généraux de la Protection contre les fichiers malicieux.

    Passez à l'étape suivante de l'Assistant.

11. Si nécessaire, modifiez les paramètres par défaut de la protection contre les fichiers malveillants.

    Passez à l'étape suivante de l'Assistant.

12. Le cas échéant, configurez les exclusions de la Protection contre les fichiers malicieux.

    Passez à l'étape suivante de l'Assistant.

13. Si nécessaire, modifiez les actions par défaut lorsqu'une menace est détectée.

    Passez à l'étape suivante de l'Assistant.

14. Sélectionnez l'état de la stratégie :

    - **Stratégie active**. La stratégie est actuellement appliquée à l'appareil. Si cette option est sélectionnée, lors de la prochaine synchronisation de l'appareil avec le Serveur d'administration, cette stratégie deviendra active sur l'appareil. Cette option est sélectionnée par défaut.

    - **Stratégie inactive**. Si cette option est sélectionnée, la stratégie ne s'applique pas à l'appareil mais reste dans le dossier **Stratégies**. Vous pouvez activer une stratégie inactive.

- **Stratégie pour les utilisateurs autonomes**. Si cette option est sélectionnée, la stratégie entre en vigueur lorsque l'appareil quitte le réseau de l'entreprise.

  Dans la stratégie de l'Agent d'administration actuellement active sur l'appareil, dans la section **Réseau → Profils de connexion**, le paramètre **Activer le mode hors-ligne lorsque le Serveur d'administration est indisponible** doit être activé.

15. Quittez l'assistant de création de stratégie.

La stratégie créée apparaîtra dans la liste des stratégies du groupe d'administration sous l'onglet **Stratégies** et dans le dossier **Stratégies** de l'arborescence de la console.

Vous pouvez modifier les paramètres de la stratégie ultérieurement. Pour des informations générales sur l'administration des stratégies, consultez l'aide de Kaspersky Security Center.

Modification des paramètres de stratégie dans la Console d'administration de Kaspersky Security Center

Pour modifier les paramètres de stratégie dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.
2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.
4. Modifiez les paramètres de la stratégie.
5. Dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur le bouton **OK** pour enregistrer les modifications.

Paramètres d'une stratégie dans la Console d'administration

L'ensemble des paramètres et des valeurs par défaut pour les paramètres de la stratégie dépendent de la licence sous laquelle l'application est activée. Certains paramètres de stratégie peuvent ou non être appliqués à l'application en fonction du mode dans lequel l'application est utilisée.

Vous pouvez configurer les paramètres de stratégie dans les sections et sous-sections de la fenêtre des propriétés de la stratégie. Pour en savoir plus sur la configuration des paramètres généraux des stratégies et des paramètres des événements, consultez l'aide de Kaspersky Security Center.

Section	Sous-sections
Protection principale	**Protection contre les fichiers malicieux**. Dans cette section, vous pouvez gérer la Protection contre les fichiers malicieux. **Exclusions de la Protection contre les fichiers malicieux**. Dans cette sous-section, vous pouvez configurer les exclusions appliquées au module Protection contre les fichiers malicieux. - **Gestion du pare-feu**. Dans cette section, vous pouvez configurer les paramètres de gestion du pare-feu. **Protection contre les menaces Internet**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces Internet. **Protection contre les menaces par emails**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces par emails. **Protection contre les menaces réseau**. Dans cette section, vous pouvez configurer les paramètres de la protection contre les menaces réseau. **Protection BadUSB**. Dans cette section, vous pouvez configurer les paramètres de la protection BadUSB.
Protection avancée	**Kaspersky Security Network**. Dans cette section, vous pouvez configurer l'utilisation de Kaspersky Security Network dans Kaspersky Endpoint Security. **Protection contre le chiffrement**. Dans cette section, vous pouvez configurer les paramètres de la protection contre le chiffrement malveillant à distance. **Détection comportementale**. Dans cette section, vous pouvez configurer les paramètres de détection comportementale des applications.
Detection and Response	**Managed Detection and Response**. Dans cette section, vous pouvez activer ou désactiver l'intégration avec Kaspersky Managed Detection and Response et charger le fichier BLOB MDR requis pour l'intégration. **EDR Expert (on-premise)**. Cette sous-section vous permet d'activer ou de désactiver l'intégration avec Kaspersky Endpoint Detection and Response (KATA) et de configurer les paramètres d'intégration. **Network Detection and Response (KATA)**. Dans cette section, vous pouvez activer ou désactiver l'intégration avec Kaspersky Network Detection and Response (KATA).
Contrôles de sécurité	**Contrôle des applications**. Dans cette section, vous pouvez configurer les paramètres de contrôle des applications. **Contrôle de l'intégrité du système**. Dans cette section, vous pouvez configurer les paramètres de contrôle de l'intégrité du système. **Contrôle des appareils**. Dans cette section, vous pouvez configurer les paramètres de contrôle des appareils. **Contrôle Internet**. Dans cette section, vous pouvez configurer les paramètres de contrôle Internet.
Tâches locales	**Gestion des tâches**. Dans cette sous-section, vous pouvez configurer les autorisations utilisateur pour la gestion des tâches. **Analyse des disques amovibles**. Dans cette sous-section, vous pouvez configurer les paramètres d'analyse des disques amovibles lorsqu'ils sont connectés à l'appareil protégé.

Section	Sous-sections
Paramètres généraux	**Paramètres du serveur proxy**. Cette sous-section permet de configurer les paramètres du serveur proxy si les utilisateurs des appareils clients accèdent à Internet via un serveur proxy. **Paramètres de l'application**. Dans cette sous-section, vous pouvez configurer les paramètres suivants : • Détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données. • Paramètres de notifications d'événements. • Limite d'utilisation de la mémoire et du processeur pour les tâches d'analyse. • Limite du nombre des tâches d'analyse personnalisées qu'un utilisateur non privilégié peut exécuter simultanément sur l'appareil. • Paramètres de démarrage de l'application. • Paramètres de traçage et d'enregistrement de vidage. • Surveillance de la stabilité de l'application. • Limite d'utilisation de la mémoire résidente par une application. • Mode d'interception des opérations sur les fichiers. **Paramètres d'analyse du conteneur**. Dans cette sous-section, vous pouvez gérer le fonctionnement du module Surveillance des conteneurs. **Paramètres réseau** Dans cette sous-section, vous pouvez configurer les paramètres d'analyse du trafic réseau. **Exclusions globales**. Dans cette sous-section, vous pouvez : • Exclusion des points de montage de l'interception des opérations sur les fichiers. • Exclusions de logiciels industriels : exclusion des processus, fichiers et répertoires associés à un type de logiciel particulier. **Exclure la mémoire des processus**. Cette sous-section permet de configurer l'exclusion de la mémoire de processus de l'analyse. **Paramètres de stockage**. Dans cette sous-section, vous pouvez : • Paramètres de la sauvegarde et de la quarantaine. • Paramètres d'envoi d'informations vers le stockage de Kaspersky Security Center. **Paramètres d'interaction avec le système d'exploitation** Dans cette sous-section, vous pouvez : • Sélectionnez le mécanisme que l'application doit utiliser pour intercepter les événements système. • Configurez les paramètres de collecte de télémétrie supplémentaires.
Intégration avec KUMA	**Intégration avec KUMA**. Dans cette sous-section, vous pouvez activer et désactiver l'intégration de Kaspersky Unified Monitoring and Analysis Platform et configurer les paramètres d'intégration.
Mode Light Agent Les paramètres de cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.	**Connexion au Serveur d'intégration**. Dans cette sous-section, vous pouvez configurer la connexion des Light Agents au Serveur d'intégration, le module Kaspersky Security for Virtualization Light Agent. **Paramètres de détection des SVM**. Dans cette sous-section, vous pouvez sélectionner le mode utilisé par les Light Agents pour détecter les SVM disponibles pour la connexion. **Tag de connexion à la SVM**. Dans cette fenêtre, vous pouvez permettre au Light Agent d'utiliser des tags et attribuer un tag que le Light Agent utilisera pour se connecter. **Algorithme de sélection des SVM**. Dans cette sous-section, vous pouvez spécifier l'algorithme de sélection de la SVM que les Light Agents doivent utiliser. **Protection de la connexion**. Dans cette sous-section, vous pouvez activer le chiffrement du canal de transmission des données entre le Light Agent et le Serveur de protection.

Gestion des tâches dans Web Console

Vous pouvez effectuer les actions suivantes sur les tâches de Kaspersky Endpoint Security dans Web Console :

- Créer les nouvelles tâches.
- Modifier les paramètres des tâches.

  Si le compte utilisateur sous lequel vous avez accédé au Serveur d'administration n'est pas autorisé à modifier les paramètres de certaines zones fonctionnelles, les paramètres de ces zones ne peuvent pas être modifiés.

- Démarrer, arrêter, suspendre ou reprendre l'exécution de la tâche.

  Il est impossible de suspendre et de reprendre la *tâche de mise à jour*. Vous pouvez uniquement l'arrêter ou la démarrer.

- Exporter et importer les tâches.
- Supprimer les tâches.

Dans la liste des tâches, vous pouvez surveiller l'exécution d'une tâche : afficher l'état de la tâche et statistiques d'exécution des tâches sur les appareils. Vous pouvez également créer une sélection d'événements pour surveiller la fin des tâches (**Surveillance et rapports** → **Sélections d'événements**). Pour en savoir plus sur la sélection d'événements, consultez la documentation de Kaspersky Security Center.

Les résultats de l'exécution des tâches sont également enregistrés localement sur l'appareil et dans les rapports de Kaspersky Security Center.

Pour des informations générales sur l'utilisation des tâches, consultez l'aide de Kaspersky Security Center.

Si l'appareil est sous le contrôle de stratégie, l'affichage et la gestion des tâches créées dans Kaspersky Security Center peuvent ne pas être disponibles via la ligne de commande ou via l'interface graphique de l'application.

Création des tâches dans Web Console

Pour créer une tâche pour un groupe ou un ensemble d'appareils dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Dans la première étape de l'Assistant, procédez comme suit :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

   b. Dans la liste déroulante **Type de tâche**, sélectionnez le type de tâche que vous souhaitez créer.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

   d. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez comment vous souhaitez définir la zone d'action de la tâche. La zone d'action d'une tâche correspond aux appareils sur lesquels la tâche sera exécutée :

      - Sélectionnez l'option **Attribuer une tâche à un groupe d'administration** si la tâche doit être effectuée sur tous les appareils membres d'un groupe d'administration spécifique.

      - Sélectionnez l'option **Spécifier les adresses des appareils manuellement ou importer à partir de la liste** si la tâche doit être effectuée sur les appareils spécifiés.

      - Sélectionnez l'option **Attribuer une tâche à une sélection d'appareils** si la tâche doit être exécutée sur des appareils inclus dans la sélection d'appareils en fonction de critères prédéfinis. Pour créer une sélection d'appareils, consultez l'aide de Kaspersky Security Center.

   Passez à l'étape suivante de l'Assistant.

4. Selon la méthode que vous choisissez pour définir la portée d'une tâche, effectuez l'une des opérations suivantes :

   - Dans l'arborescence des groupes d'administration, cochez les cases en regard des groupes d'administration requis.

   - Dans la liste des appareils, cochez les cases en regard des appareils souhaités. Si les appareils dont vous avez besoin ne figurent pas dans la liste, vous pouvez les ajouter des manières suivantes :

      - À l'aide du bouton **Ajouter des appareils**. Vous pouvez ajouter des appareils par nom ou adresse IP, ajouter des appareils à partir d'une plage IP spécifiée ou sélectionner des appareils dans la liste des appareils détectés par le Serveur d'administration lors de l'interrogation du réseau local de l'organisation.

      - À l'aide du bouton **Importer des appareils à partir d'un fichier**. Pour importer, un fichier TXT avec une liste d'adresses d'appareils est utilisé, où chaque adresse doit être située sur une ligne distincte.

   - Dans la liste, sélectionnez le nom de la sélection contenant les appareils souhaités.

   Passez à l'étape suivante de l'Assistant.

5. Pour configurer les paramètres de la tâche immédiatement après sa création, à la dernière étape de l'Assistant, cochez la case **Ouvrir la fenêtre des propriétés de la tâche après sa création**. La tâche est créée avec les paramètres par défaut.

6. Quittez l'Assistant.

La nouvelle tâche apparaît dans la liste des tâches.

Pour créer une tâche locale dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez créer une tâche et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, accédez à l'onglet **Tâches**.

   Une liste des tâches créées pour cet appareil s'ouvrira.

5. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

6. Dans la première étape de l'Assistant, procédez comme suit :

   a. Dans la liste déroulante **Application**, sélectionnez le nom de l'application Kaspersky Endpoint Security.

   b. Dans la liste déroulante **Type de tâche**, sélectionnez le type de tâche que vous souhaitez créer.

   c. Dans le champ **Nom de la tâche**, saisissez le nom de la nouvelle tâche.

7. Pour configurer les paramètres de la tâche immédiatement après sa création, à la dernière étape de l'Assistant, cochez la case **Ouvrir la fenêtre des propriétés de la tâche après sa création**. La tâche est créée avec les paramètres par défaut.

8. Quittez l'Assistant.

La nouvelle tâche apparaît dans la liste des tâches.

Modification des paramètres de tâche dans Web Console

Pour modifier les paramètres d'une tâche dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Exécutez une des actions suivantes :

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur tous les appareils inclus dans un groupe d'administration spécifique, cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et sélectionnez le groupe d'administration dans la fenêtre qui s'ouvre.

     La liste affichera uniquement les tâches configurées pour le groupe d'administration sélectionné.

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur un ou plusieurs appareils (tâches pour un ensemble d'appareils), cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et dans la fenêtre qui s'ouvre, sélectionnez le haut nœud nommé Serveur d'administration.

     La liste affichera toutes les tâches créées sur le Serveur d'administration.

3. Dans la liste des tâches, sélectionnez la tâche souhaitée et ouvrez la fenêtre des propriétés de la tâche à l'aide du lien dans le nom de la tâche.

4. Configurez les paramètres de la tâche :

   - Sous l'onglet **Général**, vous pouvez modifier le nom de la tâche.
   - Sous l'onglet **Paramètres de l'application**, vous pouvez configurer des paramètres de tâche spécifiques. La disponibilité des paramètres configurables dépend du type de tâche.
   - Sous l'onglet **Planification**, vous pouvez configurer la planification de lancement de la tâche et des paramètres supplémentaires pour démarrer et arrêter la tâche.

   Les onglets **Général**, **Résultats**, **Paramètres**, **Planification** et **Historique des révisions** de la fenêtre des propriétés de la tâche sont standard pour Kaspersky Security Center ; pour plus de détails, consultez l'aide de Kaspersky Security Center.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Démarrer, arrêter, suspendre et reprendre des tâches dans Web Console

Pour démarrer, arrêter, suspendre ou reprendre une tâche dans Web Console :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Exécutez une des actions suivantes :

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur tous les appareils inclus dans un groupe d'administration spécifique, cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et sélectionnez le groupe d'administration dans la fenêtre qui s'ouvre.

     La liste affichera uniquement les stratégies créées pour le groupe d'administration sélectionné.

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et dans la fenêtre qui s'ouvre, sélectionnez le haut nœud nommé Serveur d'administration.

     La liste affichera toutes les tâches créées sur le Serveur d'administration.

3. Dans la liste des tâches, cochez la case en regard du nom de la tâche souhaitée et cliquez sur le bouton de l'action souhaitée au-dessus de la liste des tâches.

Gestion des tâches dans la Console d'administration

Vous pouvez effectuer les actions suivantes sur les tâches de Kaspersky Endpoint Security dans la Console d'administration :

- Créer les nouvelles tâches.
- Modifier les paramètres des tâches.

  Si le compte utilisateur sous lequel vous avez accédé au Serveur d'administration n'est pas autorisé à modifier les paramètres de certaines zones fonctionnelles, les paramètres de ces zones ne peuvent pas être modifiés.

- Démarrer, arrêter, suspendre ou reprendre l'exécution de la tâche.

  Il est impossible de suspendre et de reprendre la *tâche de mise à jour*. Vous pouvez uniquement l'arrêter ou la démarrer.

- Exporter et importer les tâches.
- Supprimer les tâches.

Dans la liste des tâches, vous pouvez surveiller l'exécution d'une tâche : afficher l'état de la tâche et statistiques d'exécution des tâches sur les appareils.

Vous pouvez consulter les informations sur la progression et les résultats des tâches dans la liste des événements que Kaspersky Endpoint Security envoie au Serveur d'administration de Kaspersky Security Center (dans l'onglet **Événements** de l'espace de travail du nœud **Serveur d'administration <nom du serveur>**). Vous pouvez également créer une sélection d'événements pour surveiller l'exécution des tâches. Pour en savoir plus sur la sélection d'événements, consultez la documentation de Kaspersky Security Center.

Les résultats de l'exécution des tâches sont également enregistrés localement sur l'appareil et dans les rapports de Kaspersky Security Center.

Pour des informations générales sur l'utilisation des tâches, consultez l'aide de Kaspersky Security Center.

Si l'appareil est sous le contrôle de stratégie, l'affichage et la gestion des tâches créées dans Kaspersky Security Center peuvent ne pas être disponibles via la ligne de commande ou via l'interface graphique de l'application.

Création des tâches dans la Console d'administration

Pour créer une tâche pour un groupe ou un ensemble d'appareils dans la Console d'administration :

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez créer une tâche qui sera exécutée sur les appareils inclus dans le groupe d'administration sélectionné, dans l'arborescence de la console dans le dossier **Appareils administrés**, sélectionnez ce groupe d'administration, puis dans la zone de travail sélectionnez l'onglet **Tâches** et cliquez sur le bouton **Nouvelle tâche**.

     L'Assistant de création d'une tâche pour les appareils du groupe d'administration sélectionné démarre.

   - Si vous souhaitez créer une tâche qui sera exécutée sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console et cliquez sur le bouton **Nouvelle tâche** dans l'espace de travail.

     L'Assistant de création d'une tâche pour un ensemble d'appareils démarre.

2. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security et le type de tâche.

   Passez à l'étape suivante de l'Assistant.

3. Si vous créez une tâche pour un ensemble d'appareils, l'Assistant vous demandera de définir la zone d'action de la tâche. La zone d'action d'une tâche correspond aux appareils sur lesquels la tâche sera exécutée.

   a. Précisez la méthode de détermination de l'étendue de la tâche : sélectionnez les appareils dans la liste des appareils détectés par le Serveur d'administration ; définir les adresses des appareils manuellement ; importer une liste d'appareils à partir d'un fichier ou spécifier une sélection d'appareils préalablement configurée (pour plus de détails, consultez l'aide de Kaspersky Security Center).

   b. En fonction de la méthode que vous avez spécifiée pour définir la portée dans la fenêtre qui s'ouvre, effectuez l'une des opérations suivantes :

      - Dans la liste des appareils détectés, précisez les appareils sur lesquels la tâche sera exécutée. Pour ce faire, cochez la case dans la liste à gauche du nom de l'appareil.

      - Cliquez sur le bouton **Ajouter** ou **Ajouter une plage IP** et spécifiez manuellement les adresses des appareils.

      - Cliquez sur le bouton **Importer** et dans la fenêtre qui s'ouvre, sélectionnez un fichier TXT contenant une liste d'adresses des appareils.

      - Cliquez sur le bouton **Parcourir** et dans la fenêtre qui s'ouvre, précisez le nom de la sélection contenant les appareils sur lesquels la tâche sera exécutée.

   Passez à l'étape suivante de l'Assistant.

4. Configurez les paramètres de tâche disponibles en suivant les instructions de l'Assistant.

5. Saisissez un nom pour la nouvelle tâche et passez à l'étape suivante de l'Assistant.

6. Si vous souhaitez que la tâche s'exécute immédiatement une fois l'Assistant terminé, cochez la case **Exécuter la tâche une fois l'Assistant terminé**.

7. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

Pour créer une tâche locale dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, sélectionnez la section **Tâches**.

   Une liste des tâches créées pour cet appareil s'ouvrira.

5. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.

6. À la première étape de l'Assistant, sélectionnez le nom de l'application Kaspersky Endpoint Security et le type de tâche.

   Passez à l'étape suivante de l'Assistant.

7. Saisissez un nom pour la nouvelle tâche et configurez les paramètres de tâche disponibles en suivant les instructions de l'Assistant.

8. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

Modification des paramètres de tâche dans la Console d'administration

Pour modifier les paramètres des tâches dans la Console d'administration :

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur les appareils faisant partie d'un groupe d'administration spécifique, sélectionnez ce groupe d'administration dans l'arborescence de la console, puis sélectionnez l'onglet **Tâches** dans l'espace de travail.

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur un ou plusieurs appareils (tâches pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console.

2. Dans la liste des tâches, sélectionnez la tâche souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la tâche>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la tâche à l'aide de l'option **Propriétés** du menu contextuel de la tâche.

3. Modifiez les paramètres de la tâche. La disponibilité des paramètres configurables dépend du type de tâche.

   Les onglets **Général**, **Notification**, **Planification** et **Historique des révisions** de la fenêtre des propriétés de la tâche sont standard pour Kaspersky Security Center ; consultez l'aide de Kaspersky Security Center pour plus de détails.

4. Cliquez sur le bouton **Appliquer** ou sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la tâche>** pour enregistrer vos modifications.

Démarrer, arrêter, suspendre et reprendre des tâches dans la Console d'administration

Pour démarrer, arrêter, suspendre ou reprendre une tâche dans la Console d'administration :

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur des appareils faisant partie d'un groupe d'administration spécifique, sélectionnez ce groupe d'administration dans l'arborescence de la console, puis sélectionnez l'onglet **Tâches** dans l'espace de travail.

     Une liste des tâches créées pour le groupe d'administration sélectionné s'ouvrira.

   - Si vous souhaitez démarrer ou arrêter une tâche qui s'exécute sur un ou plusieurs appareils (une tâche pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console.

     Une liste de toutes les tâches créées sur le Serveur d'administration s'ouvrira.

2. Dans la liste des tâches, sélectionnez la tâche souhaitée, ouvrez le menu contextuel de la tâche et sélectionnez l'action que vous souhaitez effectuer.

Administrer l'application via la ligne de commande

À l'aide de la ligne de commande, vous pouvez installer et désinstaller, démarrer et arrêter l'application Kaspersky Endpoint Security sur l'appareil, ainsi que gérer le fonctionnement de l'application localement.

Le fonctionnement des modules fonctionnels de l'application est assuré par les *tâches locales de Kaspersky Endpoint Security* qui s'exécutent dans le système d'exploitation. Vous pouvez activer ou désactiver les modules fonctionnels de l'application sur l'appareil en démarrant et en arrêtant les tâches de Kaspersky Endpoint Security dans la ligne de commande. Des analyses ponctuelles des appareils sont également effectuées en exécutant des tâches de Kaspersky Endpoint Security. Vous pouvez définir les paramètres de fonctionnement des modules fonctionnels sur l'appareil et les paramètres d'analyse de l'appareil en configurant les *paramètres de la tâche* Kaspersky Endpoint Security.

En plus des paramètres des tâches, les paramètres suivants sont disponibles pour configurer l'application :

- Paramètres généraux d'analyse du conteneur.
- Paramètres d'analyse du trafic réseau.
- Paramètres généraux de l'application, qui déterminent le fonctionnement de l'application dans son ensemble et le fonctionnement des fonctions individuelles.

L'application Kaspersky Endpoint Security est gérée à partir de la ligne de commande à l'aide des *commandes de gestion de Kaspersky Endpoint Security*.

Si l'application est utilisée en mode EDR Agent, seul un sous-ensemble limité des modules et des tâches de l'application est disponible. Vous pouvez gérer certains modules de protection, activer l'application et mettre à jour les bases de données. Pour en savoir plus sur les particularités du mode EDR Agent, consultez l'article Problèmes connus et limitations.

Activation de l'achèvement automatique de la commande kesl-control (complétion bash)

Pour le shell bash, il est possible d'activer l'achèvement automatique de la commande kesl-control.

Pour activer l'achèvement automatique de la commande kesl-control dans la session actuelle du shell bash, exécutez la commande suivante :

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

Pour activer l'achèvement automatique pour toutes les nouvelles sessions du shell bash, exécutez la commande suivante :

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Gestion des tâches sur la ligne de commande

Pour gérer l'application Kaspersky Endpoint Security à l'aide de la ligne de commande, les tâches d'application suivantes sont proposées :

- *Protection contre les fichiers malicieux*. Cette tâche vous permet d'activer ou de désactiver la protection contre les menaces de fichiers en temps réel et définit les paramètres du module Protection contre les menaces de fichiers. La tâche démarre automatiquement au démarrage de l'application.
- *Analyse des logiciels malveillants*. Cette tâche vous permet d'analyser les objets du système de fichiers à la recherche de logiciels malveillants à la demande et de définir les paramètres d'analyse. Vous pouvez utiliser cette tâche pour effectuer une analyse complète ou personnalisée des appareils.
- *Analyse des zones critiques*. Cette tâche vous permet d'analyser les zones critiques du système d'exploitation à la demande et de définir les paramètres d'analyse.
- *Analyse personnalisée des fichiers*. Cette tâche est destinée à configurer et à stocker les paramètres utilisés lors de l'analyse des fichiers et répertoires spécifiés à l'aide de la commande `kesl-control --scan-file`. Suite à l'exécution de la commande, l'application crée et exécute une tâche d'analyse de fichiers temporaire.
- *Analyse du conteneur*. Cette tâche vous permet d'analyser des conteneurs et des images à la demande et définit les paramètres d'analyse.

- *Analyse personnalisée du conteneur*. Cette tâche est destinée à configurer et à stocker les paramètres utilisés lors de l'analyse du conteneur et des images spécifiés à l'aide de la commande `kesl-control [-T] --scan-container`. Suite à l'exécution de la commande, l'application crée et exécute une tâche temporaire d'analyse du conteneur.

- *Analyse des disques amovibles*. Cette tâche vous permet de surveiller en temps réel la connexion des disques amovibles à l'appareil et définit les paramètres d'analyse des disques amovibles et de leurs secteurs de démarrage pour détecter la présence de logiciels malveillants.

- *Protection contre les menaces Internet*. Cette tâche vous permet d'activer ou de désactiver la protection contre les menaces Internet et définit les paramètres de fonctionnement du module Protection contre les menaces Internet.

- *Protection contre les menaces réseau*. Cette tâche vous permet d'activer ou de désactiver la protection contre les menaces réseau et définit les paramètres de fonctionnement du module Protection contre les menaces réseau.

- *Protection contre le chiffrement*. Cette tâche vous permet d'activer ou de désactiver la protection des fichiers contre le chiffrement malveillant à distance et définit les paramètres du module Protection contre le chiffrement.

- *Gestion du pare-feu*. Cette tâche vous permet d'activer ou de désactiver la gestion du pare-feu et de définir les paramètres de surveillance des connexions réseau sur l'appareil.

- *Contrôle des applications*. Cette tâche vous permet d'activer ou de désactiver le Contrôle des applications et définit les paramètres du module Contrôle des applications.

- *Inventaire*. Cette tâche vous permet d'obtenir des informations sur tous les fichiers d'application exécutables stockés sur l'appareil.

- *Contrôle des appareils*. Cette tâche vous permet d'activer ou de désactiver le contrôle des appareils et définit les paramètres du module Contrôle des appareils. La tâche démarre automatiquement au lancement de l'application Kaspersky Endpoint Security.

- *Contrôle Internet*. Cette tâche vous permet d'activer ou de désactiver le Contrôle Internet et définit les paramètres du module Contrôle Internet.

- *Détection comportementale*. Cette tâche vous permet de surveiller l'activité des applications malveillantes sur le système d'exploitation. La tâche démarre automatiquement au lancement de l'application Kaspersky Endpoint Security.

- *Contrôle de l'intégrité du système*. Cette tâche vous permet de surveiller en temps réel les actions effectuées avec les objets de la zone de surveillance spécifiée dans les paramètres du module Contrôle de l'intégrité du système.

- *Vérification de l'intégrité du système*. Cette tâche vous permet de vérifier les modifications apportées aux fichiers et répertoires que vous avez inclus dans la zone de surveillance en comparant l'état actuel de l'objet surveillé avec un état précédemment capturé.

- *Licence*. Cette tâche offre la possibilité d'activer une application installée sur l'appareil. La tâche démarre automatiquement au démarrage de l'application et est située en permanence dans la mémoire vive de l'appareil. La tâche n'a pas de paramètres ; les clés de licence sont gérées à l'aide de commandes de gestion spéciales . La tâche ne peut pas être démarrée, arrêtée ou supprimée.

- *Mise à jour*. À l'aide de cette tâche, vous pouvez mettre à jour les bases de données et les modules de l'application selon une planification et à la demande et configurer les paramètres de mise à jour.

- *Annulation de la mise à jour des bases*. À l'aide de cette tâche, vous pouvez restaurer la dernière mise à jour des bases de données et des modules de l'application.

- *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)*. Cette tâche active et désactive l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou Kaspersky Endpoint Detection and Response (KATA) et définit les paramètres d'intégration.

- *Intégration avec Kaspersky Network Detection and Response (KATA)* Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Network Detection and Response (KATA) et de définir les paramètres d'intégration.

- *Intégration avec Sandbox*. Cette tâche vous permet d'activer ou de désactiver l'intégration avec Sandbox et de définir les options d'intégration.

- *Intégration avec KUMA*. Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Unified Monitoring and Analysis Platform et de définir les paramètres d'intégration.

- *Prévention de l'exécution des objets (EDR Expert (on-premise))* Cette tâche vous permet d'activer et de désactiver l'utilisation des règles de prévention de l'exécution de Endpoint Detection and Response Expert (on-premise), ainsi que d'afficher la liste de ces règles.

- *Prévention du lancement des objets (EDR Optimum)*. Cette tâche vous permet d'activer ou de désactiver l'utilisation des règles d'interdiction de lancer des objets du module Endpoint Detection and Response Optimum et d'afficher une liste de ces règles.

Chaque tâche de l'application possède un nom de ligne de commande, un identifiant et un type (voir le tableau ci-dessous).

Les identifiants sont uniques pour toutes les tâches, y compris celles à distance. L'application ne réutilise pas les ID de tâche supprimés. L'ID de la nouvelle tâche est le numéro qui suit l'ID de la dernière tâche créée.

Les noms de tâche ne sont pas sensibles à la casse.

Les *tâches prédéfinies* sont créées lors de l'installation de l'application. Ces tâches ne peuvent pas être supprimées. Chaque tâche prédéfinie a un nom et un identifiant réservés.

Les tâches que vous créez lorsque vous travaillez avec une application sont appelées *tâches utilisateur*. Vous spécifiez les noms de ces tâches lors de la création d'une tâche. L'application définit et attribue des identifiants de tâche utilisateur à une tâche lors de sa création. Les IDs des tâches personnalisées commencent à 100.

Pendant que l'application est en cours d'exécution, elle crée des *tâches d'analyse temporaires*. Les noms et les identifiants des tâches temporaires sont spécifiés par l'application. Les tâches temporaires sont automatiquement supprimées une fois terminées.

Tâches de l'application

Tâche	Nom de la tâche dans la ligne de commande	ID de la tâche	Type de tâche
Protection contre les fichiers malicieux	File_Threat_Protection	1	OAS
Analyse des logiciels malveillants :	Scan_My_Computer	2	ODS
Analyse des logiciels malveillants (personnalisée)	défini par l'utilisateur	à partir de 100	ODS
Analyse personnalisée des fichiers	Scan_File	3	ODS
Analyse des zones critiques.	Critical_Areas_Scan	4	ODS
Mise à jour.	Mise à jour	6	Mise à jour

Tâche	Nom de la tâche dans la ligne de commande	ID de la tâche	Type de tâche
Mise à jour (personnalisée)	défini par l'utilisateur	à partir de 100	Mise à jour
Annulation de la mise à jour.	Annulation de la mise à jour des bases	7	Annulation de la mise à jour des bases
Annulation de la mise à jour des bases (personnalisée)	défini par l'utilisateur	à partir de 100	Annulation de la mise à jour des bases
Licence	Licence	9	Licence
Contrôle de l'intégrité du système	System_Integrity_Monitoring	11	OAFIM
Contrôle de l'intégrité du système (personnalisée)	défini par l'utilisateur	à partir de 100	ODFIM
Gestion du pare-feu	Firewall_Management	12	Pare-feu
Protection contre le chiffrement	Anti_Cryptor	13	AntiCryptor
Protection contre les menaces Internet	Web_Threat_Protection	14	WTP
Contrôle des appareils	Device_Control	15	DeviceControl
Analyse des disques amovibles.	Removable_Drives_Scan	16	RDS
Protection contre les menaces réseau	Network_Threat_Protection	17	NTP
Analyse du conteneur	Container_Scan	18	ContainerScan
Analyse du conteneur (personnalisée)	défini par l'utilisateur	à partir de 100	ContainerScan
Analyse personnalisée du conteneur	Custom_Container_Scan	19	ContainerScan
Détection comportementale	Behavior_Detection	20	BehaviorDetection
Contrôle des applications	Application_Control	21	AppControl
Inventaire	Inventory_Scan	22	InventoryScan
Inventaire (personnalisée)	défini par l'utilisateur	à partir de 100	InventoryScan
Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)	KATAEDR	24	KATAEDR
Contrôle Internet	Web_Control	26	WebControl
Intégration avec Sandbox	Standalone_Sandbox	29	StandaloneSandbox
Prévention de l'exécution des objets (EDR Expert (on-premise)).	KATAEDR_Prevention	30	KATAEDRPrevention
Intégration avec Kaspersky Network Detection and Response (KATA).	KATANDR	31	KATANDR
Prévention du lancement des objets (EDR Optimum)	EDRO_Prevention	32	Prévention
Intégration avec KUMA	KUMA	33	KUMA
Protection contre les menaces par emails	Mail_Monitoring	35	MailMonitoring
Protection BadUSB	Bad_USB	37	BadUSB

Vous pouvez réaliser les opérations suivantes avec les tâches :

- Démarrer et arrêter toutes les tâches prédéfinies et personnalisées, à l'exception de la tâche *License*.
- Suspendre et reprendre les types de tâches *ODS*, *ODFIM* et *InventoryScan*.

- Créer et supprimer des tâches personnalisées. Selon le mode d'utilisation de l'application, vous pouvez créer des tâches de types suivants :
  - mode standard : *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* et *InventoryScan* ;
  - mode Light Agent pour la protection des environnements virtuels : *ODS*, *ODFIM*, *ContainerScan* et *InventoryScan*.
- Modifier les paramètres de toutes les tâches utilisateur et de toutes les tâches prédéfinies, à l'exclusion des tâches de type *Rollback* et *License*.

  Si l'application est utilisée en mode Light Agent pour protéger des environnements virtuels, les paramètres de la tâche prédéfinie *Update* ne peuvent pas être modifiés non plus.

- Configurer le calendrier de lancement des tâches.

Afficher une liste de tâches dans la ligne de commande

Pour consulter la liste des tâches de l'application, exécutez la commande suivante :

```
kesl-control --get-task-list [--json]
```

où :

`--json` – format de sortie de la liste des tâches de l'application. Si vous ne désignez pas de format de fichier, l'exportation se fera au format INI.

Affiche la liste des tâches existantes de l'application Kaspersky Endpoint Security.

Les informations suivantes sont affichées pour chaque tâche :

- `Name` : nom de la tâche.
- `ID` : identifiant de la tâche.
- `Type` : type de tâche.
- `State` : état actuel de la tâche.

Si la stratégie de Kaspersky Security Center interdit aux utilisateurs d'afficher et de modifier les tâches locales, les informations sur les tâches Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (en mode standard) et Rollback (en mode standard) ne sont pas disponibles.

Consultation de l'état de la tâche sur la ligne de commande

Pour consulter l'état d'une tâche, exécutez la commande suivante :

```
kesl-control --get-task-state <ID/nom de la tâche> [--json]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--json` : afficher les paramètres au format JSON.

Les principaux états suivants sont fournis pour les tâches de l'application :

- `Started` : en cours d'exécution.
- `Starting` : en cours de démarrage.
- `Stopped` : tâche arrêtée.
- `Stopping` : en cours d'arrêt.

Les tâches *ODS*, *ODFIM* et *InventoryScan* peuvent également présenter l'un des états suivants :

- `Pausing` : en cours de suspension ;
- `Suspended` : suspendue ;
- `Resuming` : en cours de reprise.

Création d'une tâche dans la ligne de commande

Si l'application est utilisée en mode standard, vous pouvez créer les tâches de types suivants : *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Si l'application est utilisée en mode Light Agent pour protéger les environnements virtuels, vous pouvez créer des tâches de types suivants : *ODS*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Vous pouvez créer des tâches avec les paramètres par défaut ou avec les paramètres définis dans le fichier de configuration.

Pour créer une tâche avec les paramètres par défaut, exécutez la commande suivante :

```
kesl-control --create-task <nom de la tâche> --type <type de tâche>
```

où :

- `< nom de la tâche >` est le nom que vous attribuez à la nouvelle tâche.
- `< type de tâche >` est la désignation du type de tâche que vous créez.

Pour créer une tâche selon les paramètres repris dans un fichier de configuration, exécutez la commande suivante :

```
kesl-control --create-task < nom de la tâche > --type < type de tâche > --file < chemin d'accès au fichier de configuration > [--json]
```

où :

- `< nom de la tâche >` est le nom que vous attribuez à la nouvelle tâche.
- `< type de tâche >` est l'identifiant du type de tâche que vous créez.
- `< chemin d'accès au fichier >` est le chemin d'accès complet au fichier de configuration contenant les paramètres qui seront utilisés pour créer la tâche.
- `--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Démarrer, arrêter, mettre en pause et reprendre une tâche à partir de la ligne de commande

Vous pouvez démarrer et arrêter des tâches prédéfinies et personnalisées, à l'exception de la tâche License.

Vous pouvez suspendre et reprendre les tâches ODS, ODFIM et InventoryScan.

Démarrer une tâche

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `[-W]` : activer la sortie des événements actuels liés à cette tâche.
- `[--progress]` : activer l'affichage de la progression de la tâche.

Exemple d'exécution d'une tâche avec l'identifiant 1 et d'activation de l'affichage des événements en cours associés à la tâche

```
kesl-control --start-task 1 -W
```

Si une erreur se produit lors du démarrage d'une tâche et que la tâche ne démarre pas, une fois l'application redémarrée, une nouvelle tentative de démarrage de la tâche est effectuée.

Arrêter une tâche

```
kesl-control --stop-task <task ID|name> [-W]
```

où :

- `<task ID|name>` correspond à l'identifiant attribué à la tâche au moment de sa création ou au nom de la tâche sur la ligne de commande.
- `[-W]` : activer la sortie des événements actuels liés à cette tâche.

Suspendre une tâche

```
kesl-control --suspend-task <task ID|name>
```

Reprendre une tâche

```
kesl-control --resume-task <task ID|name>
```

Suppression de la tâche dans la ligne de commande

Vous pouvez uniquement supprimer les tâches utilisateur. Les tâches prédéfinies ne peuvent pas être supprimées.

Pour supprimer une tâche, exécutez la commande suivante :

```
kesl-control --delete-task <ID/nom de la tâche>
```

où `<ID/nom de la tâche>` est l'ID attribué à la tâche au moment de sa création, ou le nom de la tâche dans la ligne de commande.

Affichage des paramètres de la tâche dans la ligne de commande

Vous pouvez afficher les valeurs actuelles des paramètres de toutes les tâches utilisateur et de toutes les tâches prédéfinies, à l'exclusion des tâches *Rollback* et *License* (ces tâches n'ont pas de paramètres).

Vous pouvez afficher les valeurs actuelles des paramètres de la tâche sur la console ou dans un fichier de configuration, que vous pouvez utiliser pour modifier les paramètres de la tâche.

Pour afficher les valeurs actuelles des paramètres de la tâche sur la console, exécutez la commande suivante :

```
kesl-control --get-settings <ID/nom de la tâche> [--json]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les valeurs actuelles des paramètres de la tâche dans le fichier de configuration, exécutez la commande suivante :

```
kesl-control --get-settings <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres de la tâche seront écrits. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Modification des paramètres de la tâche dans la ligne de commande

Vous pouvez modifier les paramètres de toutes les tâches personnalisées et de toutes les tâches prédéfinies, à l'exclusion des tâches *Rollback* et *License*.

Si l'application est utilisée en mode Light Agent pour protéger des environnements virtuels, les paramètres de la tâche prédéfinie *Update* ne peuvent pas être modifiés non plus.

Sur la ligne de commande, vous pouvez modifier les paramètres des tâches à l'aide de la commande `kesl-control --set-settings` :

- Vous pouvez modifier tous les paramètres de la tâche à l'aide du fichier de configuration, qui contient les paramètres de la tâche. Vous pouvez obtenir le fichier de configuration à l'aide de la commande d'affichage des paramètres de la tâche.
- Vous pouvez modifier les paramètres individuels de la tâche à l'aide d'options de ligne de commande au format `< nom du paramètre >=< valeur du paramètre >`. Vous pouvez obtenir les valeurs actuelles des paramètres de la tâche à l'aide de la commande d'affichage des paramètres de la tâche.
- Vous pouvez restaurer les paramètres de la tâche par défaut.

Vous pouvez ajouter et supprimer des zones d'analyse et des zones d'exclusion à l'aide d'un fichier de configuration contenant des paramètres de tâche ou des clés de la ligne de commande. La configuration des zones d'analyse et des zones d'exclusion est disponible pour les tâches de type *OAS*, *ODS*, *OAFIM*, *ODFIM* et *AntiCryptor*.

Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez définir `/.snapshots/*/snapshot/` en tant que chemin d'exclusion.

Certaines tâches disposent également de commandes de contrôle distinctes qui vous permettent de modifier les paramètres de la tâche.

Modification des paramètres de la tâche via le fichier de configuration

Pour modifier les valeurs des paramètres de tâche à l'aide d'un fichier de configuration :

1. Affichez les paramètres de la tâche dans le fichier de configuration à l'aide de la commande `kesl-control --get-settings`.
2. Ouvrez le fichier de configuration et modifiez les valeurs des paramètres nécessaires.

   Pour les tâches de type *OAS*, *ODS*, *OAFIM*, *ODFIM* et *AntiCryptor*, vous pouvez ajouter ou supprimer des zones d'analyse et des zones d'exclusion.

   Si vous souhaitez ajouter une zone d'analyse, ajoutez la section `[ScanScope.item_#]` au fichier avec les paramètres suivants :

   - `AreaDesc` : description de la zone d'analyse, qui contient des informations supplémentaires sur cette zone.
   - `UseScanArea` : activer l'analyse de la zone spécifiée.
   - `Path` est le chemin d'accès au répertoire contenant les objets à analyser. Vous pouvez spécifier le chemin d'accès à un répertoire local ou activer l'analyse des répertoires distants montés sur l'appareil client.
   - `AreaMask.item_#` : restriction de la zone d'analyse. Vous pouvez spécifier un masque pour les noms des fichiers à analyser. Par défaut, l'analyse est activée pour tous les objets dans la zone d'analyse. Vous pouvez spécifier plusieurs éléments `AreaMask.item_#`.

Si vous souhaitez ajouter une zone d'exclusion, ajoutez une section `[ExcludedFromScanScope.item_#]` au fichier avec les paramètres suivants :

- `AreaDesc` : spécifie la description de la zone d'exclusion, qui contient des informations supplémentaires sur la zone d'exclusion.
- `UseScanArea` : activer l'exclusion de la zone spécifiée.
- `Path` est le chemin d'accès au répertoire contenant les objets à exclure. Vous pouvez spécifier le chemin d'accès à un répertoire local ou exclure les répertoires distants montés sur l'appareil client. Les valeurs de paramètres possibles dépendent du type de tâche.
- `AreaMask.item_#` : limitation de la zone d'exclusion. Vous pouvez spécifier un masque pour les noms des fichiers que vous souhaitez exclure de la portée de l'analyse. Par défaut, tous les objets de portée sont exclus.

  Exemple :

  ```
  [ExcludedFromScanScope.item_0000]
  AreaDesc=
  UseScanArea=Yes
  Path=/tmp/notchecked
  AreaMask.item_0000=*
  ```

Vous pouvez spécifier plusieurs sections `[ScanScope.item_#]` et `[ExcludedFromScanScope.item_#]`. L'application traite les zones par ordre croissant d'index d'élément.

3. Conservez le fichier de configuration.
4. Exécutez la commande :

   `kesl-control --set-settings <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]`

   où :

   - `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
   - `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration depuis lequel les paramètres de la tâche seront importés.
   - `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres de tâche spécifiées dans le fichier seront importées dans l'application.

Si vous modifiez la liste d'autorisation de la tâche Contrôle des applications ou si vous interdisez le lancement de toutes les applications et/ou des applications ayant un impact sur le fonctionnement de Kaspersky Endpoint Security, il faut exécuter la commande `--set-settings` avec la clé `--accept`.

Modification des paramètres de la tâche à l'aide des clés de la ligne de commande

À l'aide des options de la commande `kesl-control --set-settings`, vous pouvez modifier les valeurs individuelles des paramètres des tâches, ainsi qu'ajouter ou supprimer des zones d'analyse et des zones d'exclusion pour des tâches de type *OAS*, *ODS*, *OAFIM*, *ODFIM* et *AntiCryptor*.

Configuration des paramètres individuels des tâches

Pour modifier les valeurs individuels des paramètres de la tâche à l'aide des commutateurs de ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings <ID/nom de la tâche> <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur de l'un des paramètres de la tâche. Vous pouvez obtenir les valeurs actuelles des paramètres de la tâche à l'aide de la commande d'affichage des paramètres de la tâche.

Les valeurs des paramètres spécifiés de la tâche seront modifiées.

Si vous modifiez la liste d'autorisation de la tâche Contrôle des applications ou si vous interdisez le lancement de toutes les applications et/ou des applications ayant un impact sur le fonctionnement de Kaspersky Endpoint Security, il faut exécuter la commande `--set-settings` avec la clé `--accept`.

Ajouter ou supprimer une zone d'analyse

Pour ajouter une zone d'analyse à l'aide de clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings <ID/nom de la tâche> --add-path <chemin d'accès>
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--add-path <chemin d'accès>` ajoute un chemin d'accès à un répertoire contenant les objets à analyser.

Une nouvelle section `[ScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application analyse les objets situés dans le répertoire défini par le paramètre `Path`. Les autres paramètres de la zone d'analyse prennent leurs valeurs par défaut.

Si les paramètres de la tâche ont déjà une section `[ScanScope.item_#]` avec la valeur spécifiée du paramètre `Path`, la section en double n'est pas ajoutée.

Si le paramètre `UseScanArea` a reçu la valeur `No`, il prend la valeur `Yes` après l'exécution de la commande et les objets situés dans ce répertoire sont analysés.

Exemple :
Ajout d'une zone d'analyse pour une tâche avec ID=100 :

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

Les paramètres suivants de la zone d'analyse seront ajoutés à la tâche :

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

Pour supprimer une zone d'analyse à l'aide de clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings <ID/nom de la tâche> --del-path <chemin d'accès>
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--del-path <chemin d'accès>` supprime un chemin d'accès à un répertoire contenant les objets à analyser.

Une section `[ScanScope.item_#]` qui contient le chemin indiqué sera supprimée depuis les paramètres de la tâche. L'application n'analysera pas les objets dans le répertoire spécifié.

Ajout ou suppression d'une zone d'exclusion

Pour ajouter une zone d'exclusion à l'aide de clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings <ID/nom de la tâche> --add-exclusion <chemin d'accès>
```

où :

- `< ID/nom de la tâche >` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--add-exclusion < chemin d'accès >` ajoute un chemin d'accès à un répertoire contenant les objets que vous souhaitez exclure de l'analyse.

  Une nouvelle section `[ExcludedFromScanScope.item_#]` sera ajoutée dans les paramètres de la tâche. L'application exclura des analyses les objets du répertoire spécifié par le paramètre `Path`. Les autres paramètres de la zone d'exclusion prennent leurs valeurs par défaut.

  Si les paramètres de la tâche ont déjà une section `[ExcludedFromScanScope.item_#]` avec la valeur spécifiée du paramètre `Path`, la section en double n'est pas ajoutée.

  Si le paramètre `UseScanArea` a reçu la valeur `No`, il prend la valeur `Yes` après l'exécution de la commande et les objets situés dans ce répertoire sont exclus de l'analyse.

Pour supprimer une zone d'exclusion à l'aide de clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-settings < ID/nom de la tâche > --del-exclusion < chemin d'accès >
```

où :

- `< ID/nom de la tâche >` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--del-exclusion < chemin d'accès >` supprime un chemin d'accès à un répertoire contenant les objets à exclure de l'analyse.

  Une section `[ExcludedFromScanScope.item_#]` qui contient le chemin indiqué sera supprimée depuis les paramètres de la tâche. L'application n'exclura pas les objets du répertoire spécifié de l'analyse.

Restauration des paramètres de tâche par défaut dans la ligne de commande

Vous pouvez restaurer les paramètres par défaut pour toutes les tâches personnalisées et toutes les tâches prédéfinies, à l'exclusion des tâches de types *Rollback* et *License* (ces tâches n'ont aucun paramètre).

Pour restaurer les paramètres de tâche par défaut, exécutez la commande suivante :

```
kesl-control --set-settings < ID/nom de la tâche > --set-to-default
```

où `< ID/nom de la tâche >` est l'ID attribué à la tâche au moment de sa création, ou le nom de la tâche dans la ligne de commande.

L'application substituera les valeurs des paramètres par les valeurs par défaut.

Planification de la tâche dans la ligne de commande

Si l'application est utilisée en mode standard, vous pouvez configurer le calendrier de lancement pour les types de tâches suivants : *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Si l'application est utilisée en mode Light Agent pour protéger les environnements virtuels, vous pouvez configurer le calendrier de lancement pour les types de tâches suivants : *ODS*, *ODFIM*, *ContainerScan* et *InventoryScan*.

Vous pouvez afficher les valeurs actuelles des paramètres de planification de lancement des tâches sur la console ou dans un fichier de configuration.

Pour afficher les paramètres actuels de la planification de lancement des tâches sur la console, exécutez la commande suivante :

```
kesl-control --get-schedule <ID/nom de la tâche> [--json]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les paramètres actuels de la planification de lancement des tâches dans le fichier de configuration, exécutez la commande suivante :

```
kesl-control --get-schedule <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres de planification de la tâche seront écrits. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

  Exemples :

  Enregistrez les paramètres de la tâche de mise à jour dans un fichier nommé update_schedule.ini et enregistrez le fichier créé dans le répertoire actif :

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  Affichez les horaires des tâches de mise à jour sur la console :

  ```
  kesl-control --get-schedule 6
  ```

Vous pouvez modifier les paramètres de planification de lancement des tâches des manières suivantes :

- Importer les paramètres à partir d'un fichier de configuration contenant tous les paramètres de planification.
- À l'aide de la ligne de commande, spécifiez les paramètres individuels de la planification de la tâche au format `<nom du paramètre>=<valeur du paramètre>`.

Pour modifier les valeurs des paramètres de planification de lancement des tâches à l'aide d'un fichier de configuration, exécutez les actions suivantes :

1. Affichez les paramètres de la tâche dans le fichier de configuration à l'aide de la commande `kesl-control --get-schedule`.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande :

   `kesl-control --set-schedule <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]`

   où :

   - `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
   - `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres de planification de la tâche seront importés.
   - `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

   Toutes les valeurs des paramètres de planification de lancement des tâches spécifiées dans le fichier seront importées dans l'application.

Exemple :
Importer dans la tâche portant l'ID=2 les paramètres de planification depuis le fichier de configuration nommé /home/test/on_demand_schedule.ini :

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

Pour modifier les valeurs individuelles des paramètres de planification de lancement des tâches à l'aide de la ligne de commande, exécutez la commande suivante :

`kesl-control --set-schedule <ID/nom de la tâche> <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]`

où :

- `<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.
- `<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur de l'un des paramètres de planification de la tâche.

Les valeurs des paramètres spécifiés de planification de lancement des tâches seront modifiées.

Exemples :

Pour planifier le démarrage de la tâche toutes les dix heures, spécifiez les paramètres suivants :

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

Pour planifier le démarrage de la tâche toutes les dix minutes, spécifiez les paramètres suivants :

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

Pour planifier le démarrage de la tâche le 15 de chaque mois, spécifiez les paramètres suivants :

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

Pour planifier le démarrage de la tâche tous les mardis, spécifiez les paramètres suivants :

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

Pour planifier le démarrage de la tâche tous les 11 jours, spécifiez les paramètres suivants :

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

Gestion des paramètres généraux de l'application via la ligne de commande

Les paramètres généraux de l'application déterminent le fonctionnement de l'application dans son ensemble et le fonctionnement des fonctions individuelles.

Vous pouvez gérer les paramètres généraux de l'application à l'aide des commandes de gestion spéciales :

- Afficher les valeurs actuelles des paramètres généraux de l'application sur la console ou dans un fichier de configuration.
- Modifiez les paramètres généraux de l'application à l'aide d'un fichier de configuration contenant tous les paramètres généraux ou d'options de ligne de commande au format < `nom du paramètre` >=< `valeur du paramètre` >.

Avec les paramètres généraux, vous pouvez :

- Configurer l'utilisation de Kaspersky Security Network et d'une version allégée des bases de données de logiciels malveillants dans le fonctionnement de l'application.
- Configurer l'utilisation d'un serveur proxy dans le fonctionnement de l'application.
- Sélectionner le mode d'interception des opérations sur les fichiers (bloquer/ne pas bloquer les fichiers pendant l'analyse).
- Configurer les exclusions d'analyse des points de montage (exclusions globales).
- Configurer des exclusions à partir de l'analyse de la mémoire de processus.
- Activer ou désactiver l'analyse du conteneur en temps réel.
- Activer ou désactiver la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.
- Activer ou désactiver l'intégration avec Kaspersky Managed Detection and Response.
- Configurer l'utilisation des journaux d'événements.
- Configurer la limite d'utilisation des ressources du processeur pour les tâches d'analyse (telles que ODS).
- Limiter le nombre de tâches d'analyse personnalisée qu'un utilisateur non privilégié peut exécuter simultanément.

Affichage des paramètres généraux de l'application

Vous pouvez afficher les valeurs actuelles des paramètres généraux de l'application sur la console ou dans un fichier de configuration, que vous pouvez utiliser pour modifier les paramètres de l'application.

Pour afficher les valeurs actuelles des paramètres généraux de l'application sur la console, exécutez la commande suivante :

```
kesl-control --get-app-settings [--json]
```

où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les valeurs actuelles des paramètres généraux de l'application dans le fichier de configuration, exécutez la commande suivante :

```
kesl-control --get-app-settings --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'application seront écrits. Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Exemple :
Affichez les paramètres généraux de l'application dans un fichier nommé kesl_config.ini. Enregistrez le fichier créé dans le répertoire actuel :

```
kesl-control --get-app-settings --file kesl_config.ini
```

Modification des paramètres généraux de l'application

Sur la ligne de commande, vous pouvez modifier les paramètres généraux de l'application à l'aide de la commande `kesl-control --set-app-settings` :

- Vous pouvez modifier tous les paramètres généraux à l'aide du fichier de configuration, qui contient les paramètres généraux de l'application. Vous pouvez obtenir le fichier de configuration à l'aide de la commande d'affichage des paramètres généraux.
- Vous pouvez modifier des paramètres individuels à l'aide d'options de ligne de commande au format `<nom du paramètre>=<valeur du paramètre>`. Vous pouvez obtenir les valeurs actuelles des paramètres généraux de l'application à l'aide de la commande d'affichage des paramètres généraux.

Pour modifier les paramètres généraux de l'application à l'aide d'un fichier de configuration :

1. Exporter les paramètres généraux de l'application dans un fichier de configuration.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande :

   ```
   kesl-control --set-app-settings --file <chemin d'accès au fichier de configuration> [--json]
   ```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux de l'application. Si vous supprimez un paramètre dans le fichier de configuration, la valeur par défaut de ce paramètre sera affichée après l'exécution de la commande.

- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres généraux spécifiées dans le fichier seront importées dans l'application.

Pour modifier les paramètres généraux de l'application à l'aide des commutateurs de ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

où `<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur de l'un des paramètres généraux de l'application.

Les valeurs des paramètres généraux spécifiés seront modifiées.

Exemples :

Importez dans l'application les paramètres généraux depuis le fichier de configuration /home/test/kesl_config.ini :

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Définissez le niveau de détails faible pour le fichier de traçage :

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Ajoutez un point de montage que vous souhaitez exclure de l'interception des opérations sur les fichiers :

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Utilisation du filtre pour limiter les résultats des requêtes

Un filtre permet de limiter les résultats d'une requête lors de l'exécution de commandes de gestion de l'application.

Les conditions du filtre sont spécifiées à l'aide d'une ou plusieurs *expressions logiques* combinées à l'aide de l'opérateur logiques `and`. Les conditions du filtrage doivent être placées entre guillemets :

```
"<champ> <opérateur de comparaison> '<valeur>'"
```

```
"<champ> <opérateur de comparaison> '<valeur>' and <champ> <opérateur de comparaison> '<valeur>'"
```

où :

- < `champ` > est le nom du champ de la base de données.
- < `opérateur de comparaison` > est l'un des opérateurs de comparaison suivants :
  - > : supérieur à.
  - < signifie « inférieur à »
  - `like` correspond à la valeur spécifiée. Lorsque vous indiquez une valeur, vous pouvez utiliser des masques % : par exemple, l'expression logique "FileName like '%etc%'" définit la restriction « contient le texte "etc" dans le champ FileName »

    > L'opération de comparaison `like` fonctionne uniquement avec les champs stockés dans la base de données au format texte. L'opération `like` ne fonctionne pas avec les champs contenant des dates, des heures, des nombres ou d'autres types de données non textuels.

  - == : égal à.
  - `!` = : pas égal à.
  - >= : supérieur ou égal à.
  - <= signifie « inférieur ou égal à »
- < `valeur` > est la valeur du champ. La valeur doit être spécifiée entre guillemets simples (').

  Vous pouvez spécifier la valeur de date dans le système d'horodatage UNIX™ (nombre de secondes depuis le 1er janvier 1970, 00:00:00 (UTC)) ou au format AAAA-MM-JJ hh:mm:ss. La valeur de date et d'heure est spécifiée par l'utilisateur et affichée par l'application dans l'heure locale de l'utilisateur.

Vous pouvez utiliser le filtre dans les commandes de gestion suivantes de l'application :

- Afficher les informations relatives à certains événements actuels de l'application (Affichage des événements en ligne de commande, Affichage des événements dans Kaspersky Security Center) :

  ```
  kesl-control -W --query "< conditions de filtrage >"
  ```

- Afficher les informations relatives à certains événements de l'application (Affichage des événements en ligne de commande, Affichage des événements dans Kaspersky Security Center) dans le journal des événements :

  ```
  kesl-control -E --query "< conditions de filtrage >"
  ```

- Afficher des informations sur certains objets dans la sauvegarde :

  ```
  kesl-control -B --query "< conditions de filtrage >"
  ```

- Suppression des objets spécifiques de la sauvegarde :

```
kesl-control -B --mass-remove --query "< conditions de filtrage >"
```

Exemples :

Obtenez des informations sur les événements qui contiennent le texte "etc" dans le champ FileName :

```
kesl-control -E --query "FileName like '%etc%'"
```

Afficher des informations sur les événements de type ThreatDetected (menace détectée) :

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Afficher des informations sur les événements de type ThreatDetected générés par les tâches de type ODS :

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Afficher les informations sur les événements générés après la date spécifiée dans le système d'horodatage UNIX (le nombre de secondes écoulées depuis 00:00:00 (UTC), le 1er janvier 1970) :

```
kesl-control -E --query "Date > '1583425000'"
```

Afficher des informations sur les événements générés après la date spécifiée au format AAAA-MM-JJ hh:mm:ss :

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

Afficher des informations sur les fichiers dans la sauvegarde qui ont un niveau d'importance élevé :

```
kesl-control -B --query "DangerLevel == 'High'"
```

Exportation et importation des paramètres de l'application

L'importation des paramètres n'est pas disponible si l'application Kaspersky Endpoint Security est administrée via Kaspersky Security Center.

Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger des environnements virtuels, les paramètres de la tâche prédéfinie de type *Update* ne sont pas disponibles pour l'exportation ou l'importation.

Kaspersky Endpoint Security permet d'exporter et d'importer tous les paramètres de l'application pour le dépannage, la vérification des paramètres ou pour simplifier la configuration de l'application sur les appareils utilisateurs. Lorsque vous exportez les paramètres, tous les paramètres de l'application (y compris les paramètres généraux de l'analyse du conteneur, les paramètres d'analyse du trafic réseau, les paramètres généraux de l'application et les paramètres des tâches) sont enregistrés dans le fichier de configuration. Vous pouvez utiliser ce fichier de configuration pour importer des paramètres dans l'application.

Lors de l'importation ou de l'exportation de paramètres, l'application doit être en cours d'exécution. Il faut relancer l'application après l'importation des paramètres.

Lors de l'importation ou de l'exportation de paramètres depuis une version antérieure de l'application, les nouveaux paramètres prennent la valeur par défaut. L'importation des paramètres dans une version antérieure de l'application est impossible.

Pour exporter les paramètres de l'application, exécutez la commande suivante :

```
kesl-control --export-settings --file < chemin d'accès au fichier de configuration > [--
json]
```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration dans lequel les paramètres de l'application seront enregistrés.
- `--json` indique que les paramètres doivent être exportés vers le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'exportation se fera vers un fichier INI.

Pour importer les paramètres d'une application à partir d'un fichier, exécutez la commande suivante :

```
kesl-control --import-settings --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés dans l'application.
- `--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Lors de l'importation des paramètres depuis un fichier, la valeur `No` est établie pour les paramètres `UseKSN` et `CloudMode` et l'intégration MDR est désactivée. Pour lancer ou reprendre l'utilisation de Kaspersky Security Network, il faut spécifier la valeur `Basic` ou `Extended` pour le paramètre `UseKSN`. Pour activer le mode cloud, vous devez définir la valeur `Yes` pour le paramètre `CloudMode`. Le mode Cloud est disponible si l'utilisation de KSN est activée. Pour activer l'intégration MDR, vous devez d'abord activer Kaspersky Security Network en mode avancé, puis définir le paramètre `UseMDR` sur `Yes`.

Après l'importation des paramètres de l'application, les identifiants des tâches internes peuvent changer. Pour gérer les tâches, il est recommandé d'utiliser des noms de tâches.

Les paramètres de stratégie suivants ne peuvent pas être importés depuis la version 12.3 du plug-in Internet de l'application vers la version 12.4 de l'application :

- Zone de protection et zone d'exclusion de la Protection contre les fichiers malicieux et de la Protection contre le chiffrement
- Exclusions de processus de l'analyse par l'Analyse comportementale
- Appareils de confiance pour le Contrôle des appareils
- Zone d'analyse et zone d'exclusion du Contrôle de l'intégrité du système
- Règles du Contrôle Internet
- Paramètres du serveur proxy
- Exclusion de l'analyse de la mémoire des processus
- Exclusions globales (points de montage exclus de l'analyse)

Gestion des rôles d'utilisateur à l'aide de la ligne de commande

L'accès aux fonctions de l'application Kaspersky Endpoint Security via la ligne de commande est octroyé à l'utilisateur conformément à son rôle. Un *rôle* est un ensemble de droits et privilèges pour l'administration de l'application.

Dans un système d'exploitation, quatre groupes d'utilisateurs système sont créés : *kesladmin*, *kesluser*, *keslaudit* et *nokesl*. Quand un rôle de l'application est octroyé à un utilisateur système, cet utilisateur est ajouté au groupe correspondant (voir le tableau *Rôles* ci-dessous). Quand vous retirez un rôle à un utilisateur, cet utilisateur est retiré du groupe correspondant.

Si aucun rôle de l'application n'est attribué à un utilisateur, cet utilisateur appartient à un groupe spécifique d'*utilisateurs sans privilèges*.

Ainsi, les rôles correspondent à quatre groupes d'utilisateurs du système d'exploitation :

- kesladmin correspond au rôle d'administrateur
- kesluser correspond au rôle Utilisateur
- keslaudit correspond au rôle d'Auditeur
- nokesl est attribué à l'utilisateur qui n'a reçu aucun rôle Dans ce cas, l'utilisateur appartient au groupe distinct d'*utilisateurs sans privilèges*.

L'application a besoin de privilèges élevés dans le système d'exploitation pour protéger les appareils. L'application requiert les privilèges root pour exécuter certaines de ses fonctions de sécurité de base.

Le modèle d'accès basé sur les rôles de l'application inclut le rôle Administrateur (admin). Dans certains cas, les actions des utilisateurs ayant le rôle Administrateur peuvent entraîner l'exécution d'opérations avec les privilèges du superutilisateur du système d'exploitation (root).

Le rôle Administrateur doit uniquement être accordé à des utilisateurs de confiance. La compromission ou l'utilisation abusive de ce rôle Administrateur entraîne la compromission de l'appareil dans son ensemble et peut avoir un impact sur la sécurité, l'intégrité ou les performances de l'infrastructure de votre organisation, ainsi que sur les données utilisateur.

L'attribution du rôle Administrateur relève de la responsabilité du propriétaire du système et doit être effectuée conformément à la stratégie de contrôle d'accès de votre organisation et au niveau de confiance accordé aux utilisateurs concernés.

Rôles utilisateur

Nom du rôle	Rôle dans l'application	Groupe d'utilisateurs du système d'exploitation	Autorisations
Administrateur	admin	kesladmin	Gérez les paramètres de l'application et les paramètres des tâches via l'interface graphique et la ligne de commande de l'application sans utiliser la commande `sudo`. Gestion des licences de l'application. Attribuer n'importe quel rôle à n'importe quel utilisateur. Attribuer et révoquer un rôle à n'importe quel utilisateur (l'administrateur ne peut pas révoquer le rôle d'admin de lui-même). Afficher et gérer les stockages des utilisateurs.

Nom du rôle	Rôle dans l'application	Groupe d'utilisateurs du système d'exploitation	Autorisations
Utilisateur	user	kesluser	Gérer uniquement les tâches d'analyse personnalisée des fichiers. Démarrer et arrêter les tâches de mise à jour. Afficher les rapports des tâches personnalisées. Afficher des événements spécifiques communs à tous les utilisateurs de l'application.
Auditeur	audit	keslaudit	Affichage des paramètres de l'application. Afficher l'état de l'application. Afficher toutes les tâches, leurs paramètres et leurs planifications. Afficher tous les événements. Afficher tous les objets dans la sauvegarde.
—	—	nokesl	Le rôle dans l'application n'est pas attribué, il n'y a pas de droits.

Affichage d'une liste d'utilisateurs et de rôles

Pour consulter la liste des utilisateurs et de leurs rôles, exécutez la commande suivante :

```
kesl-control [-U] --get-user-list
```

Attribution d'un rôle à un utilisateur

Pour attribuer un rôle à un utilisateur spécifique, exécutez la commande suivante :

```
kesl-control [-U] --grant-role <rôle> <utilisateur>
```

Exemple :
Attribuer le rôle audit à l'utilisateur test15 :

```
kesl-control --grant-role audit test15
```

Révocation d'un rôle d'un utilisateur

Pour révoquer un rôle d'un utilisateur spécifique, exécutez la commande suivante :

```
kesl-control [-U] --revoke-role <rôle> <utilisateur>
```

Exemple :
Retirer le rôle audit de l'utilisateur test15 :

```
kesl-control --revoke-role audit test15
```

Lancement et arrêt de l'application

Une fois installée sur l'appareil, l'application Kaspersky Endpoint Security démarre automatiquement. De plus, par défaut, l'application est lancée automatiquement au démarrage du système d'exploitation (pour les niveaux d'exécution par défaut applicables à chacun des systèmes d'exploitation).

Par défaut, lorsque vous démarrez l'application Kaspersky Endpoint Security, les modules fonctionnels suivants de l'application sont automatiquement lancés :

- Protection contre les fichiers malicieux.
- Contrôle des appareils.
- Détection comportementale.
- Protection contre les menaces Internet : uniquement si l'un des navigateurs pris en charge est installé dans le système d'exploitation et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas installé dans les propriétés de la stratégie).
- Protection contre les menaces réseau : uniquement si les paramètres de la protection contre les menaces réseau sur l'appareil sont définis via une stratégie. Par défaut, la protection contre les menaces réseau est activée dans les propriétés de la stratégie. Si votre appareil utilise des paramètres configurés localement, la protection contre les menaces réseau est désactivée par défaut.

Lorsque vous lancez l'application sur l'appareil, des tâches de service sont automatiquement lancées pour assurer le fonctionnement des fonctions supplémentaires de l'application : fonctions d'activation de l'application et fonctions de la sauvegarde.

Par défaut, l'application exécute également des tâches personnalisées configurées sur la ligne de commande et configurées pour s'exécuter après le démarrage de l'application (mode de lancement `PS`).

Si vous arrêtez l'application, toutes les tâches sur en cours d'exécution sur l'appareil sont interrompues. Les tâches utilisateur interrompues ne sont pas reprises automatiquement après le redémarrage de l'application.

Démarrage et arrêt d'une application à l'aide de Web Console

Pour démarrer ou arrêter une application à distance :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste, sélectionnez l'appareil sur lequel vous souhaitez démarrer ou arrêter l'application, puis cliquez sur le lien portant le nom de l'appareil pour ouvrir la fenêtre des propriétés de ce dernier.

3. Choisissez l'onglet **Applications**.

4. Cochez la case en regard de l'application Kaspersky Endpoint Security.

5. Exécutez une des actions suivantes :

   - Si vous souhaitez exécuter l'application, cliquez sur le bouton **Démarrer**.
   - Si vous souhaitez arrêter l'application, cliquez sur le bouton **Arrêter**.

Vous pouvez surveiller l'état de fonctionnement de l'application à l'aide du widget **État de la protection** dans la fenêtre **Surveillance et rapports / Panneau de surveillance**.

Démarrage et arrêt d'une application à l'aide de la Console d'administration

Pour démarrer ou arrêter l'application sur un appareil client :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil sur lequel vous voulez démarrer ou arrêter l'application. Dans le menu contextuel du appareil, sélectionnez **Propriétés**.
4. Dans la fenêtre **Propriétés : <Nom de l'appareil>**, choisissez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Choisissez l'application Kaspersky Endpoint Security.
6. Exécutez une des actions suivantes :

   - Si vous souhaitez démarrer l'application, cliquez sur à droite de la liste des applications Kaspersky ou sélectionnez l'option **Lancer** dans le menu contextuel de l'application.
   - Pour arrêter l'application, cliquez sur à droite de la liste des applications Kaspersky ou sélectionnez l'option **Arrêter** dans le menu contextuel de l'application.

Démarrer et arrêter une application à l'aide de la ligne de commande

Pour pouvoir lancer l'application, le compte utilisateur root doit être propriétaire des répertoires suivants, et seul le propriétaire doit y avoir un accès en écriture : /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Lancement, relance et arrêt de l'application Kaspersky Endpoint Security

Pour lancer l'application, exécutez la commande :

```
systemctl start kesl
```

Pour arrêter l'application, exécutez la commande :

```
systemctl stop kesl
```

Pour redémarrer l'application, exécutez la commande suivante :

```
systemctl restart kesl
```

Surveillance de l'état de l'application Kaspersky Endpoint Security

L'état de Kaspersky Endpoint Security est surveillé par le service watchdog. Ce service est lancé automatiquement au lancement de l'application.

En cas de plantage de l'application, un fichier de vidage est produit et l'application se relance automatiquement.

Pour afficher l'état de l'application, exécutez la commande suivante :

```
systemctl status kesl
```

Afficher l'état de la protection de l'appareil et les informations sur les performances de l'application

Vous pouvez afficher des informations sur l'état de protection de l'appareil et l'état de fonctionnement de l'application Kaspersky Endpoint Security et de ses modules sur l'appareil.

Vous pouvez obtenir des informations sur l'état de sécurité de l'appareil des manières suivantes :

- Dans Web Console ou dans la Console d'administration en utilisant les états des appareils clients (*OK*, *Critique*, *Avertissement*). L'appareil sur lequel est installé l'Agent d'administration de Kaspersky Security Center est un appareil client de Kaspersky Security Center. L'état d'un appareil client peut passer à *Critique* ou *Avertissement* pour les raisons suivantes :

  - Conformément aux règles définies dans Kaspersky Security Center. Par exemple, l'état change si aucune application de protection n'est installée sur l'appareil, si aucune analyse antivirus n'a été effectuée depuis longtemps, si les bases de données de l'application sont obsolètes, si la licence a expiré ou si l'application est instable. Pour plus d'informations sur les raisons du changement de l'état et la définition des conditions d'attribution des états, consultez l'aide de Kaspersky Security Center.

  - Kaspersky Security Center reçoit l'état de l'appareil de l'application gérée, c'est-à-dire de Kaspersky Endpoint Security.

    La réception de l'état de l'appareil à partir d'une application gérée doit être activée dans Kaspersky Security Center dans les listes de conditions d'attribution des états *Critique* et *Avertissement*. Les conditions d'attribution des états des appareils sont configurées dans la fenêtre des propriétés du groupe d'administration.

  Pour en savoir plus sur les états de l'appareil client, consultez l'aide de Kaspersky Security Center.

- Dans Web Console ou dans la Console d'administration en utilisant les états des modules fonctionnels de l'application Kaspersky Endpoint Security sur l'appareil. Les propriétés de l'application Kaspersky Endpoint Security installée sur l'appareil affichent une liste des modules fonctionnels de l'application. Pour chaque module, son état est affiché.

- À partir de la ligne de commande, utilisez les commandes suivantes d'administration de l'application :

  - commande `kesl-control --app-info` qui affiche les informations sur le fonctionnement de l'application et l'état des modules fonctionnels et des tâches de l'application ;

  - La commande `kesl-control --supported-tech-info`, qui affiche une liste des fonctions de l'application, des informations sur leur état (utilisées ou non) et les technologies Linux avec lesquelles ces fonctions de l'application sont implémentées.

  - commande `kesl-control --get-statistic` qui affiche des statistiques de performances de l'application et une liste de points de montage;

  - commande `kesl-control --export-metrics` qui affiche des métriques sur l'état du système d'exploitation.

Afficher l'état de protection de l'appareil dans Web Console

Pour afficher l'état de sécurité de l'appareil dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez afficher les informations et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, sous l'onglet **Général**, sélectionnez la section **Protection**.

Les informations suivantes relatives à l'appareil s'affichent dans la section **Protection** :

- **Visible dans le réseau** : visibilité de l'appareil sélectionné sur le réseau : *Oui* ou *Non*.
- **État de l'appareil** : état de l'appareil client défini sur la base des critères définis par l'administrateur pour l'état de la protection sur l'appareil et l'activité de l'appareil dans le réseau: *OK*, *Critique* ou *Avertissement*.
- **Description de l'état** : raisons du passage de l'appareil à l'état *Critique* ou *Avertissement*.
- **État de la protection** : l'état actuel de la protection contre les menaces de fichiers sur l'appareil sélectionné, par exemple : *En cours d'exécution*, *Arrêté*, *En pause*.
- **Dernière analyse complète** : date et heure de la dernière exécution de la tâche d'analyse complète sur l'appareil sélectionné.
- **Virus détectés** : nombre total d'objets malveillants détectés sur l'appareil sélectionné (compteur de menaces détectées) depuis l'installation de l'application Kaspersky Endpoint Security.
- **Objets dont la désinfection a échoué** : nombre d'objets infectés que l'application Kaspersky Endpoint Security n'a pas pu désinfecter.

Affichage de l'état de protection de l'appareil dans la Console d'administration

Pour afficher l'état de la protection de l'appareil dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Protection**.

Les informations suivantes relatives à l'appareil s'affichent dans la section **Protection** :

- **État de l'appareil** : état de l'appareil client défini sur la base des critères définis par l'administrateur pour l'état de la protection sur l'appareil et l'activité de l'appareil sur le réseau.
- **Tous les problèmes** : liste complète des problèmes détectés par les applications gérées installées sur l'appareil sélectionné. Chaque problème est associé à un état que l'application vous suggère d'attribuer à un appareil.
- **État de la protection en temps réel** : état actuel de la protection contre les fichiers malicieux sur l'appareil sélectionné, par exemple, *En cours d'exécution* ou *Arrêtée*. Lorsque l'état de protection change, le nouvel état s'affiche dans la fenêtre des propriétés de l'appareil uniquement après la synchronisation de l'appareil avec le serveur d'administration.
- **Dernière tâche d'analyse à la demande** : date et heure auxquelles la dernière recherche d'applications malveillantes a été effectuée sur l'appareil sélectionné.
- **Total de menaces détectées** : nombre total de menaces détectées sur l'appareil sélectionné depuis l'installation de l'application antivirus (première analyse de l'analyse) ou depuis la dernière réinitialisation du compteur de menaces.

  Pour réinitialiser le compteur, cliquez sur le bouton **Mettre à zéro**.
- **Menaces actives** : nombre de fichiers non traités sur l'appareil sélectionné.

Affichage des informations sur l'application dans Web Console

Pour afficher les informations sur le fonctionnement de l'application dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez afficher les informations et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

   La fenêtre des propriétés de l'application s'ouvrira.

La fenêtre affiche les informations suivantes sur l'application Kaspersky Endpoint Security :

- L'onglet **Général** de la section **Informations** contient les informations générales sur l'application installée :
  - **Nom** : nom de l'application.
  - **Version** : numéro de version de l'application.
  - **Installé** : date et heure de l'installation de l'application sur l'appareil.
  - **Dernière mise à jour logicielle** : la date et heure de la dernière mise à jour des modules de l'application Kaspersky Endpoint Security.
  - **Dernière synchronisation** : date et heure de la dernière connexion entre l'appareil et le Serveur d'administration de Kaspersky Security Center.
  - **État actuel** : état de la protection contre les fichiers malicieux sur l'appareil, par exemple *En cours* ou *Suspendu*.
  - Le groupe **Mises à jour installées** contient des informations sur les versions installées des mises à jour pour l'application.
  - Le groupe **Base de données de l'application** contient des informations sur la date et l'heure de publication de la mise à jour des bases de données de l'application, ainsi que sur la date et l'heure de la dernière mise à jour.
- L'onglet **Général** de la section **Licences** renseigne sur les clés de licence : ajoutées à l'application et les licences liées à ces clés.
- L'onglet **Général** de la section **Modules** contient une liste des modules fonctionnels de l'application. Pour chaque module, l'état (par exemple, *Arrêté, Suspendu, Non installé*) et la version s'affichent.

  Dans la ligne **Mode Light Agent de protection des environnements virtuels**, vous pouvez visualiser des informations sur le mode d'utilisation de l'application :
  - l'état *en cours d'exécution* signifie que l'application est utilisée en mode Light Agent ;
  - l'état *Non installé* signifie que l'application est utilisée en mode standard.
- L'onglet **Événements** affiche une liste des événements de l'application sur l'appareil.

- L'onglet **Configuration des événements** affiche les types d'événements que l'application enregistre dans le stockage des événements et la durée de leur enregistrement.
- Sous l'onglet **Paramètres de l'application**, vous pouvez effectuer les opérations suivantes :
  - dans la section **Detection and Response**, vous pouvez gérer l'isolation du réseau de l'appareil ;
  - dans la section **Contrôle des applications**, vous pouvez exporter les paramètres configurés du module et d'une catégorie des applications vers un fichier et les importer à partir d'un fichier ;
  - dans la section **Statistiques**, vous pouvez afficher les statistiques du fonctionnement de l'application, ainsi qu'une liste des points de montage.

Affichage des informations sur le fonctionnement de l'application dans la Console d'administration

Pour afficher des informations sur le fonctionnement de l'application dans la Console d'administration de Kaspersky Security Center :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.

   La fenêtre des propriétés de l'application s'ouvrira.

La fenêtre affiche les informations suivantes sur l'application Kaspersky Endpoint Security :

- La section **Général** contient des informations générales sur l'application installée :
  - **Numéro de version** : numéro de version de l'application.
  - **Installé** : date et heure de l'installation de l'application sur l'appareil.
  - **État en cours** : état de la protection contre les fichiers malicieux sur l'appareil, par exemple *En cours* ou *Suspendu*.
  - **Dernière mise à jour logicielle** : la date et heure de la dernière mise à jour des modules de l'application Kaspersky Endpoint Security.
  - **Mises à jour installées** : informations sur les versions installées des mises à jour de l'application.
  - **Bases de l'application** : date et heure de publication de la mise à jour des bases de données de l'application.

- dans la section **Contrôle des applications**, vous pouvez exporter les paramètres configurés du module et d'une catégorie des applications vers un fichier et les importer à partir d'un fichier ;
- La section **Statistiques** affiche les statistiques de l'application, ainsi que des informations sur les points de montage.
- La section **Modules** contient une liste de tâches prédéfinies. Pour chaque module, l'état (par exemple, *Arrêté, Suspendu, Non installé*) et la version s'affichent.

  Dans la ligne **Mode Light Agent de protection des environnements virtuels**, vous pouvez visualiser des informations sur le mode d'utilisation de l'application :

  - l'état *en cours d'exécution* signifie que l'application est utilisée en mode Light Agent ;
  - l'état *Non installé* signifie que l'application est utilisée en mode standard.
- La section **Clés de licence** contient des informations sur la clé de licence active et la clé de licence de réserve.
- La section **Configuration des événements** affiche les types d'événements que l'application enregistre dans le stockage des événements et la durée de leur enregistrement.
- La section **Avancé** contient des informations sur le plug-in d'administration des applications.

Afficher des informations sur le fonctionnement d'une application dans la ligne de commande

Pour afficher les informations sur l'application, exécutez la commande :

```
kesl-control --app-info [--json]
```

où `--json` : afficher les données au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

À la suite de l'exécution de la commande, les informations suivantes seront affichées sur la console :

- **Nom**. Le nom de l'application.
- **Version**. Version actuelle de l'application.
- **Stratégie**. Informations indiquant si la stratégie de Kaspersky Security Center est appliquée sur l'appareil.
- Informations détaillées sur la stratégie appliquée sur l'appareil :
  - Nom de la stratégie.
  - La date et l'heure de la dernière application ou mise à jour de la stratégie sur l'appareil.
  - Le groupe d'administration Kaspersky Security Center auquel appartient l'appareil.
  - Liste des profils de stratégie appliqués sur l'appareil (le cas échéant).

Les informations détaillées sur la stratégie s'affichent si la réception des données étendues de la stratégie de Kaspersky Endpoint Security est activée dans les paramètres de l'Agent d'administration installé sur l'appareil (paramètre **Application peut recevoir des données étendues de la stratégie sur le l'appareil**). Le paramètre est désactivé par défaut. Pour plus d'informations sur les paramètres de l'Agent d'administration, consultez l'aide de Kaspersky Security Center.

- Informations sur la licence de base sous laquelle l'application est utilisée :
  - **Informations sur la licence de l'application** Informations sur la licence de l'application ou sur l'état de la clé de licence de l'application.
  - **Date d'expiration de la licence de Kaspersky Endpoint Security**. Date et heure (UTC) de fin de la durée de validité de la licence de l'application.
- Informations sur la licence pour activer des fonctionnalités supplémentaires de l'application. Les champs sont affichés si des clés pour des fonctionnalités supplémentaires ont été ajoutées à l'appareil protégé :
  - **Informations sur la licence EDR Optimum**. Informations sur la licence sous laquelle le module Kaspersky Endpoint Detection and Response Optimum est activé ou sur l'état de la clé de licence EDR Optimum.
  - **Date de fin de la durée de validité de la licence EDR Optimum**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence KUMA**. Informations sur la licence sous laquelle la fonctionnalité Kaspersky Unified Monitoring and Analysis Platform est utilisée ou sur l'état de la clé de licence KUMA.
  - **Date d'expiration de la licence KUMA**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence MDR**. Informations sur la licence sous laquelle le module Kaspersky Managed Detection and Response est activé ou sur l'état de la clé de licence MDR.
  - **Date d'expiration de la licence MDR**. Date et heure (UTC) de fin de la durée de validité de la licence.
  - **Informations sur la licence EDR Expert (on-premise)**. Informations sur la licence sous laquelle le module Endpoint Detection and Response Expert (on-premise) est activé, ou sur l'état de la clé de licence EDR Expert (on-premise).
  - **Date de fin de la durée de validité de la licence EDR Expert (on-premise)**. Date et heure (UTC) de fin de la durée de validité de la licence.
- **État de l'abonnement**. État de l'abonnement. Ce champ apparaît si l'application est exécutée sous un abonnement.
- **État du fichier MDR BLOB**. État du fichier BLOB MDR utilisé pour l'intégration avec Kaspersky Managed Detection and Response.
- **Date d'expiration de la licence du fichier MDR BLOB**. Date et heure (UTC) d'expiration de la licence d'utilisation de la fonctionnalité Kaspersky Managed Detection and Response. Ce champ s'affiche si le fichier de configuration BLOB pour l'intégration avec Kaspersky Managed Detection and Response est chargé.
- État **de la sauvegarde**. Informations sur l'état de la sauvegarde.
- **Utilisation de la sauvegarde**. Taille de la sauvegarde.

- **Dernière date d'exécution de la tâche Scan_My_Computer**. Moment auquel la tâche Analyse des logiciels malveillants a été lancée pour la dernière fois.
- **Date de la dernière publication des bases de données**. Date et heure de la dernière publication des bases de l'application.
- **Bases de l'application chargées**. Informations indiquant si les bases de données de l'application sont chargées.
- **État du module de noyau mis à jour**. Informations sur l'état du module de noyau mis à jour.
- **Utilisation de Kaspersky Security Network**. Informations sur l'utilisation de Kaspersky Security Network : `Mode étendu de KSN`, `Mode KSN de base` ou `Désactivé`.
- **Mode Light Agent pour la protection des environnements virtuels**. Informations sur l'application utilisée en mode Light Agent pour la protection des environnements virtuels. Si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent, cette ligne n'est pas affichée.
- **Mode Endpoint Detection and Response Agent**. Information indiquant que l'application est utilisée en mode Endpoint Detection and Response Agent. Si l'application est utilisée en mode standard ou en mode Light Agent, cette ligne n'est pas affichée.
- **Infrastructure de Kaspersky Security Network**. Informations sur la solution d'infrastructure utilisée pour travailler avec les bases de données de réputation de Kaspersky : `Kaspersky Security Network` ou `Kaspersky Private Security Network`.
- **Intégration avec Kaspersky Managed Detection and Response**. État de l'intégration avec Kaspersky Managed Detection and Response : `Activé`, `Désactivé`.
- **Intégration avec Kaspersky Endpoint Detection and Response Optimum**. État d'intégration avec Kaspersky Endpoint Detection and Response Optimum.
- **Protection contre les fichiers malicieux**. État de la protection contre les menaces de fichiers en temps réel.
- **Surveillance du conteneur**. État de l'analyse du conteneur en temps réel (Analyse du conteneur, Surveillance des conteneurs).
- **Contrôle de l'intégrité du système**. État du module Contrôle de l'intégrité du système.
- **Gestion du pare-feu**. État du module Gestion du pare-feu.
- **Protection contre le chiffrement**. État du module Protection contre le chiffrement.
- **Protection contre les menaces Internet**. État du module Protection contre les menaces Internet.
- **Contrôle des appareils**. État du module Contrôle des appareils.
- **Analyse des disques amovibles**. État du module Analyse des disques amovibles.
- **Protection BadUSB**. État du module Protection BadUSB.
- **Protection contre les menaces réseau**. État du module Protection contre les menaces réseau.
- **Détection comportementale**. État du module Détection comportementale.
- **Contrôle des applications**. État du module Contrôle des applications.

- **Contrôle Internet**. État du module Contrôle Internet .
- **Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)**. État d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA).
- **Intégration avec Sandbox**. État d'intégration avec Sandbox.
- **Intégration avec Kaspersky Unified Monitoring and Analysis Platform**. État d'intégration avec Kaspersky Unified Monitoring and Analysis Platform.
- **Intégration avec Kaspersky Network Detection and Response (KATA)** État de l'intégration avec Kaspersky Network Detection and Response (KATA).
- **Protection contre les menaces par emails**. État du module Protection contre les menaces par emails.
- **Actions après la mise à jour**. Les actions relatives à la mise à jour de l'application et aux actions qu'un utilisateur doit effectuer.
- **L'application est instable**. Les informations relatives à l'échec de l'application et à la création d'un fichier de vidage. Ce champs s'affiche quand un échec est survenu au lancement antérieur de l'application.

Affichage des statistiques du fonctionnement de l'application

Pour améliorer les performances, vous pouvez ajouter aux exclusions d'analyse les fichiers les plus fréquemment analysés par le module Protection contre les fichiers malicieux sur les fichiers, les chemins d'accès aux processus que le module Détection comportementale analyse le plus fréquemment, ainsi que les points de montage détectés sur l'appareil.

Sur les appareils dotés de systèmes d'exploitation prenant en charge la technologie fanotify, le moyen le plus efficace d'améliorer les performances consiste à ajouter des points de montage aux exclusions.

Vous pouvez afficher les statistiques relatives aux fichiers analysés et aux processus lancés les plus fréquemment, ainsi qu'une liste des points de montage détectés, de la manière suivante :

- dans Web Console ;
- dans la Console d'administration ;
- dans la ligne de commande.

Vous pouvez configurer les paramètres de calcul et d'affichage des statistiques par l'application dans le fichier de configuration kesl.ini dans la section `[ScannerImpactStats]`.

Afficher les statistiques sur le fonctionnement de l'application dans Web Console

Pour afficher les statistiques sur le fonctionnement de l'application dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez afficher les informations et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Statistiques** → **Statistiques de l'analyse**.

   La fenêtre **Statistiques de l'analyse** s'ouvrira.

   La fenêtre **Statistiques de l'analyse** affiche les statistiques suivantes de l'application :

   - La section **Fichiers les plus fréquemment analysés (Protection contre les fichiers malicieux)** affiche les chemins d'accès aux fichiers que le module Protection contre les fichiers malicieux analyse le plus fréquemment et le nombre de fois que le module accède à ces fichiers. Les fichiers sont affichés par ordre décroissant du nombre de fois où ils ont été consultés.

   - Le groupe **Applications les plus fréquemment analysées** affiche les chemins d'accès aux processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, ainsi que le nombre de ces lancements. Les chemins d'exécution des processus sont affichés par ordre décroissant du nombre d'exécutions.

   À l'aide des boutons **Exporter** situés en haut de chaque section, vous pouvez exporter les statistiques affichées dans ce groupe vers un fichier au format texte.

Afficher les statistiques sur le fonctionnement de l'application dans la Console d'administration

Pour afficher les statistiques de fonctionnement des applications dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.

5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.

6. Dans la fenêtre qui s'ouvre, sélectionnez la section **Statistiques → Statistiques de l'analyse**.

   Les statistiques suivantes de l'application sont affichées sur le côté droit de la fenêtre :

   - La section **Fichiers les plus fréquemment analysés (Protection contre les fichiers malicieux)** affiche les chemins d'accès aux fichiers que le module Protection contre les fichiers malicieux analyse le plus fréquemment et le nombre de fois que le module accède à ces fichiers. Les fichiers sont affichés par ordre décroissant du nombre de fois où ils ont été consultés.

   - Le groupe **Applications les plus fréquemment analysées** affiche les chemins d'accès aux processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, ainsi que le nombre de ces lancements. Les chemins d'exécution des processus sont affichés par ordre décroissant du nombre d'exécutions.

   À l'aide des boutons **Exporter** situé sous chaque groupe, vous pouvez exporter les statistiques affichées dans ce groupe vers un fichier au format texte.

Affichage de la liste de points de montage dans Web Console

Pour afficher une liste de points de montage dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils) → Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Dans la liste, recherchez l'appareil pour lequel vous souhaitez afficher les informations et cliquez sur le nom de l'appareil.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Statistiques → Points de montage**.

   La fenêtre **Points de montage** s'ouvre.

La fenêtre **Points de montage** affiche un tableau contenant les colonnes suivantes :

- **Chemin du point de montage** : chemin d'accès au point de montage détecté sur l'appareil.
- **Espace de noms** : informations sur la détection du point de montage dans l'espace de noms.
- **Exclu** : informations indiquant si le point de montage est ajouté aux exclusions d'analyse.

Les chemins d'accès aux points de montage sont triés comme suit :

- points de montage statiques, système, de service et autres
- paquets snap montés et points de montage dans leurs espaces de noms
- Points de montage créés par le système de gestion des conteneurs Docker

À l'aide du bouton **Exporter** situé en haut de la fenêtre au-dessus de la liste, vous pouvez exporter la liste des points de montage vers un fichier au format texte. Le fichier contient une liste de chemins d'accès aux points de montage, ainsi que les étiquettes `[Espace de noms]` et `[Exclu]`.

Affichage de la liste des points de montage dans la Console d'administration

Pour afficher la liste des points de montage dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil dont vous avez besoin et ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** en double-cliquant.
4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, sélectionnez la section **Applications**.

   Une liste des applications de Kaspersky installées sur l'appareil s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez Kaspersky Endpoint Security et double-cliquez dessus pour ouvrir la fenêtre des propriétés de l'application. Vous pouvez également utiliser le bouton **Propriétés** dans la partie inférieure de la fenêtre.
6. Dans la fenêtre qui s'ouvre, sélectionnez la section **Statistiques → Points de montage**.

   À droite de la fenêtre, le tableau **Liste des points de montage** s'affiche, contenant les colonnes suivantes :

   - **Chemin du point de montage** : chemin d'accès au point de montage détecté sur l'appareil.
   - **Espace de noms** : informations sur la détection du point de montage dans l'espace de noms.
   - **Exclu** : informations indiquant si le point de montage est ajouté aux exclusions d'analyse.

Les chemins d'accès aux points de montage sont triés comme suit :

- points de montage statiques, système, de service et autres
- paquets snap montés et points de montage dans leurs espaces de noms
- Points de montage créés par le système de gestion des conteneurs Docker

À l'aide du bouton **Exporter** situé sous la liste, vous pouvez exporter la liste des points de montage vers un fichier au format texte. Le fichier contient une liste de chemins d'accès aux points de montage, ainsi que les étiquettes `[Espace de noms]` et `[Exclu]`.

Affichage des statistiques du fonctionnement de l'application et de la liste des points de montage dans la ligne de commande

Pour afficher les statistiques de l'application et une liste des points de montage, exécutez la commande suivante :

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

où :

- `--files` : statistiques sur les fichiers que le module Protection contre les fichiers malicieux analyse le plus souvent et le nombre de fois où le module accède à ces fichiers ;
- `--processes` : statistiques sur les processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, et le nombre de ces lancements ;

  L'exclusion de processus de l'analyse par le module Détection comportementale ne les supprime pas des statistiques, mais améliore les performances de Kaspersky Endpoint Security.

- `--mountpoints` : liste des points de montage.

  La sortie affiche les informations suivantes :

  - `[excluded]` : indique si le point de montage a été ajouté aux exclusions d'analyse.
  - `[namespace]` : informations sur la détection du point de montage dans l'espace de noms ;
  - chemin d'accès au point de montage détecté sur l'appareil.

  Les chemins d'accès aux points de montage sont triés comme suit :

  - points de montage statiques, système, de service et autres
  - paquets snap montés et points de montage dans leurs espaces de noms
  - Points de montage créés par le système de gestion des conteneurs Docker

Vous pouvez spécifier une ou plusieurs clés dans n'importe quelle combinaison, ou vous pouvez ne spécifier aucune clé du tout. Si vous ne spécifiez pas de clés, l'application affichera trois listes : des statistiques sur les fichiers les plus fréquemment analysés, des statistiques sur les processus les plus fréquemment lancés et une liste des points de montage détectés sur l'appareil.

Collecte de métriques d'état du système

L'application Kaspersky Endpoint Security affecte le système d'exploitation lors de son fonctionnement. Pour analyser ce qui se passe, il est possible de collecter des métriques liées aux performances des applications.

Vous pouvez analyser les métriques dans des outils de visualisation de données tels que Grafana. Les métriques exportées peuvent être publiées vers les principaux systèmes de surveillance, tels que Prometheus et Zabbix.

Pour configurer la collecte de mesures sur les ressources du système d'exploitation utilisées par une application, exécutez la commande suivante :

```
kesl-control [-J] --export-metrics [--period <intervalle entre les exportations en secondes>|--interactive]
```

où :

- `--period` : affichage périodique des résultats sur la ligne de commande ;
- `--interactive` : affichage interactif (en appuyant sur la touche **Enter**).

L'exécution de cette commande affichera une liste de métriques dans la console.

Liste des métriques

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_system_descriptor_opened_count Sensor	Le nombre de descripteurs actuellement ouverts par le processus kesl. Si la croissance du nombre de descripteurs dépasse 250 par heure, il est recommandé de contacter le Support technique.
lfs_system_uptime_milliseconds Counter	Le nombre de millisecondes qui se sont écoulées depuis le démarrage du système d'exploitation jusqu'à présent.
lfs_system_memory_usage_bytes étiquette type=virtual Sensor	La quantité de mémoire virtuelle actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_memory_usage_bytes étiquette type=resident Sensor	La quantité de mémoire résidente actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_memory_usage_bytes étiquette type=swap Sensor	La quantité de mémoire de fichier de pagination actuellement utilisée par le processus kesl. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_system_cpu_usage_milliseconds étiquette type=user Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace utilisateur, depuis le démarrage du processus kesl jusqu'à maintenant. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_cpu_usage_milliseconds étiquette type=kernel Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace noyau, depuis le démarrage du processus kesl jusqu'à maintenant. Il est recommandé de définir vous-même la valeur de seuil en fonction des données du système. Vous pouvez obtenir les données vous-même ou utiliser un script pour collecter des informations. Pour un exemple de script, vous pouvez contacter le Support technique.
lfs_system_cpu_usage_milliseconds étiquette type=total Counter	Le nombre de millisecondes de temps CPU consommées par le processus kesl dans l'espace utilisateur et l'espace noyau, depuis le début du processus kesl jusqu'à maintenant. Si le temps CPU du processus kesl dépasse toute autre charge, il est recommandé de contacter le Support technique.
lfs_tcpSynInterceptor_connection_hanging_count Counter	Nombre total de connexions réseau gelées au stade d'établissement de la connexion réseau TCP entre le serveur et le client depuis le début du processus kesl jusqu'à maintenant (les connexions gelées sont celles qui ont attendu que le serveur à distance décide d'autoriser ou non la connexion de 1 seconde à 2 minutes, selon le paramètre système /proc/sys/net/ipv4/tcp_syn_retries). L'augmentation peut être due au fait que le serveur à distance n'est pas disponible ou est absent. Si l'augmentation du nombre de connexions réseau gelées est supérieure à 10 par minute, il est recommandé de contacter le Support technique.
lfs_tcpSynInterceptor_connection_count Sensor	Le nombre de connexions réseau actuellement en attente de connexion au serveur distant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=allow Counter	Nombre total de connexions interceptées qui ont été établies avec succès, depuis le début du processus kesl jusqu'à maintenant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=drop Counter	Le nombre total de connexions interceptées qui n'ont pas réussi à établir une connexion, depuis le début du processus kesl jusqu'à maintenant.
lfs_tcpSynInterceptor_verdict_count étiquette verdict=unknown Counter	Nombre total de connexions réseau depuis le début du processus kesl jusqu'à présent avec une décision non traitée du serveur à distance pour autoriser la connexion.
lfs_tcpSynInterceptor_verdict_latency_milliseconds Histogram	Histogramme du temps nécessaire à un serveur à distance pour prendre une décision concernant l'autorisation d'une connexion à partir du moment où un paquet SYN est intercepté jusqu'à ce qu'une décision soit prise à son sujet.
lfs_tproxy_connection_count étiquette direction=inbound Sensor	Le nombre actuel de connexions réseau entrantes interceptées à ce moment.
lfs_tproxy_connection_count étiquette direction=outbound Sensor	Le nombre actuel de connexions réseau sortantes interceptées à ce moment.
lfs_tproxy_connection_orphaned_count Counter	Nombre total de connexions (depuis le démarrage des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet) interceptées par l'application Kaspersky Endpoint Security, bien que leur interception n'ait pas été planifiée (par exemple, en raison d'une configuration iptables incompatible ou parce que l'application n'a pas eu le temps de traiter la nouvelle configuration d'interception). De telles connexions seront rejetées. Si le nombre total de ces connexions dépasse 10, cela peut indiquer un dysfonctionnement de l'application ou du système. Il est recommandé de contacter le Support technique.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_tproxy_threadPool_task_count Counter	Nombre total de tâches (nouvelle connexion, nouvelle partie de données, données envoyées, etc.) qui sont entrées dans le pool de threads depuis que les modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet ont commencé à fonctionner. Si la différence entre le nombre total de tâches et le nombre de tâches terminées augmente régulièrement, vous devez ajouter des ressources, configurer des exclusions ou contacter le Support technique.
lfs_tproxy_threadPool_task_duration_milliseconds Histogram	Histogramme du temps d'exécution des tâches traitant les connexions interceptées. Si 95 % des tâches prennent plus d'une seconde à s'exécuter, vous devrez peut-être ajouter des ressources, configurer des exclusions ou contacter le Support technique.
lfs_tproxy_socket_count Sensor	Nombre actuel de sockets (sockets d'écoute et sockets de connexion). La connexion interceptée possède 2 sockets de connexion.
lfs_trafficScanning_object_hanging_count Sensor	Le nombre actuel de vérifications d'objets gelées dans le trafic intercepté (les vérifications gelées sont celles qui durent plus d'une minute). Si le nombre total de vérifications d'objets gelées est supérieur à 35, il y a un problème avec les bases de données de l'application. Dans de tels cas, nous vous recommandons de contacter le Support technique.
lfs_trafficScanning_object_duration_milliseconds Histogram	Histogramme du temps de vérification des objets dans le trafic intercepté. Si le temps de vérification de 95 % des objets dépasse 1 seconde, vous devez ajouter des ressources, mettre à jour les bases de données de l'application ou contacter le Support technique. Si le taux de croissance des contrôles de paquets dans le trafic intercepté est de 0 et que la valeur de la métrique lfs_tproxy_threadPool_task_count n'est pas égale à 0, vous devez mettre à jour les bases de données de l'application ou contacter le Support technique.
lfs_fileMonitor_cache_size Sensor	La taille actuelle du cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers. Si la taille actuelle du cache de File Monitor est supérieure à 50 000, nous vous recommandons de contacter le Support technique.
lfs_fileMonitor_cache_hit_count Counter	Le nombre de hits dans le cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers.
lfs_fileMonitor_cache_miss_count Counter	Le nombre d'échecs de cache de File Monitor (cache de révision de fichiers), qui suit les modifications des fichiers.
lfs_faCache_file_count Sensor	Taille actuelle du cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés. Si la taille actuelle du cache des fichiers est supérieure à 100 000, il est recommandé de contacter le Support technique.
lfs_faCache_file_hit_count Counter	Le nombre de hits dans le cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés.
lfs_faCache_file_miss_count Counter	Le nombre d'échecs de cache des fichiers de l'intercepteur fanotify qui n'ont pas besoin d'être vérifiés.
lfs_faCache_volume_count Sensor	Taille actuelle du cache du point de montage de l'intercepteur fanotify.
lfs_oas_cache_file_count Sensor	La taille actuelle du cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés. Si la taille actuelle du cache des fichiers est supérieure à 100 000, il est recommandé de contacter le Support technique.
lfs_oas_cache_file_hit_count Counter	Le nombre de hits dans le cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés.
lfs_oas_cache_file_miss_count Counter	Le nombre d'échecs du cache des fichiers de la Protection contre les fichiers malicieux qui n'ont pas besoin d'être analysés.

Nom, étiquette et type de métrique interne	Description et valeur seuil recommandée
lfs_oas_cache_volume_count Sensor	La taille actuelle du cache du point de montage de la Protection contre les fichiers malicieux.
lfs_processManager_cache_size Sensor	Le nombre actuel des processus actifs dans le système qui sont dans le cache.
lfs_processManager_sache_hit_count Counter	Le nombre de hits du cache des processus dans le système.
lfs_processManager_cache_miss_count Counter	Le nombre d'échecs du cache des processus dans le système.
lfs_blockingProcessInterceptor_cache_size Sensor	La taille actuelle du cache des interpréteurs qui peuvent être utilisés pour exécuter des processus. La quantité dépend de l'intensité d'exécution des interprètes sur un appareil particulier. Si la taille actuelle du cache des fichiers est supérieure à 10000, il est recommandé de contacter le Support technique.
lfs_blockingProcessInterceptor_cache_hit_count Counter	Le nombre de hits dans le cache de l'interpréteur.
lfs_blockingProcessInterceptor_cache_miss_count Counter	Le nombre d'échecs du cache des interprètes.
lfs_prevention_cache_file_count Sensor	Taille actuelle du cache des fichiers de la tâche Prévention du lancement des objets qui n'ont pas besoin d'être vérifiés.
lfs_prevention_cache_file_hit_count Counter	Nombre de hits dans le cache des fichiers de la tâche Prévention du lancement des objets qui n'ont pas besoin d'être vérifiés.
lfs_prevention_cache_file_miss_count Counter	Nombre d'échecs de cache des fichiers de la tâche Prévention du lancement des objets qui n'ont pas besoin d'être vérifiés.
lfs_prevention_cache_volume_count Sensor	La actuelle du cache du point de montage pour la tâche Prévention du lancement des objets.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Sensor	Le temps nécessaire à la mise à jour actuelle des métriques pour être effectuée par tous les clients enregistrés dans le registre (en millisecondes).
eka_telemetry_metrics_registry_registered_callbacks Sensor	Le nombre actuel d'appels de fonction de mise à jour de métrique que MetricsRegistry a effectués pour tous les clients enregistrés.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Sensor	Le temps nécessaire pour collecter les valeurs de toutes les métriques du registre (en millisecondes). Si 99 % des valeurs de cette métrique sont supérieures à 1 seconde pendant 10 minutes, nous vous recommandons de contacter le Support technique.

Mise à jour des bases et des modules de l'application

La fonctionnalité des mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) peut ne pas être disponible dans le logiciel aux États-Unis.

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security garantit l'actualité de la protection de l'appareil. De nouveaux virus, applications malveillantes et autres applications présentant un danger apparaissent chaque jour à travers le monde. Les bases de données de l'application contiennent des informations relatives aux menaces et aux moyens de les neutraliser. Afin de pouvoir détecter les menaces rapidement, vous êtes vivement encouragé à mettre à jour régulièrement les bases de données et les modules de l'application.

Pour pouvoir bénéficier de ces mises à jour des bases de données régulières, votre licence doit être active. Sans licence en cours, vous ne pourrez réaliser qu'une seule mise à jour.

Pendant le processus de mise à jour, les bases de données et les modules de l'application sont téléchargés et installés sur votre appareil. Vous pouvez recevoir les mises à jour des bases et des modules de l'application depuis les serveurs de mise à jour de Kaspersky, depuis le stockage du Serveur d'administration, depuis les répertoires locaux ou réseau et depuis d'autres sources de mises à jour.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, le répertoire sur la SVM est utilisé comme source de mise à jour.

Lors de la mise à jour, les modules de l'application et les bases de données installées sur votre appareil sont comparées à la version à jour présente sur la source de mises à jour. Si vos bases de données et les modules de l'application diffèrent des versions respectives à jour, la portion manquante des mises à jour est installée sur l'appareil.

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). L'espace disque nécessaire peut atteindre 3 Go.

Les mises à jour sont téléchargées depuis les serveurs de mise à jour Kaspersky ou depuis d'autres serveurs FTP, HTTP ou HTTPS via les protocoles réseau standard. Les paramètres de la connexion Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, spécifiez les paramètres du serveur proxy dans les paramètres généraux de l'application.

Quelle que soit la source de mise à jour, le téléchargement du paquet de mise à jour et l'installation des mises à jour des bases de données et des modules de l'application sur l'appareil sont effectués à l'aide de la tâche *Mise à jour*. Une tâche prédéfinie *Mise à jour* est créée dans l'application. À l'aide de cette tâche, vous pouvez mettre à jour les bases de données et les modules de l'application selon une planification et à la demande et configurer les paramètres de mise à jour.

Si l'application Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, les bases de données sur les machines virtuelles protégées sont mises à jour à l'aide d'une tâche locale spéciale *Mise à jour*, dans laquelle le répertoire sur la SVM est spécifié comme source de mise à jour. La tâche de mise à jour démarre automatiquement. Vous ne pouvez pas supprimer cette tâche et modifier ses paramètres. La mise à jour des bases de données et des modules de l'application à l'aide des tâches créées dans Kaspersky Security Center n'est pas prise en charge.

Si l'application Kaspersky Endpoint Security est utilisée en mode standard ou en mode Endpoint Detection and Response Agent, vous pouvez utiliser dans Kaspersky Security Center la tâche de groupe *Mise à jour* créée par l'Assistant de configuration initiale après l'installation du plug-in MMC d'administration ou du plug-in Internet d'administration de Kaspersky Endpoint Security. Vous pouvez également créer des tâches de mise à jour personnalisées sur la ligne de commande et dans Kaspersky Security Center.

Vous pouvez configurer les paramètres suivants pour la mise à jour des bases de données et des modules de l'application :

- Sélectionnez la source à partir de laquelle l'application recevra les mises à jour, en fonction du schéma de mise à jour utilisé.
- Configurer le temps d'attente d'une réponse de la source de mise à jour sélectionnée lorsque vous essayez de vous y connecter. Si aucune réponse n'est reçue de la source de mise à jour dans le délai spécifié, l'application contacte une autre source de mise à jour spécifiée.
- Configurez le calendrier de lancement des tâches de mise à jour. Par défaut, l'application met à jour la base de données toutes les 60 minutes.

Vous pouvez également recevoir des mises à jour d'applications installées automatiquement (correctifs automatiques). Dans les paramètres de la tâche de mise à jour, vous pouvez sélectionner le mode de téléchargement et d'installation des correctifs automatiques : télécharger et installer, télécharger seulement ou ne pas télécharger.

À propos de la mise à jour des bases de données et des modules

Lors de la réalisation d'une mise à jour, les objets suivants sont téléchargés et installés sur l'appareil :

- Bases d'applications. Les bases de l'application comprennent les bases de données de signatures d'applications malveillantes, la description des attaques de réseau, les bases de données d'adresses Internet malveillantes et de phishing, les bases de données de bannières, les bases de données de spam ainsi que d'autres données.

  Si la mise à jour de la base de données sur l'appareil est interrompue ou se solde sur une erreur, l'application continue d'utiliser la version précédemment installée des bases de données. Si les bases de l'application n'ont pas été installées précédemment, l'application continue de fonctionner en mode "sans base". La mise à jour des bases de données et des modules de l'application est toujours disponible.

Si la mise à jour de la base de données est terminée avec succès, mais les bases de données elles-mêmes sont endommagées et l'application échoue plusieurs fois de suite, les bases de données seront automatiquement supprimées. L'application continuera à fonctionner en mode « sans bases de données », la mise à jour des bases de données et des modules de l'application restera disponible.

Une base de données est considérée comme étant à jour si son téléchargement remonte à moins de trois jours. Par défaut, l'application génère l'événement *Les bases de données de l'application sont obsolètes* si les dernières mises à jour des bases de données installées ont été publiées sur les serveurs de Kaspersky il y a plus de trois jours, mais moins de sept jours. Si les bases de données n'ont pas été mises à jour depuis sept jours, l'application génère l'événement *Les bases de données de l'application sont totalement obsolètes*.

- Modules de l'application. Les mises à jour des modules servent à éliminer les vulnérabilités de l'application et à améliorer les méthodes de protection de l'appareil. Les mises à jour des modules peuvent modifier le comportement des modules de l'application et ajouter de nouvelles fonctions.

  Il est possible d'installer une mise à jour des modules de l'application quel que soit l'état de l'application (lancée ou arrêtée, administrée par une stratégie de Kaspersky Security Center) et la planification des mises à jour. Kaspersky Endpoint Security continue à protéger votre appareil durant la mise à jour des modules de l'application. Lors de la mise à niveau, les paramètres de l'application et le journal des événements de l'application sont transférés vers la nouvelle version de l'application.

  Si le transfert des paramètres de l'application échoue pour une raison ou une autre, l'application est configurée selon les valeurs par défaut.

  Les modifications apportées aux paramètres de l'application après la fin de la mise à jour et avant le redémarrage de l'application ne sont pas enregistrées.

  Si l'application ne fonctionne pas correctement après sa mise à jour, elle rétablit automatiquement la version précédente. Nous vous conseillons de contacter le Support Technique de Kaspersky.

À propos des sources et des schémas de mise à jour

Une *source des mises à jour* est une ressource qui contient les mises à jour des bases de données et des modules de l'application Kaspersky Endpoint Security. Les sources de mises à jour peuvent être des serveurs FTP, HTTP ou HTTPS (par exemple, les serveurs de mise à jour de Kaspersky) ou des répertoires locaux ou réseau montés au préalable par l'utilisateur.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, les bases de données des machines virtuelles protégées sont mises à jour à partir du répertoire sur la SVM.

Les serveurs de mises à jour de Kaspersky sont les principales sources de mises à jour. Vous pouvez spécifier d'autres sources de mises à jour dans les paramètres de la tâche *Mise à jour*. Si une mise à jour ne peut pas être réalisée au départ d'une source de mise à jour, l'application Kaspersky Endpoint Security passe à la suivante.

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 mises à jour Kaspersky. Les serveurs de mise à jour Kaspersky sont répartis à travers le monde, ce qui garantit la haute fiabilité des mises à jour. Si une mise à jour ne peut être réalisée depuis un serveur, l'application passe au serveur suivant. Les mises à jour sont téléchargées via le protocole HTTPS.

- 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.

Vous pouvez utiliser le stockage du Serveur d'administration de Kaspersky Security Center comme stockage.

Le paquet de mise à jour est téléchargé dans le stockage du Serveur d'administration par la tâche du Serveur d'administration nommée *Télécharger les mises à jour dans le référentiel du Serveur d'administration*.

Si vous gérez une application à l'aide de Kaspersky Security Center Cloud Console, vous pouvez utiliser le stockage des points de distribution (appareils sur lesquels l'Agent d'administration est installé) comme stockage. Pour en savoir plus sur les points de distribution, reportez-vous à l'aide de Kaspersky Security Center.

2. Distribuer le paquet de mise à jour aux appareils clients.

   Le paquet de mise à jour est distribué aux appareils clients via *tâche de mise à jour* de Kaspersky Endpoint Security. Dans les paramètres de la tâche, vous devez sélectionner Kaspersky Security Center comme source de mises à jour.

- Mise à jour depuis un répertoire local ou réseau (SMB/NFS) monté par l'utilisateur, ou depuis un serveur FTP, HTTP ou HTTPS. Vous pouvez indiquer la sources de mises à jour personnalisée dans les paramètres de la tâche *Mise à jour*.

Mise à jour des bases de données et des modules de l'application dans Web Console

Dans Web Console, vous pouvez mettre à jour les bases de données et les modules de l'application à l'aide de la tâche *Mettre à jour*. Vous pouvez utiliser la tâche de groupe *Mise à jour* créée automatiquement et également créer des tâches de mise à jour personnalisées.

Pour configurer les paramètres de mise à jour dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Exécutez une des actions suivantes :

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur tous les appareils inclus dans un groupe d'administration spécifique, cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et sélectionnez le groupe d'administration dans la fenêtre qui s'ouvre.

     La liste affichera uniquement les tâches configurées pour le groupe d'administration sélectionné.

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur un ou plusieurs appareils (tâches pour un ensemble d'appareils), cliquez sur le lien dans le champ **Chemin actuel** en haut de la fenêtre et sélectionnez le nœud supérieur nommé Serveur d'administration dans la fenêtre qui s'ouvre.

     La liste affichera toutes les tâches créées sur le Serveur d'administration.

3. Dans la liste des tâches, sélectionnez la tâche souhaitée **Mise à jour** et ouvrez la fenêtre des propriétés de la tâche à l'aide du lien dans le nom de la tâche.

4. Dans la fenêtre des propriétés de la tâche, choisissez la section **Paramètres de l'application**. Sélectionnez la section **Sources des mises à jour** dans la liste de gauche.

5. Dans le tableau, sélectionnez la source de mise à jour à partir de laquelle l'application recevra les mises à jour de la base de données et des modules, en fonction du schéma de mise à jour utilisé.

   La liste des sources de mises à jour contient deux sources : les serveurs de mise à jour de Kaspersky et Kaspersky Security Center. La colonne **État** indique si l'application utilise cette source de mises à jour lors de l'exécution de la tâche. Vous pouvez ajouter d'autres sources de mises à jour à la liste en cliquant sur le bouton **Ajouter**. Vous pouvez désigner des serveurs FTP, HTTP ou HTTPS en tant que sources de mises à jour. Si une mise à jour ne peut pas être réalisée au départ d'une source de mise à jour, l'application Kaspersky Endpoint Security passe à la suivante. L'application s'adresse aux sources de mises à jour dans l'ordre où celles-ci apparaissent dans le tableau.

6. Sélectionnez la section **Paramètres** et configurez d'autres paramètres de mise à jour.

7. Sélectionnez l'onglet **Planification** et configurez la planification d'exécution de la tâche de mise à jour.

   Si vous avez sélectionné **Kaspersky Security Center** comme source de mise à jour, dans la liste déroulante **Lancement de la tâche**, sélectionnez **Lors du téléchargement des mises à jour dans le référentiel**. Pour plus d'informations sur la planification des tâches, consultez l'aide de Kaspersky Security Center.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

La tâche s'exécutera selon le calendrier configuré. Vous pouvez également exécuter la tâche manuellement.

Section Sources de mises à jour de la tâche Mise à jour

Paramètre	Description

Tableau des sources de mises à jour	Le tableau contient la liste des sources de mises à jour des bases de données. Au cours de la mise à jour, l'application s'adresse aux sources de mise à jour dans l'ordre où celles-ci apparaissent dans le tableau.
	Ce tableau contient les colonnes suivantes :
	• **Source des mises à jour** : adresse de la source de mises à jour :
	  • **Serveurs de mise à jour Kaspersky** qui hébergent les mises à jour des bases de données pour toutes les applications de Kaspersky (valeur par défaut).
	  • **Kaspersky Security Center** : Serveur d'administration de Kaspersky Security Center.
	  • Autres sources sur le réseau local ou sur Internet ajoutées par l'utilisateur : serveurs HTTP, HTTPS ou FTP ou répertoires sur les serveurs de réseau local.
	• **État** indique si la source de mises à jour est utilisée dans la tâche (**Activé** ou **Désactivé**). Vous pouvez modifier l'état à l'aide du commutateur dans le tableau ou à l'aide du commutateur **Utiliser cette source** dans la fenêtre **Source des mises à jour**, qui s'ouvre en cliquant sur le lien portant le nom de la source.
	Vous pouvez **ajouter**, **modifier**, supprimer, **déplacer vers le haut** ou **déplacer vers le bas** les sources de mise à jour dans le tableau.
	Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.
	Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Section Paramètres de la tâche Mise à jour

Paramètre	Description
Durée d'attente maximale de la réponse de la source des mises à jour (en secondes)	Temps d'attente maximal de la réponse à la demande de l'application en provenance de la source de mises à jour sélectionnée (en secondes). En l'absence de réponse à l'expiration de ce délai, l'événement relatif à la perte de connexion à la source de mises à jour est consigné dans le journal d'exécution des tâches. Valeurs admises : 0 à 120. Si vous saisissez la valeur 0, le délai d'attente de la réponse de la ressource choisie à la demande de l'application n'est pas limité. Valeur par défaut : 10 secondes.

Paramètre	Description
Mode de téléchargement des mises à jour de l'application	Dans la liste déroulante, vous pouvez sélectionner le mode de téléchargement des mises à jour d'applications installées automatiquement (correctifs automatiques) : • **Ne pas télécharger**. Lorsque cette option est sélectionnée, les correctifs automatiques ne sont pas téléchargés automatiquement. • **Télécharger seulement**. Lorsque cette option est sélectionnée, les correctifs automatiques sont téléchargés automatiquement, mais ne sont pas installés sur les appareils clients (valeur par défaut). • **Télécharger et installer**. La sélection de cette option de la liste téléchargera et installera automatiquement les correctifs automatiques sur les appareils clients. Après avoir installé le correctif automatique, l'application redémarrera automatiquement.

Mise à jour des bases de données et des modules de l'application dans la Console d'administration

Dans la Console d'administration, vous pouvez mettre à jour les bases de données et les modules de l'application à l'aide de la tâche *Mettre à jour*. Vous pouvez utiliser la tâche de groupe *Mise à jour* créée automatiquement et également créer des tâches de mise à jour personnalisées.

Pour configurer les paramètres de mise à jour dans la Console d'administration :

1. Dans la Console d'administration, effectuez l'une des opérations suivantes :

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur les appareils faisant partie d'un groupe d'administration spécifique, sélectionnez ce groupe d'administration dans l'arborescence de la console, puis sélectionnez l'onglet **Tâches** dans l'espace de travail.

   - Si vous souhaitez modifier les paramètres d'une tâche qui s'exécute sur un ou plusieurs appareils (tâches pour un ensemble d'appareils), sélectionnez le dossier **Tâches** dans l'arborescence de la console.

2. Dans la liste des tâches, sélectionnez la tâche nécessaire **Mise à jour** et ouvrez la fenêtre des propriétés d'un double-clic.

3. Dans la fenêtre des propriétés de la tâche, ouvrez la liste de gauche et sélectionnez l'option **Sources des mises à jour**.

4. Dans le tableau, sélectionnez la source de mise à jour à partir de laquelle l'application recevra les mises à jour de la base de données et des modules, en fonction du schéma de mise à jour utilisé.

   La liste des sources de mises à jour contient deux sources : les serveurs de mise à jour de Kaspersky et Kaspersky Security Center. La colonne **État** indique si l'application utilise cette source de mises à jour lors de l'exécution de la tâche. Vous pouvez ajouter d'autres sources de mises à jour à la liste en cliquant sur le bouton **Ajouter**. Vous pouvez désigner des serveurs FTP, HTTP ou HTTPS en tant que sources de mises à jour. Si une mise à jour ne peut pas être réalisée au départ d'une source de mise à jour, l'application Kaspersky Endpoint Security passe à la suivante. L'application s'adresse aux sources de mises à jour dans l'ordre où celles-ci apparaissent dans le tableau.

5. Sélectionnez la section **Paramètres** et configurez d'autres paramètres de mise à jour.

6. Sélectionnez la section **Planification** et configurez la planification d'exécution de la tâche de mise à jour.

   Si vous avez sélectionné **Kaspersky Security Center** comme source de mise à jour, dans la liste déroulante **Lancement planifié**, sélectionnez **Lors du téléchargement des mises à jour dans le référentiel**. Pour plus d'informations sur la planification des tâches, consultez l'aide de Kaspersky Security Center.

7. Cliquez sur le bouton **Appliquer** ou sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la tâche>** pour enregistrer vos modifications.

La tâche s'exécutera selon le calendrier configuré. Vous pouvez également exécuter la tâche manuellement.

Section Sources de mises à jour de la tâche Mise à jour

Paramètre	Description

Source des mises à jour	Le tableau contient la liste des sources de mises à jour des bases de données. Au cours de la mise à jour, l'application s'adresse aux sources de mise à jour dans l'ordre où celles-ci apparaissent dans le tableau.
	Ce tableau contient les colonnes suivantes :
	• **Adresse de la source** : adresse de la source de mises à jour.
	  • **Serveurs de mise à jour Kaspersky** qui hébergent les mises à jour des bases de données pour toutes les applications de Kaspersky (valeur par défaut).
	  • **Kaspersky Security Center** : Serveur d'administration de Kaspersky Security Center.
	  • Autres sources sur le réseau local ou sur Internet ajoutées par l'utilisateur : serveurs HTTP, HTTPS ou FTP ou répertoires sur les serveurs de réseau local.
	• **État** indique si la source de mises à jour est utilisée dans la tâche (**Utilisé** ou **Pas utilisé**). Vous pouvez modifier l'état en cochant ou en décochant la case **Utiliser cette source** dans la fenêtre **Source des mises à jour** qui s'ouvre lorsque vous cliquez sur le bouton **Modifier**.
	Vous pouvez **ajouter**, **modifier**, supprimer, **déplacer vers le haut** ou **déplacer vers le bas** les sources de mise à jour dans le tableau.
	Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.
	Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Section Paramètres de la tâche Mise à jour

Paramètre	Description
Durée d'attente maximale de la réponse de la source des mises à jour (en secondes)	Temps d'attente maximal de la réponse à la demande de l'application en provenance de la source de mises à jour sélectionnée (en secondes). En l'absence de réponse à l'expiration de ce délai, l'événement relatif à la perte de connexion à la source de mises à jour est consigné dans le journal d'exécution des tâches. Valeurs admises : 0 à 120. Si vous saisissez la valeur 0, le délai d'attente de la réponse de la ressource choisie à la demande de l'application n'est pas limité. Valeur par défaut : 10 secondes.
Mode de téléchargement des mises à jour de l'application	Dans la liste déroulante, vous pouvez sélectionner le mode de téléchargement des mises à jour d'applications installées automatiquement (correctifs automatiques) : • **Ne pas télécharger**. Lorsque cette option est sélectionnée, les correctifs automatiques ne sont pas téléchargés automatiquement. • **Télécharger seulement**. Lorsque cette option est sélectionnée, les correctifs automatiques sont téléchargés automatiquement, mais ne sont pas installés sur les appareils clients (valeur par défaut). • **Télécharger et installer**. La sélection de cette option de la liste téléchargera et installera automatiquement les correctifs automatiques sur les appareils clients. Après avoir installé le correctif automatique, l'application redémarrera automatiquement.

Mise à jour des bases de données et des modules de l'application dans la ligne de commande

Sur la ligne de commande, vous pouvez mettre à jour les bases de données et les modules de l'application des manières suivantes :

- Utilisation de la tâche prédéfinie Mise à jour (*Update*). Vous pouvez démarrer, arrêter, suspendre et reprendre cette tâche manuellement et configurer la planification de son exécution. Vous pouvez gérer les paramètres de mise à jour en modifiant les paramètres de cette tâche.

- Utilisation des tâches personnalisées des mises à jour (tâches de type *Update*). Vous pouvez exécuter des tâches personnalisées manuellement et configurer des planifications de lancement de tâches.

Paramètres de la tâche de la mise à jour

Paramètre	Description	Valeurs
`ConnectionTimeout`	Temps d'attente (en secondes) pour une réponse de la source de mise à jour lorsque vous essayez de vous y connecter. Si la source de mise à jour n'a pas répondu à l'issue du délai indiqué, l'application contacte la source de mise à jour suivante dans la liste.	Vous pouvez indiquer uniquement des nombres entiers compris entre 0 et 120. Valeur par défaut : 10.
`ApplicationUpdateMode`	Mode de téléchargement et d'installation des mises à jour d'applications installées automatiquement (correctifs automatiques).	`Disabled` : ne pas télécharger et ne pas installer les correctifs automatiques. `DownloadOnly` (valeur par défaut) : télécharger automatiquement les correctifs automatiques, mais ne les pas installer. `DownloadAndInstall` : télécharger et installer automatiquement les correctifs automatiques. Après avoir installé le correctif automatique, l'application redémarrera automatiquement.
La section **[Sources.item_#]** contient les paramètres suivants :		
`Enabled`	Utilisation de la source de mises à jour spécifiée via le paramètre `SourceType`. Pour exécuter la tâche, il faut activer l'utilisation d'au moins une source de mise à jour.	`Yes` (valeur par défaut) : l'application utilise la source de mises à jour. `No` : l'application n'utilise pas la source de mise à jour.
`SourceType`	Source à partir de laquelle l'application va recevoir les mises à jour.	`KLServers` (valeur par défaut) : l'application récupère les mises à jour depuis un des serveurs de mise à jour de Kaspersky. Les mises à jour sont téléchargées via le protocole HTTPS. `SCServer`. L'application télécharge les mises à jour sur l'appareil protégé depuis le Serveur d'administration installé dans le réseau local. Vous pouvez sélectionner cette source de mise à jour si vous utilisez l'application Kaspersky Security Center pour l'administration centralisée de la protection des appareils au sein de votre entreprise. `Custom`. L'application télécharge les mises à jour depuis une source personnalisée spécifiée dans le paramètre `URL`. Vous pouvez désigner les répertoires des serveurs HTTP, HTTP ou FTP ainsi que tous les répertoires sur tout appareil monté sur l'appareil client protégé, y compris les répertoires des appareils distants montés via les protocoles Samba ou NFS.

Paramètre	Description	Valeurs
URL	Adresse de la source de mise à jour personnalisée sur le réseau local ou sur Internet.	La valeur par défaut n'est pas définie. Exemples : `URL=http://example.com/bases/` : adresse du serveur HTTP sur lequel se trouve le répertoire contenant les mises à jour. `URL=/home/bases/` : répertoire qui contient les bases de l'application sur l'appareil protégé.

Mise à jour à l'aide de Kaspersky Update Utility

Afin d'économiser le trafic Internet, vous pouvez configurer les mises à jour des bases de données et des modules de l'application sur les appareils du réseau local de l'organisation à partir d'un répertoire partagé à l'aide de Kaspersky Update Utility. Pour ce faire, un des appareils du réseau local de l'organisation doit recevoir les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou depuis les serveurs de mise à jour de Kaspersky, puis copier les paquets de mise à jour reçus dans le répertoire partagé à l'aide de l'utilitaire. Les autres appareils du réseau local de l'organisation peuvent alors recevoir le paquet de mise à jour depuis ce répertoire partagé.

Pour configurer Kaspersky Security Center afin qu'il mette à jour les bases de données à partir d'un répertoire partagé à l'aide de l'utilitaire Kaspersky Update Utility :

1. Installez Kaspersky Update Utility sur l'un des appareils du réseau local de l'organisation.

   Vous pouvez télécharger le paquet de distribution de Kaspersky Update Utility depuis le site Internet du Support technique de Kaspersky.

2. Configurez la copie du paquet de mise à jour dans le répertoire partagé dans les paramètres de Kaspersky Update Utility.

   Sélectionnez la source de mises à jour (par exemple, le stockage du Serveur d'administration) et le répertoire partagé dans lequel Kaspersky Update Utility va copier les paquets de mise à jour. Pour des informations détaillées sur l'utilisation de Kaspersky Update Utility, consultez la Base de connaissances Kaspersky.

3. Configurez la mise à jour des bases et des modules de l'application à partir du répertoire partagé indiqué vers les autres appareils du réseau local de l'organisation :

   a. Ouvrez les propriétés de la tâche **Mise à jour** qui sera effectuée sur l'appareil souhaité à l'aide de Web Console ou à l'aide de la Console d'administration.

   b. Dans les propriétés de la tâche, accédez à la section **Sources de mises à jour**.

   c. Sélectionnez l'option **Autres sources sur le réseau local ou sur Internet** dans le groupe **Source des mises à jour**.

   d. Dans le tableau des sources de mises à jour, cliquez sur le bouton **Ajouter** et précisez le chemin d'accès au répertoire partagé.

      L'adresse de la source des mises à jour doit correspondre à l'adresse renseignée dans les paramètres de Kaspersky Update Utility.

   e. Cochez la case **Utiliser cette source**, puis cliquez sur **OK**.

f. Dans le tableau des sources de mises à jour, définissez l'ordre d'utilisation à l'aide des boutons **Haut** et **Bas**.

g. Enregistrez les modifications apportées aux paramètres de la tâche.

Pour configurer dans la ligne de commande les mises à jour des bases de données à partir d'un répertoire partagé à l'aide de Kaspersky Update Utility :

1. Installez Kaspersky Update Utility sur l'un des appareils du réseau local de l'organisation.

   Vous pouvez télécharger le paquet de distribution de Kaspersky Update Utility depuis le site Internet du Support technique de Kaspersky.

2. Configurez la copie du paquet de mise à jour dans le répertoire partagé dans les paramètres de Kaspersky Update Utility.

   Sélectionnez la source de mises à jour (par exemple, le stockage du Serveur d'administration) et le répertoire partagé dans lequel Kaspersky Update Utility va copier les paquets de mise à jour. Pour des informations détaillées sur l'utilisation de Kaspersky Update Utility, consultez la Base de connaissances Kaspersky.

3. Configurez la mise à jour des bases de données et des modules de l'application à partir du répertoire partagé spécifié sur d'autres appareils du réseau local de l'organisation : dans les `Update` paramètres de la tâche, définissez `SourceType=Custom` et indiquez le chemin d'accès au répertoire partagé dans la section `[Sources.item_#]`.

   L'adresse de la source des mises à jour doit correspondre à l'adresse renseignée dans les paramètres de Kaspersky Update Utility.

Annulation de la mise à jour des bases et des modules de l'application

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'annulation de la mise à jour des bases à l'aide d'une tâche n'est pas prise en charge.

Une fois les bases de données mises à jour pour la première fois, la fonction d'annulation de la mise à jour des bases de données de l'application est disponible.

Chaque fois qu'un utilisateur démarre le processus de mise à jour, Kaspersky Endpoint Security crée une copie de sauvegarde des bases de données actuelles. Cela vous permet de ramener les bases de l'application à une version antérieure si nécessaire.

L'annulation de la dernière mise à jour est utile, par exemple, lorsque la nouvelle version de la base de données de l'application contient une signature non valide qui fait que l'application Kaspersky Endpoint Security bloque une application ne présentant aucun danger.

Dans la ligne de commande pour restaurer les mises à jour, vous pouvez exécuter la tâche prédéfinie *Annulation de la mise à jour des bases (Rollback)* ou créer et lancer des tâches personnalisées d'annulation de mise à jour des bases (tâches de type *Rollback*).

Dans Kaspersky Security Center, vous pouvez créer des tâches d'annulation des mises à jour pour les groupes d'administration ou les appareils individuels à l'aide de Web Console ou à l'aide de la Console d'administration.

La tâche *Annulation de la mise à jour des bases* n'a pas de paramètres.

Protection contre les fichiers malicieux

Le module Protection contre les fichiers malicieux permet d'éviter l'infection du système de fichiers de l'appareil. Le module est activé automatiquement avec les paramètres par défaut lorsque vous lancez l'application Kaspersky Endpoint Security. Il réside dans la mémoire vive de l'appareil et analyse en temps réel tous les fichiers ouverts, enregistrés et exécutés.

Lorsqu'une application malveillante est détectée, Kaspersky Endpoint Security peut supprimer le fichier infecté et mettre fin au processus malveillant lancé à partir de ce fichier.

Le fonctionnement du module est affecté par le mode d'interception des opérations sur les fichiers, que vous pouvez sélectionner dans les paramètres généraux de l'application. Par défaut, l'accès au fichier est bloqué pendant l'analyse.

Si un utilisateur disposant des privilèges root n'a pas accès à un fichier situé dans un répertoire distant monté sur l'appareil via le protocole NFS4, l'application bloque l'accès à ce fichier pour tous les utilisateurs.

Si la Protection contre les fichiers malicieux est activée et que la Surveillance des conteneurs (Analyse du conteneur, Surveillance des conteneurs) est activée, l'application analyse également tous les espaces de noms et conteneurs sur tous les systèmes d'exploitation pris en charge.

Vous pouvez activer et désactiver la protection contre les fichiers malicieux, ainsi que configurer les paramètres de la protection :

- Sélectionnez le mode d'analyse des fichiers (à l'ouverture, à l'ouverture et à la modification).
- Activer ou désactiver l'analyse des archives, des bases de données de messagerie et des messages électroniques au format texte.
- Excluez temporairement les fichiers au format texte de la nouvelle analyse.
- Limitez la taille de l'objet analysé et la durée de l'analyse de l'objet.
- Sélectionner les actions que l'application va exécuter sur les objets infectés.
- Configurer les *zones d'analyse*. L'application analysera les objets dans la zone spécifiée du système de fichiers.
- Configurez les exclusions d'objets de l'analyse. Une *exclusion de l'analyse* est un ensemble de conditions. Lorsque ces conditions sont remplies, l'application n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez exclure de l'analyse :
  - objets par noms ou masques ;
  - objets par les noms des menaces détectées dans les objets ;
  - fichiers et répertoires dans des zones spécifiées du système de fichiers ;
  - processus et fichiers modifiés par le processus spécifié.

L'application exclut automatiquement certains processus internes de l'analyse, comme le processus du serveur Watchdog.

- Configurer l'utilisation de l'analyseur heuristique et de la technologie iChecker pendant l'analyse.
- Activer ou désactiver l'enregistrement dans le journal des informations sur les objets non infectés analysés, sur l'analyse des objets dans les archives et sur les objets non traités.

Pour optimiser le fonctionnement du module Protection contre les fichiers malicieux, vous pouvez configurer l'exclusion de l'analyse des fichiers copiés à partir des répertoires réseau. L'analyse des fichiers aura lieu uniquement après la fin de la copie dans le répertoire local. Pour exclure de l'analyse les fichiers des répertoires réseau, vous devez configurer une exclusion de processus pour l'utilitaire destiné à copier les fichiers depuis les répertoires réseau (par exemple, pour l'utilitaire `cp`). Si vous gérez une application à l'aide de Kaspersky Security Center, vous pouvez configurer l'exclusion par processus dans Web Console ou dans la Console d'administration. Si vous gérez votre application à l'aide de la ligne de commande, vous pouvez configurer l'exclusion par processus en ajoutant la section [ExcludedForProgram.item_#] aux `[ExcludedForProgram.item_#]` de type OAS.

Configuration de la protection contre les menaces de fichiers dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de la protection contre les fichiers malicieux dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Protection contre les fichiers malicieux**).

Configuration de la protection contre les fichiers malicieux dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les fichiers malicieux dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale** → **Protection contre les fichiers malicieux**).

Paramètres du module Protection contre les fichiers malicieux

Paramètre	Description
Activer la Protection contre les fichiers malicieux	La case active ou désactive le module Protection contre les fichiers malicieux sur tous les appareils administrés. La case est cochée par défaut.
Mode de la Protection contre les fichiers malicieux	Cette liste déroulante permet de sélectionner le mode de fonctionnement du module Protection contre les fichiers malicieux : • **Mode intelligent** (valeur par défaut) analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture, s'il a été modifié. Si un processus accède plusieurs fois à un fichier au cours d'une certaine période et le modifie, l'application analyse à nouveau le fichier uniquement lorsque le processus le ferme pour la dernière fois. • **À l'accès** analyse le fichier lors de la tentative d'ouverture pour lecture, exécution ou modification. • **À l'accès et à la modification** analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture, s'il a été modifié.

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre <Nouvelle zone d'analyse>

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la Protection contre les fichiers malicieux.

Paramètres de la Protection contre les menaces sur les fichiers

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si cette case est cochée, Kaspersky Endpoint Security analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en activant et en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les archives. La case est décochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si cette case est cochée, Kaspersky Endpoint Security analyse les archives autoextractibles. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est décochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, Kaspersky Endpoint Security analyse les fichiers des bases de messagerie. Si la case est décochée, Kaspersky Endpoint Security n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, Kaspersky Endpoint Security analyse les messages au format texte brut. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer les fichiers texte	Exclusion temporaire de l'analyse des fichiers au format texte. Si la case est cochée, Kaspersky Endpoint Security n'analysera pas les fichiers texte si ces fichiers ont été utilisés à nouveau par le même processus au cours des 10 minutes après la dernière analyse. Ce paramètre permet d'optimiser l'analyse des journaux de fonctionnement des applications. Si cette case est décochée, Kaspersky Endpoint Security analyse les fichiers texte. La case est décochée par défaut. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.
Ignorer les fichiers journaux de la base de données	Exclure temporairement les fichiers journaux de base de données de l'analyse. Si la case est cochée, l'application ne vérifiera pas le fichier journal de la base de données si le fichier journal est réutilisé par le même processus dans les 10 minutes suivant la dernière vérification. Ce paramètre permet d'optimiser la vérification des journaux de la base de données. Si la case à cocher est décochée, l'application vérifie les fichiers journaux de la base de données. La case est décochée par défaut. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.

Paramètre	Description
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, Kaspersky Endpoint Security interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 60.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, Kaspersky Endpoint Security analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *ObjectProcessed* pour tout objet analysé. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *ObjectProcessed*. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *ObjectNotProcessed*. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *ObjectNotProcessed*. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, Kaspersky Endpoint Security enregistre dans le journal les événements de type *PackedObjectDetected*. Si cette case est décochée, Kaspersky Endpoint Security n'enregistre pas dans le journal les événements de type *PackedObjectDetected*. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, Kaspersky Endpoint Security analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, Kaspersky Endpoint Security analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Paramètres de la Protection contre les menaces sur les fichiers

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; bloquer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application bloque l'accès à l'objet infecté. • **Bloquer**. Lorsque vous sélectionnez cette action, l'application bloque l'accès à l'objet infecté. Une fois désinfecté et supprimé, une copie de l'objet infecté sera placée dans la sauvegarde.

Exclusions de la Protection contre les fichiers malicieux

Une *exclusion de la protection* est un ensemble de conditions qui doivent être remplies pour que l'application Kaspersky Endpoint Security ne recherche pas de virus et autres applications malveillantes dans les objets. Vous pouvez également exclure des objets de l'analyse en fonction des masques et noms de menaces et configurer des exclusions pour les processus.

Dans la Console d'administration, vous pouvez gérer les exclusions de la Protection contre les fichiers malicieux dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale → Exclusions de la Protection contre les fichiers malicieux**).

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Exclusions par processus	Ce groupe de paramètres contient le bouton **Configurer**, qui ouvre la fenêtre **Exclusions par processus**. Dans cette fenêtre, vous pouvez configurer l'exclusion de l'activité de processus de l'analyse.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.

Paramètre	Description
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre <Nouvelle zone d'exclusion>

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions par processus

La fenêtre contient les zones d'exclusion en fonction des processus. La zone d'exclusion en fonction des processus vous permet de configurer l'exclusion de l'activité d'analyse du processus spécifié et des fichiers modifiés par le processus spécifié. Par défaut, la liste contient deux zones d'exclusion contenant les chemins d'accès aux Agents d'administration. Vous pouvez supprimer ces exclusions si nécessaire.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.

Paramètre	Description
Chemin	Chemin d'accès complet au processus exclu.
État	L'état indique si cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Processus de confiance

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**. Le champ de saisie ne peut être vide.
Chemin d'accès au processus exclu	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse. Si un module de noyau mis à jour est utilisé pour intercepter les événements système, le processus spécifié est exclu de l'interception dans tous les espaces de noms.
Appliquer aux processus enfants	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre **Chemin d'accès au processus exclu**. La case est décochée par défaut.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion de cette zone pour l'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Chemin d'accès aux fichiers modifiés	Le groupe de paramètres vous permet de définir des exclusions d'analyse pour les fichiers que le processus modifie. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si **Monté** ou **Partagé** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante des protocoles d'accès : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des **masques** pour spécifier le chemin. Le champ de saisie ne peut être vide. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ **Chemin d'accès aux fichiers modifiés**. Vous pouvez ajouter, modifier et supprimer des masques.

Configuration de la Protection contre les fichiers malicieux via la ligne de commande

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces de fichiers à l'aide de la tâche prédéfinie de protection contre les fichiers malicieux (*File_Threat_Protection*).

La tâche Protection contre les fichiers malicieux est lancée par défaut. Vous pouvez démarrer et arrêter cette tâche manuellement.

Les privilèges du rôle d'administrateur sont nécessaires pour arrêter et démarrer la tâche Protection contre les fichiers malicieux à partir de la ligne de commande.

Vous pouvez configurer les paramètres de protection contre les fichiers malicieux en modifiant les paramètres de la tâche prédéfinie Protection contre les fichiers malicieux.

Paramètres de la tâche de protection contre les fichiers malicieux

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Protection contre les fichiers malicieux.

Paramètres de la tâche de protection contre les fichiers malicieux

Paramètre	Description	Valeurs
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées. Il n'est pas recommandé d'activer ce paramètre, car l'analyse des archives réduit les performances du fait que l'accès au fichier d'archive est bloqué avant que le fichier ne soit décompressé dans un répertoire temporaire et analysé.	`Yes` : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` (valeur par défaut) : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` : analyse les archives autoextractibles. `No` (valeur par défaut) : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SkipPlainTextFiles`	Exclusion temporaire de l'analyse des fichiers au format texte. Ce paramètre permet d'optimiser l'analyse des journaux de fonctionnement des applications. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.	`Yes` : n'analyse pas les fichiers au format texte si ceux-ci ont été à nouveau utilisés par ce même processus au cours des 10 minutes suivant la dernière analyse. `No` (valeur par défaut) : analyse les fichiers au format texte.
`SkipDatabaseJournals`	Exclure temporairement les fichiers journaux de base de données de l'analyse. Ce paramètre permet d'optimiser la vérification des journaux de la base de données. Ce paramètre est appliqué si vous utilisez le mécanisme d'interception des événements système basé sur fanotify. Lors de l'utilisation du module de noyau mis à jour, la vérification est optimisée par la mise en cache des résultats.	`Yes` : ne pas analyser les fichiers journaux de la base de données si ceux-ci ont été à nouveau utilisés par ce même processus au cours des 10 minutes suivant la dernière analyse. `No` (valeur par défaut) : analyser les fichiers journaux de la base de données.

Paramètre	Description	Valeurs
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 60.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectBlockIfNotPossible` (désinfecter ; bloquer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application bloque l'accès à l'objet infecté. `Block` (bloquer) : l'application bloque l'accès à un objet infecté. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque.
	Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

Paramètre	Description	Valeurs
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`ScanByAccessType`	Mode de fonctionnement de la tâche Protection contre les fichiers malicieux. Le paramètre `ScanByAccessType` s'applique seulement à la tâche de protection contre les fichiers malicieux.	`SmartCheck` (valeur par défaut) : analyse un fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture s'il a été modifié. Si un processus lors de son fonctionnement accède plusieurs fois à un fichier et le modifie, l'application analyse à nouveau le fichier uniquement lorsque le processus le ferme pour la dernière fois. `OpenAndModify` : analyse le fichier en cas de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermeture s'il a été modifié. `Open` : analyse le fichier en cas de tentative d'ouverture en lecture, ou pour exécution ou modification.
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`. Exemple : `AreaDesc=" Analyse des bases de messagerie "`
`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple : `AreaMask_item_< numéro d'élément >=*doc`

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS.

Paramètre	Description	Valeurs
		`Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application évite d'analyser uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut de l'analyse tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets de l'analyse).

Paramètre	Description	Valeurs
Path	Le chemin d'accès au répertoire contenant les objets exclus.	< chemin d'accès au répertoire local > – exclut les objets du répertoire spécifié (y compris les sous-répertoires) de l'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • [container-id:<id>]/<path to local directory> • [container-name:<name>]/<path to local directory> • [image-id:<id>]/<path to local directory> • [image-name:<name>]/<path to local directory> Où : <id> est l'ID du conteneur. <name> est le nom du conteneur <path to local directory> est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : [container-id:<id>], [container-name:<name>], [image-id:<id>] et [image-name:<name>]/path to local directory>. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • [container-name:<name>][image-name:<name>]/path to local directory> • [container-id:<id>][image-name:<name>]/<path to local directory> • [image-name:<name>][image-id:<id>]/<path to local directory> • [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory> • [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory> Vous pouvez utiliser des masques (caractères ? et *) dans les noms et les identifiants. Vous pouvez utiliser le caractère * (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère * au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère / dans le nom du fichier ou du répertoire. Par exemple, /dir/*/file ou /dir/*/*/file. Vous pouvez saisir deux caractères * consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, /dir/**/file*/ ou /dir/file**/. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/file est un masque incorrect. Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Mounted:NFS : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS.

Paramètre	Description	Valeurs
		`Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<type de système de fichiers>` : exclure de l'analyse toutes les ressources du système de fichiers de l'appareil spécifié.
La section **[ExcludedForProgram.item_#]** contient les paramètres suivants :		
`ProgramPath`	Chemin d'accès au processus exclu. Si un module de noyau mis à jour est utilisé pour intercepter les événements système, le processus spécifié est exclu de l'interception dans tous les espaces de noms.	`< chemin d'accès complet au processus >` – Exclut de l'analyse le processus dans le répertoire local spécifié.
`ApplyToDescendants`	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre `ProgramPath`.	`Yes` : exclut le processus spécifié et tous ses processus enfants de l'analyse. `No` (valeur par défaut) : exclut uniquement le processus spécifié de l'analyse, n'exclut pas les processus enfants de l'analyse.
`AreaDesc`	Description de la zone d'exclusion de processus.	Valeur par défaut : `All objects`.
`UseExcludedForProgram`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de processus. Dans la zone d'exclusion des processus, l'application évite d'analyser uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut de l'analyse tous les objets de la zone d'exclusion des processus. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets de l'analyse).

Paramètre	Description	Valeurs
`Path`	Chemin d'accès au répertoire contenant des fichiers que le processus modifie.	`< chemin d'accès au répertoire local >` exclut les objets du répertoire indiqué de l'analyse. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. `Shared:NFS` : exclut de l'analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : exclut de l'analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : exclut de l'analyse toutes les ressources du système de fichiers de l'appareil partagées via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué.

Optimisation de la vérification des répertoires réseau

Pour optimiser la protection contre les menaces de fichiers, vous pouvez configurer l'exclusion de l'analyse des fichiers copiés des répertoires réseau vers un répertoire local. Pour ce faire, vous devez configurer une exclusion de processus pour un utilitaire conçu pour copier à partir de répertoires réseau (par exemple, pour l'utilitaire `cp`).

Pour configurer l'exclusion des répertoires réseau de l'analyse :

1. Affichez les paramètres de la tâche Protection contre les fichiers malicieux (*File_Threat_Protection*, ID:1) dans le fichier de configuration à l'aide de la commande :

   ```
   kesl-control --get-settings 1 --file < chemin d'accès complet au fichier de configuration > [--json]
   ```

2. Ouvrez le fichier de configuration et ajoutez une section `[ExcludedForProgram.item_#]` avec les paramètres suivants :

   - `ProgramPath` : chemin d'accès au processus à exclure ou au répertoire contenant des processus à exclure.
   - `ApplyToDescendants` – paramètre indiquant si les processus enfants du processus exclu doivent être exclus de l'analyse (valeurs possibles : `Yes` ou `No`).
   - `AreaDesc` : description de la zone d'exclusion en fonction des processus et qui contient des informations supplémentaires sur la zone d'exclusion.
   - `UseExcludedForProgram` : activer l'exclusion de la zone spécifiée lorsque la tâche est en cours d'exécution (valeurs possibles : `Yes` ou `No`).
   - `Path` : chemin d'accès au répertoire contenant des fichiers que le processus modifie.
   - `AreaMask.item_#` : masque de nom de fichier pour les fichiers à exclure de l'analyse. Vous pouvez également renseigner le chemin d'accès complet au fichier.

   Exemple :

   ```
   [ExcludedForProgram.item_0000]
   ProgramPath=/usr/bin/cp
   ApplyToDescendants=No
   AreaDesc=
   UseExcludedForProgram=Yes
   Path=AllRemoteMounted
   AreaMask.item_0000=*
   ```

3. Exécutez la commande :

   `kesl-control --set-settings 1 --file <chemin d'accès complet au fichier de configuration> [--json]`

   Spécifiez la clé `--json` si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

L'application n'analysera pas les fichiers dans les répertoires réseau, mais la commande `cp` (pour l'exemple cité ci-dessus) et les fichiers locaux seront quant à eux vérifiés.

Particularités de l'analyse des liens symboliques et matériels

L'application Kaspersky Endpoint Security permet d'analyser les liens symboliques et matériels vers les fichiers.

Analyse des liens symboliques

L'application analyse les liens symboliques uniquement si le fichier auquel se réfère le lien symbolique entre dans la zone d'analyse du module de protection contre les fichiers malicieux.

Si un fichier accessible via un lien symbolique n'est pas inclus dans la zone d'analyse du module Protection contre les fichiers malicieux, l'application n'analyse pas ce fichier. Toutefois, si un tel fichier contient un code malveillant, la sécurité de l'appareil est menacée.

Analyse des liens matériels

Lors du traitement d'un fichier comportant plusieurs liens physiques, l'application désinfecte le fichier d'origine. Si la désinfection échoue, l'application supprime le lien matériel et crée à la place une copie du fichier source portant le nom du lien matériel supprimé. Lors de la suppression, l'application supprime le lien physique en cours de traitement, les autres liens physiques vers ce fichier ne seront pas traités.

Quand vous restaurez un fichier avec un lien matériel depuis la sauvegarde, l'application crée la copie du fichier source portant le nom du lien matériel précédemment déplacé vers la sauvegarde. Les liens avec les autres liens matériels vers le fichier source ne sont pas restaurés.

Analyse des logiciels malveillants

Une *Analyse des logiciels malveillants* est une analyse unique, complète ou personnalisée des fichiers sur l'appareil à la demande. L'application Kaspersky Endpoint Security peut effectuer simultanément plusieurs tâches de recherche d'un logiciel malveillant.

L'application crée une tâche prédéfinie *Analyse des logiciels malveillants (Scan_My_Computer)*. Vous pouvez utiliser cette tâche pour effectuer une analyse complète de l'appareil. Dans le cadre de la vérification complète, l'application analyse tous les objets sur les disques locaux de l'appareil, ainsi que tous les objets montés et communs, accessibles via les protocoles Samba et NFS, selon les paramètres de sécurité recommandés.

Si un utilisateur disposant des privilèges root n'a pas accès à un fichier situé dans un répertoire distant monté sur l'appareil via le protocole NFSv4, l'application bloque l'accès à ce fichier pour tous les utilisateurs.

Dans Kaspersky Security Center, l'Assistant de configuration initiale de Kaspersky Security Center crée automatiquement une tâche de groupe pour rechercher les logiciels malveillants après l'installation du plug-in MMC d'administration ou du plug-in Web d'administration de Kaspersky Endpoint Security.

Pendant l'analyse complète du disque, le processeur est occupé. Il est recommandé d'exécuter la tâche de vérification complète lorsque l'entreprise est inactive.

Vous pouvez configurer les paramètres des tâches créées automatiquement dans Kaspersky Security Center et sur la ligne de commande, ainsi que créer des tâches d'analyse des logiciels malveillants définies par l'utilisateur.

Lorsqu'une application malveillante est détectée, Kaspersky Endpoint Security peut supprimer le fichier infecté et mettre fin au processus malveillant lancé à partir de ce fichier.

Si, lors de la Analyse des logiciels malveillants, l'application a été redémarrée par le service de contrôle ou manuellement par l'utilisateur, l'exécution de la tâche est interrompue. L'application consigne l'événement *OnDemandTaskInterrupted*.

Vous pouvez exécuter des tâches d'analyse des logiciels malveillants et configurer les paramètres d'analyse :

- Sélectionnez les objets du système d'exploitation qui doivent être analysés : fichiers, archives, secteurs de démarrage, mémoire de processus et mémoire du noyau, objets de démarrage.
- Limitez la taille de l'objet analysé et la durée de l'analyse de l'objet.
- Sélectionner les actions que l'application va exécuter sur les objets infectés.
- Configurez les exclusions des objets de l'analyse :
  - par des noms ou des masques ;
  - par les noms des menaces détectées dans les objets.

Sur les systèmes d'exploitation utilisant le système de fichiers parsecfs (Astra Linux Special Edition), il est recommandé d'ajouter les chemins de montage de ce système de fichiers aux exclusions d'analyse.

- Activer ou désactiver l'utilisation des exclusions globales et des exclusions de protection contre les fichiers malveillants lors de la vérification.
- Inclut un enregistrement de journal contenant des informations sur les objets analysés non infectés, sur les objets analysés dans les archives et sur les objets non traités.
- Configurer l'utilisation de l'analyseur heuristique et de la technologie iChecker pendant l'analyse.
- Limiter l'ensemble des appareils dont les secteurs de démarrage doivent être analysés.
- Configurer les zones d'analyse et les zones d'exclusion de l'analyse.

Analyse des logiciels malveillants dans Web Console

Dans Web Console, vous pouvez rechercher les logiciels malveillants à l'aide de la tâche *Analyse des logiciels malveillants*.

Vous pouvez lancer une tâche de groupe créée automatiquement, ainsi que créer et exécuter des tâches d'analyse personnalisées. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de la tâche d'analyse des logiciels malveillants.

Paramètres d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.

Paramètre	Description
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.
Zones d'analyse	Un tableau contenant les zones vérifiées par la tâche. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local. Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'analyse dans le tableau. Vous pouvez également importer une liste des zones d'analyse à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones d'analyse vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones d'analyse ou à ajouter des zones d'analyse à une liste existante.

Fenêtre d'ajout d'une zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau **Zones d'analyse** dans la section **Paramètres d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Cette liste déroulante permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
Protocole d'accès	Cette liste déroulante permet sélectionner le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après. La liste déroulante est accessible si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers.

Paramètre	Description
Chemin	Champ de saisie du chemin du répertoire à inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Ce champ est accessible si le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom de la ressource partagée	Champ de saisie du nom du partage du système de fichiers dans lequel se trouvent les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante **Protocole d'accès**.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Zones d'analyse

Vous pouvez configurer les paramètres d'une zone d'analyse pour la tâche Analyse des logiciels malveillants. L'application vous permet d'analyser les fichiers, les secteurs d'amorçage, la mémoire de l'appareil client et les objets de démarrage automatique.

Paramètres de la zone d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si la case est cochée, l'application analyse les fichiers. Si la case est décochée, l'application n'analyse pas les fichiers. La case est cochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si la case est cochée, l'application analyse les secteurs d'amorçage. Si cette case est décochée, l'application n'analyse pas les secteurs d'amorçage. La case est décochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil client. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, l'application ne vérifie pas les noyaux et les processus en cours d'exécution. La case est décochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si la case est cochée, l'application analyse les objets de démarrage. Si la case est décochée, l'application n'analyse pas les objets de démarrage. La case est décochée par défaut.
Appareils à analyser	Cliquez sur le lien **Configurer les masques d'appareil** pour ouvrir la fenêtre **Zone d'analyse**, où vous pouvez définir les appareils dont les secteurs de démarrage doivent être analysés.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Section Zones d'exclusion

Dans la section **Zones d'exclusion** pour la tâche Analyse des logiciels malveillants, vous pouvez configurer les zones d'exclusion, les exclusions par masque et par nom de menace, ainsi que l'utilisation d'exclusions globales et d'exclusions de la Protection contre les fichiers malicieux pendant l'exécution de la tâche.

Paramètres des exclusions de l'analyse

Paramètre	Description
Configurer des zones d'exclusion	Cliquez sur le lien **Configurer les zones d'exclusion** pour ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des exclusions de l'analyse.
Configurer les exclusions par masque	Cliquez sur le lien **Configurer les exclusions par masque** pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Configurer les exclusions par nom de menace	Cliquez sur le lien **Configurer les exclusions par nom de menace** pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Fenêtre d'ajout d'une zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse ou de la protection pendant son fonctionnement. Si la case est décochée, l'application inclut cette zone dans l'analyse ou dans la protection pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone de l'analyse ou de la protection après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	La liste déroulante permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'analyse : • **Local** : répertoires locaux. • **Monté** : les répertoires distants montés sur l'appareil. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
Protocole d'accès	Cette liste déroulante permet sélectionner le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après. La liste déroulante est accessible si vous avez choisi l'élément **Monté** dans la liste déroulante des systèmes de fichiers.

Paramètre	Description
Chemin	Champ de saisie du chemin du répertoire à inclure dans la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. Ce champ est accessible si le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers.
Nom de la ressource partagée	Champ de saisie du nom du partage du système de fichiers dans lequel se trouvent les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante **Protocole d'accès**.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ **Chemin**. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Nom de menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse des logiciels malveillants dans la Console d'administration

Dans la Console d'administration, vous pouvez rechercher les logiciels malveillants à l'aide de la tâche *Analyse des logiciels malveillants*.

Vous pouvez lancer une tâche de groupe créée automatiquement, ainsi que créer et exécuter des tâches d'analyse personnalisées. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de la tâche d'analyse des logiciels malveillants.

Dans la section **Paramètres** des propriétés de la tâche Analyse des logiciels malveillants, vous pouvez configurer les paramètres indiqués dans le tableau ci-dessous.

Paramètres d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse, des paramètres de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans la section **Exclusions** dans les propriétés de la tâche Analyse des logiciels malveillants, vous pouvez configurer les zones d'exclusion, les exclusions selon un masque et selon un nom de la menace.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre <Nouvelle zone d'analyse>

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Paramètres de la zone d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse pendant le fonctionnement de la tâche Analyse des logiciels malveillants. L'application vous permet d'analyser les fichiers, les secteurs d'amorçage, la mémoire de l'appareil et les objets de démarrage automatique.

Paramètres de la zone d'analyse

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si la case est cochée, l'application analyse les fichiers. Si la case est décochée, l'application n'analyse pas les fichiers. La case est cochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si la case est cochée, l'application analyse les secteurs d'amorçage. Si cette case est décochée, l'application n'analyse pas les secteurs d'amorçage. La case est décochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, l'application ne vérifie pas les noyaux et les processus en cours d'exécution. La case est décochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si la case est cochée, l'application analyse les objets de démarrage. Si la case est décochée, l'application n'analyse pas les objets de démarrage. La case est décochée par défaut.
Appareils à analyser	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce bouton pour ouvrir la fenêtre **Zones d'analyse**, dans laquelle vous pouvez spécifier les appareils dont les secteurs de démarrage doivent être analysés.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.

Paramètre	Description
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Une *exclusion de l'analyse* est un ensemble de conditions. Lorsque ces conditions sont réunies, Kaspersky Endpoint Security n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez également exclure des objets de l'analyse sur la base de masques et de noms de menaces.

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse des logiciels malveillants dans la ligne de commande

À partir de la ligne de commande, vous pouvez analyser des logiciels malveillants des manières suivantes :

- Utilisation de la tâche prédéfinie Analyse des logiciels malveillants (*Scan_My_Computer*). Vous pouvez démarrer, arrêter, suspendre et reprendre cette tâche manuellement et configurer la planification de son exécution. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

- Utilisation des tâches personnalisées d'analyse de logiciels malveillants (tâches de type *ODS*). Vous pouvez démarrer, arrêter, suspendre et reprendre les tâches d'utilisateur manuellement et configurer la planification de lancement de la tâche.

À l'aide de la commande `kesl-control --scan-file`, vous pouvez effectuer une *analyse personnalisée* des fichiers et des répertoires spécifiés.

Paramètres de la tâche prédéfinie Analyse des logiciels malveillants

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Analyse des logiciels malveillants.

Paramètres d'analyse de la tâche Analyse des logiciels malveillants

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fichiers. `No` : ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.

Paramètre	Description	Valeurs
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.

Paramètre	Description	Valeurs
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `< masque de nom d'appareil >` – analyser les secteurs d'amorçage des appareils dont les noms correspondent au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`. Exemple : `AreaDesc=" Mail bases scan "`
`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple : `AreaMask.item_< numéro d'élément >=*doc`

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Analyse personnalisée des fichiers et des répertoires dans la ligne de commande

Vous pouvez effectuer une analyse personnalisée des fichiers et des répertoires spécifiés à l'aide de la commande suivante : `kesl-control --scan-file`.

Une analyse personnalisée est effectuée avec les paramètres stockés dans la tâche prédéfinie *Scan_File* (ID:3). Vous pouvez configurer les paramètres d'analyse personnalisée des fichiers en modifiant les paramètres de cette tâche (voir le tableau ci-dessous).

Pour exécuter une analyse personnalisée des fichiers et répertoires spécifiés, exécutez la commande suivante :

```
kesl-control --scan-file <chemin d'accès> [--action <action>]
```

où :

- `<chemin>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

- `--action <action>` est l'action que l'application doit exécuter sur les objets infectés. Valeurs possibles : `DisinfectDeleteIfNotPossible, DisinfectInformIfNotPossible, Inform`. Si vous ne spécifiez pas la clé `--action`, l'application effectuera l'action `DisinfectDeleteIfNotPossible`.

À la suite de l'exécution de la commande, une tâche temporaire d'analyse des fichiers est créée, qui est automatiquement supprimée une fois terminée. Parallèlement, les résultats de l'analyse sont affichés dans la console.

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche *Scan_File*.

> Les sections `[ScanScope.item_#]` et `[ExcludedFromScanScope.item_#]` spécifiées dans la tâche *Scan_File* ne sont pas prises en compte lors de l'exécution d'une analyse personnalisée.

Paramètres de la tâche Scan_File

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fichiers. `No` : ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` : analyser les secteurs d'amorçage. `No` (valeur par défaut) — ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` — analyser la mémoire des processus et la mémoire du noyau. `No` (valeur par défaut) : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` : analyser les objets de démarrage. `No` (valeur par défaut) — ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.

Paramètre	Description	Valeurs
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.	La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.

Paramètre	Description	Valeurs
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `< masque de nom d'appareil >` – analyser les secteurs d'amorçage des appareils dont les noms correspondent au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`. Exemple : `AreaDesc=" Analyse des bases de messagerie "`
`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple : `AreaMask.item_< numéro d'élément >=*doc`

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Analyse des zones critiques

Lors de l'analyse des zones critiques, Kaspersky Endpoint Security peut analyser les secteurs de démarrage, les objets de démarrage, la mémoire des processus et la mémoire du noyau.

Lorsqu'une application malveillante est détectée, l'application peut supprimer le fichier infecté et mettre fin au processus malveillant lancé à partir de ce fichier.

Si un utilisateur disposant des privilèges root n'a pas accès à un fichier situé dans un répertoire distant monté sur l'appareil via le protocole NFSv4, l'application bloque l'accès à ce fichier pour tous les utilisateurs.

Vous pouvez exécuter une analyse des zones importantes et configurer les paramètres d'analyse :

- Sélectionnez les objets du système d'exploitation à analyser. Par défaut, l'analyse des secteurs de démarrage, de la mémoire de processus et de la mémoire du noyau, des objets de démarrage et des archives est activée. Les fichiers ne sont pas analysés par défaut lors de l'analyse des zones critiques.
- Limitez la taille de l'objet analysé et la durée de l'analyse de l'objet.
- Sélectionner les actions que l'application va exécuter sur les objets infectés.
- Configurez les exclusions des objets de l'analyse :
  - par des noms ou des masques ;
  - par les noms des menaces détectées dans les objets.

  Sur les systèmes d'exploitation utilisant le système de fichiers parsecfs (Astra Linux Special Edition), il est recommandé d'ajouter les chemins de montage de ce système de fichiers aux exclusions d'analyse.
- Activer ou désactiver l'utilisation des exclusions globales et des exclusions de protection contre les fichiers malveillants lors de la vérification.
- Inclut un enregistrement de journal contenant des informations sur les objets analysés non infectés, sur les objets analysés dans les archives et sur les objets non traités.
- Configurer l'utilisation de l'analyseur heuristique et de la technologie iChecker pendant l'analyse.
- Limiter l'ensemble des appareils dont les secteurs de démarrage doivent être analysés.
- Configurer les zones d'analyse et les zones d'exclusion de l'analyse.

Analyse des zones critiques dans Web Console

Dans Web Console, vous pouvez analyser les zones critiques du système d'exploitation de l'appareil protégé à l'aide de la tâche *Analyser les zones critiques*.

Vous pouvez créer et lancer les tâches d'analyse des zones critiques personnalisées. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Paramètres de la tâche d'analyse des zones critiques

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Notifier sur les fichiers non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.

Paramètre	Description
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Action en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.
Zones d'analyse	Un tableau contenant les zones vérifiées par la tâche. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local. Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'analyse dans le tableau. Vous pouvez également importer une liste des zones d'analyse à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones d'analyse vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones d'analyse ou à ajouter des zones d'analyse à une liste existante.

Fenêtre d'ajout d'une zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau **Zones d'analyse** dans la section **Paramètres d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Cette liste déroulante permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
Protocole d'accès	Cette liste déroulante permet sélectionner le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après. La liste déroulante est accessible si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers.

Paramètre	Description
Chemin	Champ de saisie du chemin du répertoire à inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Ce champ est accessible si le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom de la ressource partagée	Champ de saisie du nom du partage du système de fichiers dans lequel se trouvent les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante **Protocole d'accès**.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Zones d'analyse

Paramètres de la zone d'analyse de la tâche Analyse des zones critiques

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si la case est cochée, l'application analyse les fichiers. Si la case est décochée, l'application n'analyse pas les fichiers. La case est décochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si la case est cochée, l'application analyse les secteurs d'amorçage. Si cette case est décochée, l'application n'analyse pas les secteurs d'amorçage. La case est cochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil client. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, l'application ne vérifie pas les noyaux et les processus en cours d'exécution. La case est cochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si la case est cochée, l'application analyse les objets de démarrage. Si la case est décochée, l'application n'analyse pas les objets de démarrage. La case est cochée par défaut.
Appareils à analyser	Cliquez sur le lien **Configurer les masques d'appareil** pour ouvrir la fenêtre **Zone d'analyse**, où vous pouvez définir les appareils dont les secteurs de démarrage doivent être analysés.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Section Zones d'exclusion

Dans la section **Zones d'exclusion** de la tâche Analyse des zones critiques, vous pouvez configurer les zones d'exclusion , les exclusions par masque et par nom de menace , ainsi que l'utilisation d'exclusions globales et d'exclusions de protection contre les fichiers malveillants pendant l'exécution de la tâche.

Paramètres des exclusions de l'analyse

Paramètre	Description
Configurer des zones d'exclusion	Cliquez sur le lien **Configurer les zones d'exclusion** pour ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des exclusions de l'analyse.
Configurer les exclusions par masque	Cliquez sur le lien **Configurer les exclusions par masque** pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Configurer les exclusions par nom de menace	Cliquez sur le lien **Configurer les exclusions par nom de menace** pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.

Paramètre	Description
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Fenêtre d'ajout d'une zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse ou de la protection pendant son fonctionnement. Si la case est décochée, l'application inclut cette zone dans l'analyse ou dans la protection pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone de l'analyse ou de la protection après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	La liste déroulante permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'analyse : • **Local** : répertoires locaux. • **Monté** : les répertoires distants montés sur l'appareil. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
Protocole d'accès	Cette liste déroulante permet sélectionner le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après. La liste déroulante est accessible si vous avez choisi l'élément **Monté** dans la liste déroulante des systèmes de fichiers.

Paramètre	Description
Chemin	Champ de saisie du chemin du répertoire à inclure dans la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. Ce champ est accessible si le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers.
Nom de la ressource partagée	Champ de saisie du nom du partage du système de fichiers dans lequel se trouvent les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante **Protocole d'accès**.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ **Chemin**. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Nom de menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse des zones critiques dans la Console d'administration

Dans la Console d'administration, vous pouvez analyser les zones critiques du système d'exploitation de l'appareil protégé à l'aide de la tâche *Analyser les zones critiques*.

Vous pouvez créer et lancer les tâches d'analyse des zones critiques personnalisées. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Dans la section **Paramètres** des propriétés de la tâche Analyse des zones critiques, vous pouvez configurer les paramètres indiqués dans le tableau ci-dessous.

Paramètres de la tâche d'analyse des zones critiques

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse, des paramètres de la zone d'analyse et des paramètres d'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans la section **Exclusions** dans les propriétés de la tâche Analyse des zones critiques, vous pouvez configurer les zones d'exclusion, les exclusions selon un masque et selon un nom de la menace.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone d'analyse.

Paramètres de la zone d'analyse

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone d'analyse pendant son fonctionnement. Si cette case est décochée, l'application ne traite pas cette zone d'analyse pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** (valeur par défaut) : répertoires locaux. Si cet élément est sélectionné, vous devez spécifier le chemin d'accès à un répertoire local. • **Monté** : répertoires distants ou locaux montés. Si cet élément est sélectionné, vous devez spécifier le protocole ou le nom du système de fichiers. • **Partagé** affiche les ressources du système de fichiers du serveur protégé accessibles via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur protégé accessibles via les protocoles Samba et NFS.
	Si le type **Partagé** ou **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, alors vous pouvez sélectionner dans la liste déroulante de droite le protocole d'accès à distance : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local. Si le chemin n'est pas indiqué alors que le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers, l'application analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'analyse. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Paramètres de la zone d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse pendant le fonctionnement de la tâche Analyse des zones critiques. Lors de l'exécution de la tâche, l'application analyse les fichiers, les secteurs d'amorçage, les objets de démarrage automatique, la mémoire des processus et la mémoire du noyau.

Paramètres de la zone d'analyse

Paramètre	Description
Analyser les fichiers	La case active ou désactive l'analyse des fichiers. Si cette case est cochée, Kaspersky Endpoint Security analyse les fichiers. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les fichiers. La case est décochée par défaut.
Analyser les secteurs d'amorçage	La case active ou désactive l'analyse des secteurs d'amorçage. Si cette case est cochée, Kaspersky Endpoint Security analyse les secteurs de démarrage. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les secteurs de démarrage. La case est cochée par défaut.
Analyser la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire de l'appareil. Si la case est cochée, Kaspersky Endpoint Security vérifie la mémoire du noyau et les processus en cours d'exécution. Si la case est décochée, Kaspersky Endpoint Security ne vérifie pas la mémoire du noyau ni les processus en cours d'exécution. La case est cochée par défaut.
Analyser des objets de démarrage	La case active ou désactive l'analyse des objets de démarrage automatique. Si cette case est cochée, Kaspersky Endpoint Security analyse les objets de démarrage. Si cette case est décochée, Kaspersky Endpoint Security n'analyse pas les objets de démarrage automatique. La case est cochée par défaut.
Appareils à analyser	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce bouton pour ouvrir la fenêtre **Zones d'analyse**, dans laquelle vous pouvez spécifier les appareils dont les secteurs de démarrage doivent être analysés.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.
Utiliser les exclusions de la Protection contre les fichiers malicieux	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les fichiers malicieux pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exclusions du module Protection contre les fichiers malicieux. La case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des appareils, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom d'appareil **/**** (tous les appareils).

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètres d'analyse

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.

Paramètre	Description
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Une *exclusion de l'analyse* est un ensemble de conditions. Lorsque ces conditions sont réunies, Kaspersky Endpoint Security n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez également exclure des objets de l'analyse sur la base de masques et de noms de menaces.

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.

Paramètre	Description
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse des zones critiques via la ligne de commande

À partir de la ligne de commande, vous pouvez analyser les zones critiques du système d'exploitation de l'appareil protégé à l'aide de la tâche prédéfinie Analyser les zones critiques (*Critical_Areas_Scan*).

Vous pouvez démarrer, arrêter, suspendre et reprendre cette tâche manuellement et configurer la planification de son exécution. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

Paramètres de la tâche d'analyse des zones critiques

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` : analyse les fichiers. `No` (valeur par défaut) — Ne pas analyser les fichiers.
`ScanBootSectors`	Activation de l'analyse des secteurs d'amorçage.	`Yes` (valeur par défaut) : analyser les secteurs d'amorçage. `No` : ne pas analyser les secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la mémoire du noyau.	`Yes` (valeur par défaut) — Analyser la mémoire des processus et la mémoire du noyau. `No` : ne pas analyser la mémoire des processus et la mémoire du noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` (valeur par défaut) : analyser les objets de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.

Paramètre	Description	Valeurs
`UseExcludeMasks`	Activation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.
	Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`UseOASExclusions`	Activez l'utilisation des exclusions de la Protection contre les fichiers malicieux lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions de la Protection contre les fichiers malicieux. `No` : ne pas utiliser les exclusions de la Protection contre les fichiers malicieux.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.

Paramètre	Description	Valeurs
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.
`DeviceNameMasks.item_#`	Liste des noms d'appareils. L'application analysera les secteurs de démarrage de ces appareils. La valeur de réglage ne peut pas être vide. Pour exécuter la tâche, vous devez définir au moins un masque de nom de l'appareil.	`AllObjects` – vérifier les secteurs d'amorçage de tous les appareils. `< masque de nom d'appareil >` – Analyser les secteurs d'amorçage des appareils dont les noms correspondent au masque indiqué. Valeur par défaut : `/**` (tout ensemble de caractères dans le nom de l'appareil, y compris le caractère `/`).
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'analyse contient des informations complémentaires sur la zone d'analyse. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`. Exemple : `AreaDesc=" Mail bases scan "`
`UseScanArea`	Active l'analyse de la zone spécifiée. Pour exécuter la tâche, il faut inclure au moins une zone d'analyse.	`Yes` (valeur par défaut) : analyser la zone indiquée. `No` : n'analyse pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'analyse. Dans la zone d'analyse, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'analyse. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets). Exemple : `AreaMask.item_< numéro d'élément >=*doc`
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources du système de fichiers de l'appareil accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `AllShared` : analyse toutes les ressources du système de fichiers de l'appareil accessibles via les protocoles Samba et NFS. `<file system type>` – Analyser toutes les ressources de l'appareil du système de fichiers indiqué.
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de l'analyse contient des informations complémentaires sur la zone d'exclusion.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de l'analyse de la zone indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.

Paramètre	Description	Valeurs
`AreaMask.item_#`	Restriction de la zone d'exclusion de l'analyse. Dans la zone d'exclusion, l'application exclut uniquement les fichiers renseignés à l'aide de masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'exclusion. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<path to local directory>` – Exclure de l'analyse les objets du répertoire indiqué (y compris les sous-répertoires). Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Sur les systèmes avec un système de fichiers btrfs et des instantanés actifs activés, il est recommandé d'ajouter le chemin avec les instantanés montés en mode lecture seule aux exclusions afin d'optimiser les tâches de validation. Par exemple, sur les systèmes basés sur SUSE/OpenSUSE, vous pouvez ajouter une exclusion de type `/.snapshots/*/snapshot/`. Le chemin d'accès `/` est indiqué par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local. `Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole NFS. `Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur l'appareil via le protocole Samba. `AllRemoteMounted` : exclut de l'analyse tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS. `<file system type>` – Exclure de l'analyse toutes les ressources de l'appareil du système de fichiers indiqué. Les répertoires distants sont exclus de l'analyse par l'application uniquement s'ils ont été montés avant le lancement de la tâche. Les répertoires distants montés après le lancement de la tâche ne sont pas exclus de l'analyse.

Analyse des disques amovibles

Kaspersky Endpoint Security peut analyser les lecteurs amovibles suivants lorsqu'ils sont connectés à l'appareil protégé : lecteurs CD/DVD, lecteurs Blu-ray, lecteurs flash (y compris les modems USB), disques durs externes et disquettes.

Si l'analyse des lecteurs amovibles est activée, Kaspersky Endpoint Security surveille la connexion des lecteurs amovibles à l'appareil protégé et, lorsqu'un lecteur amovible connecté est détecté, analyse le lecteur et ses secteurs de démarrage à la recherche de virus et autres logiciels malveillants.

Par défaut, l'application ne contrôle pas la connexion des disques amovibles et ne les vérifie pas.

Configuration de l'analyse des disques amovibles dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'analyse des disques amovibles dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Analyse des disques amovibles**).

Configuration de l'analyse des disques amovibles dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de l'Analyse des disques amovibles dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Tâches locales** → **Analyse des disques amovibles**).

Paramètres du module Analyse des disques amovibles

Paramètre	Description
Activer l'analyse des disques amovibles à la connexion à l'appareil	La case active ou désactive l'analyse des disques amovibles lors de la connexion à l'appareil de l'utilisateur. La case est décochée par défaut.
Action à réaliser en cas de connexion d'un disque amovible	La liste déroulante permet de sélectionner l'action que l'application va exécuter en cas de connexion de disques amovibles à l'appareil de l'utilisateur : • **Ne pas analyser** les disques amovibles lors de la connexion (valeur par défaut). • L'**Analyse rapide** permet d'analyser les fichiers de **certains types** stockés sur des disques amovibles (à l'exclusion des lecteurs CD/DVD et des disques Blu-ray) et ne décompresse pas les objets composés. Une analyse rapide est effectuée avec les paramètres par défaut de la tâche *Analyse des zones critiques*. Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • L'option **Analyse détaillée** est destinée à l'analyse de tous les fichiers sur les disques amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray). Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Analyse des logiciels malveillants*.

Paramètre	Description
Action à réaliser en cas de connexion d'un lecteur CD / DVD	La liste déroulante permet de sélectionner l'action que l'application va exécuter en cas de connexion de lecteurs CD/DVD et de disques Blu-ray à l'appareil de l'utilisateur : • **Ne pas analyser** les lecteurs CD/DVD et les disques Blu-ray à la connexion (valeur par défaut). • **Analyse rapide** : analyser uniquement **certains types** de fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse rapide est effectuée avec les paramètres par défaut de la tâche *Analyse des zones critiques*. Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • L'option **Analyse complète** est destinée à l'analyse de tous les fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Analyse des logiciels malveillants*.
Bloquer l'accès au disque amovible pendant l'analyse	Cette case active ou désactive le blocage des fichiers à la connexion du disque lors de la tâche d'analyse. La case est décochée par défaut.

Configuration de l'Analyse des disques amovibles sur la ligne de commande

Sur la ligne de commande, vous pouvez gérer l'analyse des disques amovibles à l'aide de la tâche prédéfinie *Analyse des disques amovibles* (*Removable_Drives_Scan*).

Par défaut, la tâche *Analyse des disques amovibles* n'est pas démarrée. Vous pouvez démarrer et arrêter cette tâche manuellement. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.

Si la tâche est en cours d'exécution, l'application surveille la connexion des disques amovibles à l'appareil et, lorsque le disque amovible est connecté, crée et exécute une tâche temporaire d'analyse du secteur de démarrage (tâche de type *ODS*). Cette tâche ne peut pas être arrêtée. Une fois la tâche exécutée, l'application la supprime automatiquement.

Si vous avez activé l'analyse des fichiers dans les paramètres de la tâche *Analyse des disques amovibles*, l'application exécute également une ou plusieurs tâches temporaires d'analyse personnalisée des fichiers (tâches de type *ODS*). Si nécessaire, un utilisateur disposant de privilèges d'administrateur peut arrêter l'exécution de telles tâches.

Lors de la modification des paramètres de la tâche *Analyse des disques amovibles*, les nouvelles valeurs ne sont pas appliquées aux tâches temporaires déjà en cours d'exécution. Lorsque vous arrêtez la tâche *Analyse des disques amovibles*, les tâches temporaires déjà en cours d'exécution ne sont pas arrêtées.

Paramètres de tâche d'analyse des disques amovibles

Paramètre	Description	Valeurs
`ScanRemovableDrives`	Activation de l'analyse des disques amovibles lors de la connexion à l'appareil. Cette option n'est pas appliquée aux lecteurs CD/DVD et aux disques Blu-ray (cf. le paramètre `ScanOpticalDrives`).	`DetailedScan` : analyse tous les fichiers sur les disques amovibles (à l'exception des lecteurs CD/DVD et des disques Blu-ray). Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Scan_File* (ID:3). `QuickScan` : analyser uniquement **certains types** de fichiers sur les lecteurs amovibles (à l'exclusion des lecteurs CD/DVD et des disques Blu-ray). Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. L'analyse rapide est effectuée avec les paramètres par défaut de la tâche *Critical_Areas_Scan* (ID:4). `NoScan` (valeur par défaut) : n'analyse pas les disques amovibles lors de la connexion.

Paramètre	Description	Valeurs
`ScanOpticalDrives`	Activation de l'analyse des lecteurs CD/DVD et des disques Blu-ray lors de la connexion à l'appareil.	`DetailedScan` : analyse tous les fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Une analyse détaillée est effectuée avec les paramètres par défaut de la tâche *Scan_File* (ID:3). `QuickScan` : analyser uniquement **certains types** de fichiers sur les lecteurs CD/DVD et les disques Blu-ray. Les formats de fichiers suivants sont analysés sur les lecteurs amovibles : com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. L'analyse rapide est effectuée avec les paramètres par défaut de la tâche *Critical_Areas_Scan* (ID:4). `NoScan` (valeur par défaut) : n'analyse pas les lecteurs CD/DVD et les disques Blu-ray à la connexion.
`BlockDuringScan`	Activation du blocage des fichiers à la connexion du disque lors de l'analyse. Lors de l'analyse des secteurs de démarrage, les fichiers ne sont pas bloqués.	`Yes` : bloque les fichiers pendant l'analyse. `No` (valeur par défaut) : ne bloque pas les fichiers pendant l'analyse.

Analyser les conteneurs.

Vous pouvez analyser les conteneurs et les images à la recherche de logiciels malveillants en temps réel et à la demande :

- Le *module Surveillance des conteneurs (Analyse du conteneur, Surveillance des conteneurs)* permet d'analyser en temps réel les conteneurs en cours de démarrage et les espaces de noms.
- À l'aide des tâches *Analyse du conteneur*, vous pouvez analyser des conteneurs et des images à la demande.

Pour utiliser les fonctionnalités d'analyse du conteneur, vous avez besoin d'une licence incluant cette fonctionnalité.

L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc.

L'intégration avec le système d'administration par les conteneurs Docker version 28.5.2 et antérieures est prise en charge.

Surveillance des conteneurs

Par défaut, le module Surveillance du conteneur est activé. L'application vérifie les conteneurs et les espaces de noms en cours d'exécution en temps réel.

Pour que le module Surveillance du conteneur fonctionne, le module Protection contre les fichiers malicieux doit être activé. Les paramètres du module Protection contre les fichiers malicieux sont appliqués lors de l'analyse des conteneurs et des espaces de noms.

L'application ne vérifie pas les espaces de noms et les conteneurs à moins que les modules permettant de travailler avec les conteneurs et les espaces de noms ne soient installés sur le système d'exploitation. Dans ce cas, l'état du module pour Surveillance du conteneur sur la ligne de commande s'affiche sous la forme `La tâche est disponible et n'est pas en cours d'exécution`, tandis que dans Kaspersky Security Center, il s'affiche comme « `Arrêtée` ».

Vous pouvez activer ou désactiver le module Surveillance du conteneur, ainsi que configurer les paramètres d'analyse du conteneur et des espaces de noms en temps réel :

- Sélectionner l'action que l'application effectuera sur le conteneur lorsqu'un objet infecté est détecté.

  Cette option est disponible lors de l'utilisation de l'application sous une licence qui active cette fonctionnalité.

- Configurer l'intégration de l'application Kaspersky Endpoint Security avec le système d'administration des conteneurs Docker, de l'environnement CRI-O, des utilitaires Podman et runc.

  L'intégration avec le système d'administration par les conteneurs Docker version 28.5.2 et antérieures est prise en charge.

Configuration de la surveillance des conteneurs dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'analyse du conteneur dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres d'analyse du conteneur**).

Configuration de la surveillance des conteneurs dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de traçage de l'application dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres d'analyse du conteneur**).

Paramètres de surveillance des conteneurs

Paramètre	Description
Activer la surveillance des espaces de noms et des conteneurs	La case active ou désactive la vérification en temps réel des espaces des noms et des conteneurs. La case est cochée par défaut.
Action sur le conteneur en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur le conteneur en cas de détection d'un objet infecté lors de l'analyse : • L'option **Ignorer le conteneur** signifie que l'application n'effectue aucune action sur le conteneur lorsqu'un objet infecté est détecté. • L'option **Arrêter le conteneur** signifie que l'application arrête le conteneur suite à la détection d'un objet infecté. • **Arrêter en cas d'échec de la désinfection** (valeur par défaut) : l'application arrête le conteneur si la désinfection d'un objet infecté a échoué. Cette option est disponible lors de l'utilisation de l'application sous une licence qui active cette fonctionnalité.
Paramètres d'analyse de conteneur	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre Paramètres d'analyse des conteneurs.

Fenêtre Paramètres d'analyse de conteneur

Dans cette fenêtre, vous pouvez configurer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec le système d'administration des conteneurs Docker, de l'environnement CRI-O et des utilitaires Podman et runc.

Paramètre	Description
Utiliser Docker	Cette case active ou désactive l'utilisation du système d'administration des conteneurs Docker. La case est cochée par défaut. L'utilisation du système d'administration par les conteneurs Docker version 28.5.2 et antérieures est prise en charge.
Chemin du socket de Docker	Champ de saisie du chemin d'accès ou URI (ID universel de ressource) du socket de Docker. Valeur par défaut : /var/run/docker.sock.
Utiliser CRI-O	La case permet d'activer ou de désactiver l'utilisation de l'environnement CRI-O. La case est cochée par défaut.
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier de configuration CRI-O. Valeur par défaut : /etc/crio/crio.conf.
Utiliser Podman	La case permet d'activer ou de désactiver l'utilisation de l'utilitaire Podman. La case est cochée par défaut.
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier exécutable de l'utilitaire Podman. Valeur par défaut : /usr/bin/podman.
Dossier racine	Champ de saisie du chemin d'accès au dossier racine du stockage de conteneurs. Valeur par défaut : /var/lib/containers/storage
Utiliser runc	La case permet d'activer ou de désactiver l'utilisation de l'utilitaire runc. La case est cochée par défaut.
Chemin d'accès au fichier.	Champ de saisie du chemin d'accès au fichier exécutable de l'utilitaire runc. Valeur par défaut : /usr/bin/runc.
Dossier racine	Champ de saisie du chemin d'accès au dossier racine du stockage de l'état des conteneurs. Valeur par défaut : /run/runc.

Configurer la surveillance des conteneurs dans la ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver la surveillance en temps réel des espaces de noms et des conteneurs à l'aide de l'option `NamespaceMonitoring=Yes/No` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre `NamespaceMonitoring` à l'aide du fichier de configuration, qui contient tous les paramètres généraux de l'application, ou à l'aide des clés de la ligne de commande.

La vérification en temps réel des espaces de noms et des conteneurs utilise les paramètres généraux d'analyse du conteneur. Vous pouvez afficher et modifier ces paramètres à l'aide des commandes spéciales de gestion de Kaspersky Endpoint Security :

- Vous pouvez afficher les valeurs actuelles des paramètres généraux de l'analyse du conteneur sur la console ou dans un fichier de configuration. Vous pouvez utiliser ce fichier pour modifier les paramètres.
- Vous pouvez modifier tous les paramètres généraux de l'analyse du conteneur à l'aide du fichier de configuration contenant les paramètres. Vous pouvez obtenir le fichier de configuration à l'aide de la commande pour afficher les paramètres généraux de l'analyse du conteneur.
- Vous pouvez modifier des paramètres individuels à l'aide d'options de ligne de commande au format `< nom du paramètre >=< valeur du paramètre >`. Vous pouvez obtenir les valeurs actuelles des paramètres à l'aide de la commande pour afficher les paramètres généraux de l'analyse du conteneur.

Pour afficher les valeurs actuelles des paramètres généraux de l'analyse du conteneur sur la console, exécutez la commande suivante :

```
kesl-control --get-container-settings [--json]
```

où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les valeurs actuelles des paramètres généraux de l'analyse du conteneur dans un fichier, exécutez la commande suivante :

```
kesl-control --get-container-settings --file < chemin d'accès au fichier de configuration > [--json]
```

où :

- `--file < chemin d'accès au fichier de configuration >` est le chemin d'accès au fichier dans lequel les paramètres généraux d'analyse du conteneur seront enregistrés. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour modifier les valeurs des paramètres généraux de l'analyse du conteneur à l'aide d'un fichier de configuration :

1. Générez les paramètres généraux de l'analyse du conteneur dans le fichier de configuration comme décrit ci-dessus.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande :

   ```
   kesl-control --set-container-settings --file < chemin d'accès au fichier de configuration > [--json]
   ```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux d'analyse du conteneur.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres généraux de l'analyse du conteneur spécifiées dans le fichier seront importées dans l'application.

Pour modifier les valeurs des options générales de l'analyse du conteneur à l'aide des commutateurs de ligne de commande, exécutez la commande suivante :

```
kesl-control --set-container-settings <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

où `<nom du paramètre>=<valeur du paramètre>` correspond au nom et à la valeur de l'un des paramètres généraux d'analyse du conteneur.

Les valeurs des paramètres généraux de l'analyse du conteneur spécifiés seront modifiées.

Analyse à la demande du conteneur et des images

Lors de l'exécution de la tâche *Analyse du conteneur*, Kaspersky Endpoint Security analyse les conteneurs et les images à la recherche de virus et autres logiciels malveillants. Une application peut effectuer simultanément plusieurs tâches d'analyse du conteneur.

Pour utiliser la tâche Analyse du conteneur, vous avez besoin d'une licence incluant cette fonctionnalité.

L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc.

L'intégration avec le système d'administration par les conteneurs Docker version 28.5.2 et antérieures est prise en charge.

Vous pouvez exécuter une analyse du conteneur et configurer les paramètres de l'analyse :

- Spécifiez les conteneurs et les images à analyser par nom ou masque de nom.
- Activer la vérification de tous les calques et conteneurs d'images.
- Sélectionnez l'action que l'application effectuera sur le conteneur et l'action que l'application effectuera sur l'image lorsqu'un objet infecté est détecté.

- Configurez les paramètres d'analyse des objets à l'intérieur de conteneurs ou d'images :
  - Activer ou désactiver l'analyse des archives, des bases de données de messagerie et des messages électroniques au format texte.
  - Limitez la taille de l'objet analysé et la durée de l'analyse de l'objet.
  - Sélectionner les actions que l'application va exécuter sur les objets infectés.
  - Configurez les exclusions des objets de l'analyse :
    - par des noms ou des masques ;
    - par les noms des menaces détectées dans les objets.
  - Activer ou désactiver l'utilisation des exclusions globales lors de la vérification.
  - Configurer l'utilisation de l'analyseur heuristique et de la technologie iChecker pendant l'analyse.
  - Activer ou désactiver l'enregistrement dans le journal des informations sur les objets non infectés analysés, sur l'analyse des objets dans les archives et sur les objets non traités.

Analyse du conteneur dans Web Console

Dans Web Console, vous pouvez valider les conteneurs et les images à l'aide de la tâche *Analyse du conteneur*.

Vous pouvez créer et lancer des tâches d'analyse définies par l'utilisateur du conteneur. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.

Paramètre	Description
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.
Analyser les conteneurs	La case active ou désactive l'analyse du conteneur. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les conteneurs à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les conteneurs à analyser. Par défaut, le masque * est utilisé (tous les conteneurs seront analysés).

Paramètre	Description
Action en cas de détection d'une menace	Vous pouvez sélectionner une action que l'application exécutera sur l'image en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer le conteneur** pour n'effectuer aucune action sur le conteneur lorsqu'un objet infecté a été détecté. • **Arrêter le conteneur** : arrête le conteneur à la suite de la détection d'un objet infecté. • **Arrêter en cas d'échec de la désinfection** (valeur par défaut) : arrêter le conteneur si l'objet infecté n'a pas pu être désinfecté ou si la menace n'a pas pu être éliminée. En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action **Arrêter le conteneur**.
Analyser les images	La case active ou désactive l'analyse des images. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les images à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les images à analyser. Par défaut, le masque * est utilisé (toutes les images seront analysées).
Action en cas de détection d'une menace	Vous pouvez sélectionner une action que l'application exécutera sur l'image en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer l'image** (valeur par défaut) : n'effectue aucune action sur l'image lorsqu'un objet infecté a été détecté. • **Supprimer l'image** lorsqu'un objet infecté a été détecté (déconseillé). Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.
Analyser chaque couche	Cette case active ou désactive l'analyse de toutes les couches des images et des conteneurs lancés. La case est décochée par défaut.

Section Zones d'exclusion

Dans la section **Zones d'exclusion** pour la tâche Analyse du conteneur, vous pouvez configurer les exclusions par masque et par nom de menace, ainsi que l'utilisation des exclusions globales pendant l'exécution de la tâche.

Paramètres des exclusions de l'analyse

Paramètre	Description
Configurer les exclusions par masque	Cliquez sur le lien **Configurer les exclusions par masque** pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Configurer les exclusions par nom de menace	Cliquez sur le lien **Configurer les exclusions par nom de menace** pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Cliquez sur le bouton **Ajouter** ou **Modifier** pour ouvrir la fenêtre **Nom de menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse du conteneur dans la Console d'administration

Dans la Console d'administration, vous pouvez analyser du conteneur et les images à l'aide de la tâche *Analyse du conteneur*.

Vous pouvez créer et lancer des tâches d'analyse définies par l'utilisateur du conteneur. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Dans la section **Paramètres** des propriétés de la tâche Analyse du conteneur, vous pouvez configurer les paramètres indiqués dans le tableau ci-dessous.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration des paramètres d'analyse du conteneur et des paramètres généraux de l'analyse.
Actions en cas de détection d'une menace	Ce groupe de paramètres contient le bouton **Configurer**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Action lors de la détection d'une menace**, dans laquelle vous pouvez configurer les actions que l'application effectue sur les objets infectés détectés.

Dans la section **Exclusions** dans les propriétés de la tâche Analyse du conteneur, vous pouvez également configurer des exclusions par masque et par nom de la menace.

Fenêtre Paramètres d'analyse de conteneur

Cette fenêtre permet de configurer les paramètres d'analyse du conteneur et des images.

Paramètres d'analyse du conteneur et des images

Paramètre	Description
Analyser les conteneurs	La case active ou désactive l'analyse du conteneur. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les conteneurs à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les conteneurs à analyser. Par défaut, le masque * est utilisé (tous les conteneurs seront analysés).
Action en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur le conteneur en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer le conteneur** pour n'effectuer aucune action sur le conteneur lorsqu'un objet infecté a été détecté. • **Arrêter le conteneur** : arrête le conteneur à la suite de la détection d'un objet infecté. • **Arrêter en cas d'échec de la désinfection** (valeur par défaut) : arrêter le conteneur si l'objet infecté n'a pas pu être désinfecté ou si la menace n'a pas pu être éliminée. En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action **Arrêter le conteneur**.
Analyser les images	La case active ou désactive l'analyse des images. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les images à analyser. La case est cochée par défaut.
Masque de nom	Champ de saisie pour un nom ou un masque définissant les images à analyser. Par défaut, le masque * est utilisé (toutes les images seront analysées).
Action en cas de détection d'une menace	La liste déroulante permet de sélectionner une action que l'application exécutera sur l'image en cas de détection d'un objet infecté lors de l'analyse : • **Ignorer l'image** (valeur par défaut) : n'effectue aucune action sur l'image lorsqu'un objet infecté a été détecté. • **Supprimer l'image** lorsqu'un objet infecté a été détecté (déconseillé). Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.
Analyser chaque couche	Cette case active ou désactive l'analyse de toutes les couches des images et des conteneurs lancés. La case est décochée par défaut.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement de la tâche.

Paramètres d'analyse

Paramètre	Description
Analyser les archives	La case active ou désactive l'analyse des archives. Si la case est cochée, l'application analyse les archives. Pour analyser une archive, l'application doit d'abord la décompresser, ce qui peut ralentir l'analyse. Vous pouvez réduire la durée d'analyse des archives en configurant les paramètres **Ignorer un fichier si son analyse prend plus de (secondes)** et **Ignorer un fichier si sa taille est supérieure à (Mo)** dans le groupe **Paramètres généraux d'analyse**. Si la case est décochée, l'application n'analyse pas les archives. La case est cochée par défaut.

Paramètre	Description
Analyser les archives autoextractibles	Cette case active ou désactive l'analyse des *archives autoextractibles*. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Si la case est cochée, l'application analyse les archives autoextractibles. Si la case est décochée, l'application n'analyse pas les archives autoextractibles. La case est disponible si la case **Analyser les archives** est décochée. La case est cochée par défaut.
Analyser les bases de messagerie	Cette case active ou désactive l'analyse des bases de messagerie des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie. Si la case est cochée, l'application analyse les fichiers des bases de messagerie. Si la case est décochée, l'application n'analyse pas les fichiers des bases de messagerie. La case est décochée par défaut.
Analyser les fichiers au format de messagerie	Cette case active ou désactive l'analyse des fichiers des messages électroniques au format texte brut. Si cette case est cochée, l'application analyse les messages au format texte brut. Si cette case est décochée, l'application n'analyse pas les messages au format texte brut. La case est décochée par défaut.
Ignorer un fichier si son analyse prend plus de (secondes)	Champ dans lequel vous devez indiquer la durée maximale de l'analyse d'un fichier en secondes. Une fois le délai indiqué écoulé, l'application interrompt l'analyse du fichier. Valeurs admises : 0 à 9999. Si la valeur est définie sur 0, la durée d'analyse est illimitée. Valeur par défaut : 0.
Ignorer un fichier si sa taille est supérieure à (Mo)	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en mégaoctets. Valeurs admises : 0 à 999999. Si la valeur est définie sur 0, l'application analyse les fichiers de n'importe quelle taille. Valeur par défaut : 0.
Journaliser les objets non infectés	Cette case active ou désactive l'enregistrement des événements de type *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. Si cette case n'est pas cochée, l'application n'enregistre pas les événements de type *ObjectProcessed* dans le journal pour tout objet analysé. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements de type *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre les événements de type *ObjectNotProcessed* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *ObjectNotProcessed* dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements de type *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre les événements de type *PackedObjectDetected* dans le journal. Si cette case est décochée, l'application n'enregistre pas les événements de type *PackedObjectDetected* dans le journal. La case est décochée par défaut.
Utiliser la technologie iChecker	Cette case active ou désactive l'analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse. Si la case est cochée, l'application analyse seulement les nouveaux fichiers ou les fichiers modifiés depuis la dernière analyse. Si cette case est décochée, l'application analyse les fichiers sans tenir compte de la date de création et de modification. La case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse des fichiers. La case est cochée par défaut.

Paramètre	Description
Niveau de l'analyse heuristique	Si la case **Utiliser l'analyse heuristique** est cochée, vous pouvez sélectionner le niveau de l'analyse heuristique dans la liste déroulante : • **Faible** est le niveau d'analyse le moins détaillé, avec une charge système minimale. • **Normal** est le niveau d'analyse normale, avec une charge système équilibrée. • **Élevé** est le niveau d'analyse le plus détaillé, avec une charge système maximale. • **Recommandé** (valeur par défaut) : niveau optimal recommandé par les spécialistes de Kaspersky. Il assure une combinaison optimale de la qualité de la protection et du degré d'influence sur les performances des appareils protégés.

Fenêtre Actions en cas de détection d'une menace

Cette fenêtre permet de configurer les actions que Kaspersky Endpoint Security exécutera sur l'objet infecté détecté :

Actions en cas de détection d'une menace

Paramètre	Description
Actions en cas de détection d'une menace	Vous pouvez sélectionner les actions que l'application effectuera sur l'objet infecté détecté : • **Désinfecter ; supprimer si la désinfection est impossible** (valeur par défaut). Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. • **Désinfecter ; informer si la désinfection est impossible**. Lorsque vous sélectionnez cette action, l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. • **Informer**. Lorsque vous sélectionnez cette action, l'application enregistre les informations sur l'objet infecté dans le journal.

Section Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.
Exclusions d'après le nom de la menace	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le nom de la menace**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base du nom de la menace.
Utiliser des exclusions globales	La case à cocher active ou désactive l'exclusion des points de montage spécifiés dans les exclusions globales pendant l'exécution de l'application. Si cette case est cochée, l'application exclut les points de montage configurés de l'analyse. La case est cochée par défaut.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Fenêtre Exclusions d'après le nom de la menace

Vous pouvez configurer l'exclusion des objets de l'analyse, en fonction d'un nom de menace. L'application ne bloquera pas les menaces spécifiées. Par défaut, la liste des noms de menaces est vide.

Vous pouvez ajouter, modifier et supprimer les noms de menaces.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Analyse du conteneur sur la ligne de commande

À partir de la ligne de commande, vous pouvez analyser les conteneurs et les images des manières suivantes :

- Utilisation de la tâche prédéfinie Analyse du conteneur (*Container_Scan*). Vous pouvez démarrer et arrêter cette tâche et configurer la planification de son exécution. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.
- Utilisation des tâches personnalisées de l'analyse du conteneur (tâches de type *ContainerScan*). Vous pouvez démarrer et arrêter des tâches personnalisées manuellement et configurer des planifications de lancement de tâches.
- À l'aide de la commande `kesl-control --scan-container`, vous pouvez effectuer une *analyse personnalisée* des conteneurs et images spécifiés.

Paramètres de la tâche Analyse du conteneur

Toutes les valeurs disponibles et les valeurs par défaut pour chaque paramètre d'analyse du conteneur et des images sont décrites dans le tableau.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description	Valeurs
`ScanContainers`	Analyse des conteneurs spécifiés par un masque Vous pouvez définir les masques à l'aide du paramètre `ContainerNameMask`.	`Yes` (valeur par défaut) : analyse les conteneurs définis par masque. `No` : n'analyse pas les conteneurs définis par masque.

`ContainerNameMask`	Nom ou un masque de nom qui définit un conteneur à analyser.
	Les masques sont définis dans le format de l'interpréteur de commandes. Vous pouvez utiliser les caractères ? et *.
	Avant de définir ce paramètre, assurez-vous que la valeur du paramètre `ScanContainers=Yes`.
		Valeur par défaut : * (analyser tous les conteneurs).
		Exemples :
		Analysez un conteneur avec le nom my_container :
		`ContainerNameMask=my_container`
		Analysez tous les conteneurs dont les noms commencent par my_container :
		`ContainerNameMask=my_container*`
		Analysez tous les conteneurs dont les noms commencent par my_, puis contiennent cinq caractères, puis _container et se terminent par une séquence de caractères :
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Analyse des images spécifiées par un masque Vous pouvez définir les masques à l'aide du paramètre `ImageNameMask`.	`Yes` (valeur par défaut) : analyse les images définies par masque. `No` : n'analyse pas les images définies par masque.

`ImageNameMask`	Spécifie un nom ou un masque de nom qui définit les images à analyser.
	Avant de définir ce paramètre, assurez-vous que le paramètre `ScanImages` possède la valeur `Yes`.
	Les masques sont définis dans le format de l'interpréteur de commandes.
	Si vous souhaitez définir plusieurs masques, chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.
		Valeur par défaut : * (analyser tous les modèles).
		Exemples :
		Analysez une image avec le nom my_image et la valeur de tag latest :
		`ImageNameMask=my_image:latest`
		Analysez toutes les images dont les noms commencent par my_image_ et avec n'importe quelle valeur de tag :
		`ImageNameMask=my_image*`

`DeepScan`	Analyse de toutes les couches des images et des conteneurs lancés.	`Yes` : analyse toutes les couches. `No` (valeur par défaut) : n'analyse pas toutes les couches.
`ContainerScanAction`	Spécifie l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté. Les actions sur un objet infecté à l'intérieur du conteneur sont décrites ci-dessous.	`StopContainerIfFailed` (valeur par défaut) : l'application arrête le conteneur si elle ne parvient pas à désinfecter ou à supprimer l'objet infecté. Lorsque cette valeur est sélectionnée, l'action effectuée sur le conteneur dépend également de la valeur spécifiée du paramètre `ActionOnThreat`, qui s'applique aux objets à l'intérieur des conteneurs et des images (voir le tableau ci-dessous). Si le paramètre `ActionOnThreat` est défini sur `DisinfectDeleteIfNotPossible` et que l'application ne parvient pas à désinfecter ou à supprimer l'objet infecté lors de l'exécution de l'action, le conteneur sera arrêté. En raison du fonctionnement de l'environnement CRI-O, l'objet infecté n'est ni désinfecté ni supprimé dans le conteneur de l'environnement CRI-O. Il est recommandé de sélectionner l'action `StopContainer`. `StopContainer` : l'application arrête le conteneur lorsqu'un objet infecté est détecté. `Skip` : l'application n'effectue aucune action sur les conteneurs lorsqu'un objet infecté est détecté.
`ImageAction`	Spécifie l'action à effectuer sur une image lorsqu'un objet infecté est détecté. Les actions sur un objet infecté à l'intérieur de l'image sont décrites ci-dessous.	`Skip` (valeur par défaut) : l'application n'effectue aucune action sur l'image lorsqu'un objet infecté est détecté. `Delete` : l'application supprime l'image lorsqu'un objet infecté est détecté (non recommandé). Toutes les dépendances seront également supprimées. Les conteneurs en exécution seront arrêtés, puis supprimés.

Les paramètres décrits ci-dessous sont appliqués aux objets à l'intérieur des conteneurs et des images.

Paramètres de la tâche Analyse du conteneur

Paramètre	Description	Valeurs
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX). L'application analyse les archives telles que : .zip ; .7z* ; .7-z ; .rar ; .iso ; .cab ; .jar ; .bz ; .bz2 ; .tbz ; .tbz2 ; .gz ; .tgz ; .arj. La liste des formats d'archive pris en charge dépend des bases de données de l'application utilisées.	`Yes` (valeur par défaut) : analyse les archives. Si la valeur `DisinfectDeleteIfNotPossible` est spécifiée pour le paramètre `ActionOnThreat`, et si la désinfection n'est pas possible, alors, selon le type d'archive, l'application supprime soit l'objet infecté, soit l'archive entière contenant la menace. `No` : n'analyse pas les archives.
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) — analyser les archives autoextractibles. `No` : n'analyse pas les archives autoextractibles.
`ScanMailBases`	Activation de l'analyse des bases de données email des applications Microsoft Outlook, Outlook Express, The Bat! et autres clients de messagerie.	`Yes` : analyse les fichiers des bases de données email. `No` (valeur par défaut) : n'analyse pas les fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniques au format texte. `No` (valeur par défaut) : n'analyse pas les messages électroniques au format texte.
`TimeLimit`	Durée maximale d'analyse de l'objet (en secondes). L'application interrompt l'analyse de l'objet si sa durée dépasse la valeur définie pour ce paramètre.	0 – 9999 0 : la durée de l'analyse des objets n'est pas limitée. Valeur par défaut : 0.
`SizeLimit`	Taille maximale d'une archive à analyser (en mégaoctets). Si la taille de l'objet à analyser dépasse la valeur spécifiée, l'application ignore l'objet pendant l'analyse.	0 – 999999 0 : l'application analyse les objets de n'importe quelle taille. Valeur par défaut : 0.
`ActionOnThreat`	Sélection d'une action que l'application va exécuter sur les objets infectés.	`DisinfectDeleteIfNotPossible` (désinfecter ; supprimer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection échoue, par exemple, le type de l'objet ou le type de la menace dans l'objet ne peut pas être désinfecté, l'application supprime l'objet infecté. `DisinfectInformIfNotPossible` (désinfecter ; informer si la réparation est impossible) : l'application tente de désinfecter l'objet infecté en enregistrant une copie de l'objet dans la sauvegarde. Si la désinfection n'est pas possible (par exemple, le type d'objet ou le type de menace dans l'objet ne permet pas le traitement), l'application enregistre des informations à ce sujet dans le journal. `Inform` (informer) : l'application ne tente pas de désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Utilisation de l'exclusion de l'analyse des objets définis à l'aide du paramètre `ExcludeMasks.item_#`.	`Yes` : exclut de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le paramètre `ExcludeMasks.item_#`.

`ExcludeMasks.item_#`	Exclusion de l'analyse des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell.	La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

Paramètre	Description	Valeurs
`UseExcludeThreats`	Utilisation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets contenant les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les menaces désignées par le paramètre `ExcludeThreats.item_#`.

`ExcludeThreats.item_#`	Exclusion de l'analyse des objets en fonction des noms des menaces détectées dans ceux-ci. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeThreats` est activé.
	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet.
	Par exemple, vous utilisez un utilitaire pour collecter des informations sur votre réseau. Pour que l'application ne le bloque pas, ajoutez le nom complet de la menace qu'il comporte à la liste des menaces exclues de l'analyse.
	Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exclusions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser des exclusions globales. `No` : ne pas utiliser les exclusions globales.
`ReportCleanObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés que l'application a considéré comme non infecté. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet quelconque a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives aux objets non infectés. `No` (valeur par défaut) : n'enregistre pas les informations relatives aux objets non infectés dans le journal.
`ReportPackedObjects`	Activation de l'enregistrement dans le journal des informations relatives aux objets analysés qui font partie d'objets composés. Vous pouvez activer ce paramètre par exemple pour confirmer qu'un objet qui se trouve dans une archive a bien été analysé par l'application.	`Yes` : enregistre dans le journal les informations relatives à l'analyse des objets des archives. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives à l'analyse des objets des archives.
`ReportUnprocessedObjects`	Activation de la consignation dans le journal des informations relatives aux objets qui n'ont pas été traités pour une raison quelconque.	`Yes` : enregistre dans le journal les informations relatives aux objets non traités. `No` (valeur par défaut) : n'enregistre pas dans le journal les informations relatives aux objets non traités.
`UseAnalyzer`	Activation de l'analyse heuristique. Grâce à l'analyse heuristique, l'application peut détecter les nouvelles menaces avant leur détection par les analystes antivirus.	`Yes` (valeur par défaut) : active l'analyse heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique. Vous pouvez définir le niveau de l'analyse heuristique. Celui-ci définit l'équilibre entre la minutie de la recherche des menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse heuristique est élevé, plus le volume de ressources et le temps consacrés à l'analyse augmentent.	`Light` : analyse la moins minutieuse avec une charge minimale sur le système. `Medium` : niveau de l'analyse heuristique normal avec une charge équilibrée sur le système d'exploitation. `Deep` : analyse la plus minutieuse avec une charge maximale sur le système d'exploitation. `Recommended` (valeur par défaut) : valeur recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisation de la technologie iChecker. `No` : désactive l'utilisation de la technologie iChecker.

Analyse personnalisée du conteneur et des images

Vous pouvez effectuer une analyse personnalisée des conteneurs et des images indiqués à l'aide de la commande `kesl-control --scan-container`.

Une analyse personnalisée est effectuée avec les paramètres stockés dans la tâche prédéfinie *Custom_Container_Scan* (ID:19). Vous pouvez configurer les paramètres de l'analyse personnalisée du conteneur et des images en modifiant les paramètres de cette tâche. Par défaut, la tâche *Custom_Container_Scan* a les mêmes paramètres que la tâche *Container_Scan* (ID:18).

Pour lancer la tâche Analyse personnalisée du conteneur, exécutez la commande :

```
kesl-control --scan-container <ID/nom[:tag]>
```

où `<ID/nom[:tag]>` est le nom ou l'ID du conteneur ou de l'image. Pour vérifier plusieurs objets, vous pouvez utiliser des **masques**.

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

S'il existe plusieurs entités portant le même nom, l'application les analyse toutes.

À la suite de l'exécution de la commande, une tâche temporaire d'analyse du conteneur et des images est créée, qui est automatiquement supprimée une fois terminée. Parallèlement, les résultats de l'analyse sont affichés dans la console.

Exemples :
Analyse du conteneur baptisé my_container :
```
kesl-control --scan-container my_container
```
Analysez l'image portant le nom my_image (tous les tags) :
```
kesl-control --scan-container my_image*
```

Intégration à Jenkins

Kaspersky Endpoint Security prend en charge l'intégration à Jenkins. Les plug-ins Jenkins Pipeline peuvent être utilisés pour analyser des images Docker à différentes étapes. Par exemple, vous pouvez analyser des images Docker dans un référentiel pendant le processus de développement ou avant la publication.

Pour intégrer Kaspersky Endpoint Security à Jenkins :

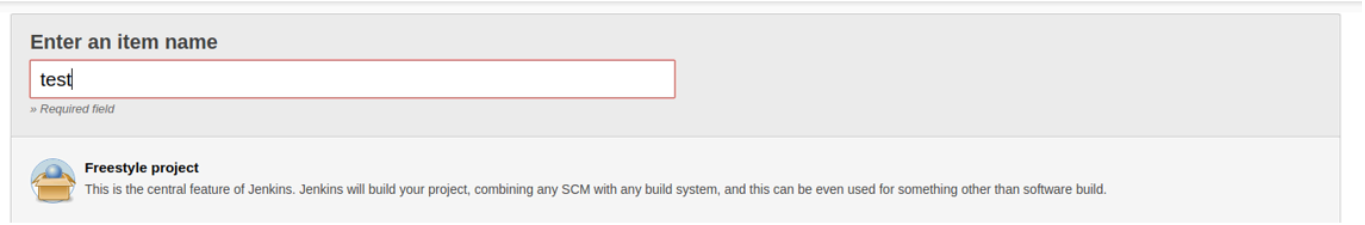
1. Installez Kaspersky Endpoint Security sur un nœud Jenkins.
2. Installez Docker Engine sur un nœud Jenkins.

   Pour en savoir plus, reportez-vous à la documentation de Docker Engine.
3. Octroyez les privilèges d'administrateur de l'application Kaspersky Endpoint Security à l'utilisateur Jenkins :

   ```
   kesl-control --grant-role admin <nom d'utilisateur Jenkins>
   ```
4. Ajoutez un utilisateur Jenkins au groupe de dockers :

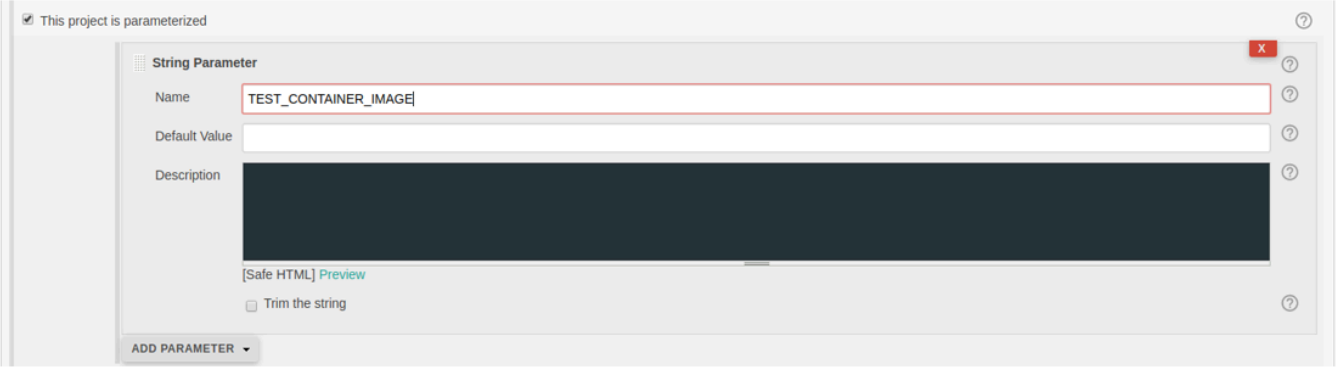
   ```
   sudo usermod -aG docker <nom d'utilisateur Jenkins>
   ```

   En général, le nom jenkins est utilisé.
5. Dans Jenkins, créez une tâche de compilation nommée `test` (**New Item** → **Enter an item name**).



6. Configurez votre projet, selon vos besoins. On suppose qu'en conséquence, vous avez une image ou un conteneur démarré que vous devez analyser.
7. Pour démarrer le conteneur Docker, ajoutez le script suivant à la procédure de build Jenkins. Si vous utilisez des plug-ins Jenkins ou une autre façon de démarrer les conteneurs Docker, enregistrez l'ID du conteneur Docker en cours d'exécution dans le fichier /tmp/kesl_cs_info pour une analyse ultérieure :

   ```
   TMP_FILE="/tmp/kesl_cs_info"
   EXIT_CODE=0
   echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
   CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
   /storage/docker_process.sh)
   if [ -z "${CONTAINER_ID}" ] ; then
   echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
   exit 1
   fi
   echo "${CONTAINER_ID}" > ${TMP_FILE}
   exit ${EXIT_CODE}
   ```



8. Après avoir construit les artefacts, ajoutez le script suivant aux étapes de construction des jenkins.

   Ce script prend en charge un conteneur pour l'analyse. Si nécessaire, modifiez le script selon vos besoins.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. Pour lancer l'analyse d'une image Docker à partir d'un référentiel, utilisez le script suivant :

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
```

```
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Enregistrez la tâche de build.

Gestion du pare-feu

Quand un appareil est connecté à des réseaux locaux (LAN) ou à Internet, il est exposé à des virus, d'autres applications malveillantes et une multitude d'attaques qui exploitent des vulnérabilités dans les systèmes d'exploitation et dans les logiciels. Le pare-feu du système d'exploitation protège les données sauvegardées sur l'appareil de l'utilisateur en bloquant la plupart des menaces pesant sur le système d'exploitation lorsque l'appareil est connecté à Internet ou au réseau local.

Le pare-feu du système d'exploitation vous permet de détecter toutes les connexions réseau sur l'appareil de l'utilisateur et de fournir une liste de ses adresses IP. Le module Gestion du pare-feu vous permet de définir l'état de ces connexions réseau en configurant des règles de paquets réseau.

À l'aide des règles de paquets réseau, vous pouvez définir le niveau souhaité de protection de l'appareil, du blocage complet de l'accès Internet pour toutes les applications à l'autorisation d'un accès illimité. Toutes les connexions sortantes sont autorisées par défaut, sauf si des règles d'interdiction correspondantes ont été définies pour le module Gestion du pare-feu.

Par défaut, le module Gestion du pare-feu est désactivé.

Désactivez les autres outils de gestion de pare-feu du système d'exploitation avant d'activer le module Gestion du pare-feu.

Lorsque vous activez le module Gestion du pare-feu, Kaspersky Endpoint Security supprime automatiquement toutes les règles utilisateur configurées pour le pare-feu à l'aide du système d'exploitation. Après désactivation du module, ces règles ne sont pas restaurées. Si nécessaire, enregistrez les règles de pare-feu personnalisées avant d'activer le module de gestion du pare-feu.

Si la gestion du pare-feu est activée, Kaspersky Endpoint Security vérifie le pare-feu du système d'exploitation et bloque toute tentative de modification des paramètres du pare-feu, par exemple lorsqu'une application ou un utilitaire tente d'ajouter ou de supprimer une règle de pare-feu. Kaspersky Endpoint Security vérifie le pare-feu du système d'exploitation toutes les 60 secondes et, si nécessaire, restaure l'ensemble des règles de pare-feu créées à l'aide de l'application. Il est impossible de modifier la fréquence d'analyse.

Kaspersky Endpoint Security vérifie toujours le pare-feu du système d'exploitation lorsque la gestion du pare-feu est désactivée. Cela permet à l'application de rétablir les règles dynamiques.

Vous pouvez activer ou désactiver la gestion du pare-feu, et également configurer les paramètres suivants :

- Configurer une liste de règles de paquets réseau que Kaspersky Endpoint Security appliquera lorsqu'il détectera une tentative d'établir une connexion réseau. Vous pouvez ajouter et supprimer des règles de paquets réseau et modifier la priorité d'exécution d'une règle de paquets réseau.

  Dans certains systèmes d'exploitation sous Red Hat Enterprise Linux, les règles du pare-feu créées à l'aide de l'application Kaspersky Endpoint Security ne peuvent être affichées qu'à l'aide des lignes de commande de gestion(commande `kesl-control -F --query`).

- Sélectionner les actions par défaut à appliquer aux connexions et aux paquets entrants si d'autres règles pour les paquets réseau ne s'appliquent pas à ce type de connexion.

- Configurer les adresses réseau pour les associer à des réseaux prédéfinis. Vous pouvez ajouter des adresses IP ou des sous-réseaux aux réseaux disponibles et supprimer des adresses des réseaux disponibles.
- Activer ou désactiver l'ajout automatique de règles d'autorisation pour les ports de l'Agent d'administration.

À propos des règles de paquet réseau

Les *règles de paquet réseau* sont des actions autorisées ou interdites exécutées par Kaspersky Endpoint Security en cas de détection d'une tentative de connexion réseau.

Les règles de paquet réseau imposent des restrictions sur les paquets réseau, quelle que soit l'application. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné.

Toutes les connexions sortantes sont autorisées par défaut (paramètre d'action par défaut), sauf si les règles d'interdiction correspondantes ont été définies pour le module Gestion du pare-feu. L'action par défaut est exécutée selon la priorité la plus faible : si aucune autre règle de paquet réseau n'a été déclenchée ou si aucune règle de paquet réseau n'a été définie, la connexion est autorisée.

La gestion du pare-feu définit certaines règles de paquet réseau par défaut. Vous pouvez créer vos propres règles de paquet réseau et définir des priorités d'exécution pour chacune d'entre elles.

À propos des règles dynamiques

L'application Kaspersky Endpoint Security vous permet d'ajouter et de supprimer des *règles dynamiques* sur le pare-feu nécessaires au bon fonctionnement de l'application. Par exemple, l'Agent d'administration ajoute des règles dynamiques qui autorisent les connexions à Kaspersky Security Center lancées à la fois par l'application et par Kaspersky Security Center. Règles de protection contre le chiffrement sont également dynamiques.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, des règles dynamiques sont automatiquement ajoutées au pare-feu qui autorisent les connexions à la SVM et au Serveur d'intégration.

Kaspersky Endpoint Security ne contrôle pas les règles dynamiques et ne bloque pas l'accès aux ressources réseau pour les modules de l'application. Les règles dynamiques ne dépendent pas de l'état du module Gestion du pare-feu (activé/désactivé) ni de l'évolution des paramètres de fonctionnement du module. La priorité d'exécution des règles dynamiques est supérieure à la priorité des règles de paquets réseau. L'application rétablit un ensemble de règles dynamiques à l'aide de l'utilitaire iptables en cas de suppression d'une d'entre elles.

Vous pouvez consulter l'ensemble des règles dynamiques (à l'aide de la commande `kesl-control -F --query`), mais les paramètres des règles dynamiques ne peuvent pas être modifiés.

À propos des réseaux préconfigurés disponibles

Un *réseau accessible* est un groupe spécifique d'adresses IP ou de sous-réseaux. En utilisant un réseau accessible, vous pouvez employer les mêmes règles pour plusieurs adresses ou sous-réseaux IP au lieu de créer une règle séparée pour chacun d'entre eux. Le réseau accessible peut être utilisé comme valeur du paramètre d'adresse distante lors de la création d'une règle de paquet réseau. Kaspersky Endpoint Security propose trois réseaux préconfigurés :

- **Publics**. Un réseau qui n'est pas protégé par une application antivirus, un pare-feu ou des filtres (comme les réseaux des cybercafés).
- **Local**. Un réseau dont les utilisateurs sont autorisés à accéder aux fichiers et aux imprimantes de cet appareil (comme les réseaux locaux ou domestiques).
- **De confiance**. Un réseau sécurisé dans lequel l'appareil n'est pas exposé aux attaques ou aux tentatives d'accès non autorisées.

Vous ne pouvez pas créer un nouveau réseau ni supprimer un réseau prédéfini, mais vous pouvez ajouter des adresses IP et des sous-réseaux à un réseau ou les en supprimer.

Gestion du pare-feu dans Web Console

Dans Web Console, vous pouvez gérer les paramètres du Firewall dans les propriétés de la stratégie (**Paramètres de l'application** → **Communication et protection Internet** → **Pare-feu**).

Gestion du pare-feu dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de Gestion du Firewall dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale** → **Gestion du Firewall**).

Paramètres du module Gestion du pare-feu

Paramètre	Description
Activer la tâche de gestion du pare-feu	La case active ou désactive le module Gestion du pare-feu. La case est décochée par défaut.
Règles de paquet réseau	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Règles pour les paquets réseau**. Cette fenêtre permet de configurer les règles de paquets réseau exécutées par le module Gestion du pare-feu lorsqu'il détecte la tentative de connexion réseau.
Réseaux disponibles	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Réseaux disponibles**. Cette fenêtre permet de configurer une liste de réseaux que le module Gestion du pare-feu va surveiller.
Connexions entrantes	Cette liste déroulante permet de sélectionner une action à réaliser sur les connexions réseau entrantes : • **Autoriser** les connexions réseau (valeur par défaut). • **Bloquer** les connexions réseau entrantes.

Paramètre	Description
Paquets entrants	Dans cette liste déroulante, vous pouvez sélectionner une action à effectuer pour les paquets entrants : • **Autoriser** les paquets entrants (valeur par défaut). • **Bloquer** les paquets entrants.
Toujours ajouter les règles d'autorisation pour les ports de l'Agent d'administration	Cette case active ou désactive l'ajout automatique de règles d'autorisation pour les ports de l'Agent d'administration. La case est cochée par défaut.

Fenêtre Règles de paquet réseau

Le tableau **Règles de paquet réseau** contient des règles de paquet réseau que le module Gestion du pare-feu utilisera pour surveiller l'activité réseau. Pour les règles de paquet réseau, vous pouvez configurer les paramètres décrits dans le tableau ci-dessous.

Paramètres des règles de paquet de réseau

Paramètre	Description
Nom	Le nom de la règle de paquet réseau.
Action	Action que le module Gestion du pare-feu doit effectuer suite à la détection de l'activité réseau.
Adresse locale	Adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
Adresse à distance	Adresses réseau des appareils à distance qui peuvent envoyer et/ou recevoir des paquets réseau.
Enregistrement des événements dans le journal	Cette colonne indique si l'application enregistrera ou non les actions de règles de paquets réseau dans le rapport. Si la colonne indique **Oui**, l'application enregistre les actions de la règle de paquet réseau dans le journal. Si la colonne indique **Non**, l'application n'enregistre pas les actions de la règle de paquet réseau.

Par défaut, le tableau des règles de paquet réseau est vide.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les règles de paquet réseau dans le tableau.

Fenêtre Ajout d'une règle de paquet réseau

Cette fenêtre permet de configurer les paramètres de la règles de paquet réseau ajouté.

Paramètres des règles pour les paquets réseau

Paramètre	Description
Protocole.	Vous pouvez sélectionner le type de protocole de transfert de données pour lequel vous souhaitez surveiller l'activité réseau : • **Tous** (valeur par défaut) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**

Paramètre	Description
Direction	Vous pouvez définir la direction de l'activité réseau surveillée : • **Paquets entrants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les paquets entrants. • **Entrant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les connexions entrantes. • **Entrants/Sortants** (valeur par défaut). Si cet élément est sélectionné, le module Gestion du pare-feu contrôle à la fois les connexions entrantes et sortantes. • **Paquets entrants/sortants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle à la fois les paquets entrants et sortants. • **Paquets sortants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les paquets sortants. • **Sortant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle uniquement les connexions sortantes.
Type ICMP	Vous pouvez indiquer le type ICMP. Le module Gestion du pare-feu contrôle les messages d'un type spécifié envoyés par un hôte ou une passerelle. Si vous avez choisi l'option **Spécifié**, le champ de saisie du type ICMP s'affiche. Cette fenêtre s'affiche uniquement si vous avez sélectionné les protocoles de transfert de données **ICMP** ou **ICMPv6** dans la liste déroulante **Protocole**.
Code ICMP	Vous pouvez préciser le code ICMP. Le module Gestion du pare-feu surveillera les messages du type spécifié dans le champ **Type ICMP** et avec le code spécifié dans le champ **Code ICMP**, envoyés par l'hôte ou la passerelle. Si vous avez choisi l'option **Spécifié**, le champ de saisie du code ICMP s'affiche. Cette fenêtre s'affiche uniquement si vous avez sélectionné les protocoles de transfert de données **ICMP** ou **ICMPv6** dans la liste déroulante **Protocole**.
Ports distants	Vous pouvez spécifier le numéro de port ou la plage de numéros de ports des appareils à distance entre lesquels la connexion doit être contrôlée. Si vous avez choisi l'option **Spécifié**, le champ de saisie des numéros des ports s'affiche. Cette fenêtre s'ouvre uniquement si vous avez sélectionné les protocoles de transfert de données **TCP** ou **UDP** dans la liste déroulante **Protocole**.
Ports locaux	Vous pouvez spécifier le numéro de port ou la plage de numéros de ports des appareils locaux entre lesquels la connexion doit être contrôlée. Si vous avez choisi l'option **Spécifié**, le champ de saisie des numéros des ports s'affiche. Cette fenêtre s'ouvre uniquement si vous avez sélectionné les protocoles de transfert de données **TCP** ou **UDP** dans la liste déroulante **Protocole**.
Adresses à distance	Vous pouvez préciser les adresses réseau des appareils distants qui peuvent envoyer et recevoir des paquets réseau. • **Toute adresse** (valeur par défaut). Si cette option est sélectionnée, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils distants avec toute adresse IP. • **Adresse ou plage d'adresses spécifiée**. Si vous sélectionnez cette option, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils à distance portant les adresses IP spécifiées dans le champ en-dessous. En cliquant sur le bouton **Ajouter** au-dessus du tableau, vous ouvrez la fenêtre **Ajout d'adresses IP**, dans laquelle vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil. • **Par type de réseau**. Si vous avez sélectionné cette option, la règle du réseau contrôle les paquets réseau envoyés et reçus par des appareils distants avec des adresses IP associées au type de réseaux sélectionné dans la liste déroulante : **Réseaux publics**, **Réseaux locaux** ou **Réseaux approuvés**.
Adresses locales	Vous pouvez renseigner les adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et recevoir des paquets réseau. • **Toute adresse** (valeur par défaut). Si cette option est sélectionnée, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des appareils hébergeant Kaspersky Endpoint Security et portant n'importe quelle adresse IP. • **Adresse ou plage d'adresses spécifiée**. Si cette option est sélectionnée, la règle réseau contrôle les adresses réseau des appareils sur lesquels Kaspersky Endpoint Security est installé et qui peuvent envoyer et recevoir des paquets réseau. Ces adresses réseau sont spécifiées dans le tableau ci-dessous. En cliquant sur le bouton **Ajouter** au-dessus du tableau, vous ouvrez la fenêtre **Ajout d'adresses IP**, dans laquelle vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil.
Action	Vous pouvez définir l'action que le module Gestion du pare-feu effectuera en cas de détection de l'activité réseau : • **Bloquer** l' activité réseau. • **Autoriser** l'activité réseau (valeur par défaut).
Enregistrement des événements dans le journal	Vous pouvez indiquer si les actions de la règle de réseau doivent être prises en compte dans le rapport.
Nom de la règle	Le champ de saisie pour le nom de la règle de paquet réseau.

Fenêtre Ajout d'adresses IP

Dans cette fenêtre, vous pouvez spécifier l'adresse IP, l'adresse réseau ou la plage d'adresses IP de l'appareil.

Vous pouvez spécifier plusieurs adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie.

Fenêtre Réseaux disponibles

Le tableau **Réseaux disponibles** contient les réseaux que le module Gestion du pare-feu va surveiller. Par défaut, le tableau des réseaux disponibles est vide.

Paramètres Réseaux disponibles

Paramètre	Description
Adresse IP ;	Adresse IP du réseau.
Type de réseau	Les types de réseau (**Réseau public**, **Réseau local** ou **Réseau de confiance**).

Vous pouvez ajouter, modifier et supprimer les réseaux disponibles.

Fenêtre Connexion réseau

Cette fenêtre permet de configurer la connexion réseau que le module Gestion du pare-feu surveillera.

Connexion réseau

Paramètre	Description
Adresse IP ;	Champ de saisie de l'adresse IP du réseau.
Type de réseau	Vous pouvez sélectionner le type de réseau : • **Réseau public**. • **Réseau local**. • **Réseau de confiance**.

Gestion du pare-feu dans la ligne de commande

Sur la ligne de commande, vous pouvez configurer la gestion du pare-feu à l'aide de la tâche prédéfinie de gestion du pare-feu (*Firewall_Management*).

Par défaut, la tâche Gestion du pare-feu n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres de gestion du pare-feu en modifiant les paramètres de la tâche prédéfinie Gestion du pare-feu.

Vous pouvez également configurer les paramètres de gestion du pare-feu à l'aide des commandes de gestion du pare-feu :

- Créer et supprimer des règles de paquets réseau et modifier leur priorité d'exécution.
- Générer une liste des adresses IP ou des sous-réseaux dans les zones réseau.
- Afficher les règles du pare-feu créées dans l'application à l'aide de la commande `kesl-control -F --query`.

Paramètres de Gestion du pare-feu

Paramètre	Description	Valeurs
`DefaultIncomingAction`	L'action par défaut à exécuter sur une connexion entrante, si aucune règle réseau ne peut être appliquée à ce type de connexion.	`Allow` (valeur par défaut) : autorise les connexions entrantes. `Block` : bloquer la connexion entrante.
`DefaultIncomingPacketAction`	L'action par défaut à exécuter sur un paquet entrant, si aucune règle de paquet réseau ne peut être appliquée à ce type de connexion.	`Allow` (valeur par défaut) : autorise les paquets entrants. `Block` : bloquer le paquet entrant.
`OpenNagentPorts`	Ajout de règles dynamiques pour l'Agent d'administration aux règles de paquets.	`Yes` (valeur par défaut) : ajoute des règles dynamiques pour l'Agent d'administration aux règles de paquets. `No` : n'ajoute des règles dynamiques pour l'Agent d'administration aux règles de paquets.
La section **[PacketRules.item_#]** définit les règles de paquet réseau de la tâche Gestion du pare-feu. Vous pouvez définir plusieurs sections `[PacketRules.item_#]` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. Chaque section `[PacketRules.item_#]` contient les paramètres suivants :		
`Name`	Le nom de la règle de paquet réseau.	Valeur par défaut : `Packet rule #<n>`, où n est un index.
`FirewallAction`	Action à réaliser sur les connexions définies dans cette règle de paquet réseau.	`Allow` (valeur par défaut) : autorise les connexions réseau. `Block` : bloquer la connexion réseau.

`Protocol`	Type de protocole pour lequel l'activité réseau doit être contrôlée.	`Any` (valeur par défaut) : la tâche de gestion du pare-feu contrôle toute l'activité réseau.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

`RemotePorts`	Numéros de port des appareils à distance entre lesquels la connexion doit être contrôlée. Vous pouvez spécifier la valeur sous forme d'entier ou d'intervalle. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `TCP` ou `UDP`.	`Any` (valeur par défaut) : contrôle tous les ports distants. `0` : `65535`.
`LocalPorts`	Numéros de port des appareils locaux entre lesquels la connexion doit être contrôlée. Vous pouvez spécifier la valeur sous forme d'entier ou d'intervalle. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `TCP` ou `UDP`.	`Any` (valeur par défaut) : contrôle tous les ports locaux. `0` : `65535`.
`ICMPType`	Type de paquet ICMP. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `ICMP` ou `ICMPv6`.	`Any` (valeur par défaut) : contrôle tous les types de paquet ICMP. Entier nombre en fonction d'une spécification du protocole de transfert de données.

Paramètre	Description	Valeurs
`ICMPCode`	Code du paquet ICMP. Ce paramètre peut être défini uniquement si le paramètre `Protocol` a la valeur `ICMP` ou `ICMPv6`.	`Any` (valeur par défaut) : contrôle tous les codes des paquets ICMP. Entier nombre en fonction d'une spécification du protocole de transfert de données.
`Direction`	Direction de l'activité réseau contrôlée.	`IncomingOutgoing` ou `InOut` (valeur par défaut) : contrôle les connexions entrantes et sortantes. `Incoming` ou `In` : contrôler uniquement les connexions entrantes. `Outgoing` ou `Out` : contrôler uniquement les connexions sortantes. `IncomingPacket` ou `InPacket` : contrôler uniquement les paquets entrants. `OutgoingPacket` ou `OutPacket` : contrôler uniquement les paquets sortants. `IncomingOutgoingPacket` ou `InOutPacket` : contrôle les paquets entrants et sortants.
`RemoteAddress`	Adresses réseau des appareils distants qui peuvent envoyer et recevoir des paquets réseau.	`Any` (valeur par défaut) : contrôle les paquets réseau envoyés et/ou reçus par des appareils distants possédant n'importe quelle adresse IP. `Trusted` : zone réseau prédéfinie pour les réseaux de confiance. `Local` : zone réseau prédéfinie pour les réseaux locaux. `Public` : zone réseau prédéfinie pour les réseaux publics. `d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d – d.d.d.d` : plage d'adresses de la version IPv4. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` : plage d'adresses de la version IPv6. x:x:x:x:x:x:x:x/p : sous-réseau d'adresse de la version IPv6, où p est un nombre compris entre 0 et 128, vous pouvez utiliser **::** pour l'abréviation.
`LocalAddress`	Adresses réseau des appareils dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.	`Any` (valeur par défaut) : contrôle les paquets réseau envoyés et/ou reçus par des appareils locaux possédant n'importe quelle adresse IP. `d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d – d.d.d.d` : plage d'adresses de la version IPv4. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` : plage d'adresses de la version IPv6. x:x:x:x:x:x:x:x/p : sous-réseau d'adresse de la version IPv6, où p est un nombre compris entre 0 et 128, vous pouvez utiliser **::** pour l'abréviation.
`LogAttempts`	Incluez un enregistrement dans le rapport d'action des règles de réseau.	`Yes` : enregistrer les actions dans un rapport. `No` (valeur par défaut) : ne pas enregistrer les actions dans un rapport.
La section **[NetworkZonesPublic]** contient les adresses réseau associées aux réseaux publics. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		

Paramètre	Description	Valeurs
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : "" (pas d'adresses réseau dans cette zone).
La section **[NetworkZonesLocal]** contient les adresses réseau associées aux réseaux locaux. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : `""` (pas d'adresses réseau dans cette zone).
La section **[NetworkZonesTrusted]** contient les adresses réseau associées aux réseaux de confiance. Vous pouvez définir plusieurs adresses IP ou des sous-réseaux d'adresses IP.		
`Address.item_#`	Indique l'adresse IP ou le sous-réseau IP.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. Valeur par défaut : `""` (pas d'adresses réseau dans cette zone).

Configuration d'une liste de règles pour les paquets réseau sur la ligne de commande

Pour ajouter une règle de paquet réseau, exécutez la commande suivante :

```
kesl-control --add-rule [--name <nom de la règle>] [--action <action>] [--protocol
<protocole>] [--direction <direction>] [--remote <adresse distante>[:<port ou plage
de ports>]] [--local <adresse locale>[:<port ou plage de ports>]] [--at <index>]
```

où :

- `--name <nom de la règle>` est le nom de la règle de paquet réseau.
- `--action <action>` est l'action à réaliser sur les connexions définies dans la règle de paquet réseau.
- `--protocol <protocole>` est le type de protocole de communication pour lequel vous souhaitez surveiller l'activité réseau.

- `--direction <sens>` est le sens de l'activité réseau surveillée.
- `--remote <adresse distante[:<port ou plage de ports>]>` est l'adresse réseau de l'appareil distant. Vous pouvez spécifier le nom d'une zone réseau prédéfinie comme adresse distante.
- `--local <adresse locale[:<port ou plage de ports>]>` est l'adresse réseau de l'appareil sur lequel Kaspersky Endpoint Security est installé.
- `--at <index>` est l'index des règles dans la liste des règles pour les paquets réseau. Si le commutateur `--at` n'est pas spécifié ou si sa valeur est supérieure au nombre de règles dans la liste, la nouvelle règle est ajoutée à la fin de la liste.

Les paramètres pour lesquels vous ne spécifiez pas de valeurs dans la commande sont définis sur les valeurs par défaut.

Exemples :
Pour créer une règle qui bloque toutes les connexions entrantes et établies au port TCP 23, exécutez la commande suivante :

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Pour créer une règle qui bloque toutes les connexions entrantes et établies au port TCP 23 de la zone réseau Public, exécutez la commande suivante :

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

Pour supprimer une règle de paquet réseau, exécutez une des commandes suivantes :

- `kesl-control --del-rule --name <nom de la règle>`
- `kesl-control --del-rule --index <indice>`

où :

- `--name <nom de la règle>` est le nom de la règle de paquet réseau.
- `--index <index>` est l'index actuel de la règle dans la liste des règles pour les paquets réseau.

Si la liste des règles de paquets réseau contient plusieurs règles portant le même nom ou ne contient pas de règle portant le nom ou l'index spécifié, une erreur se produit.

Pour modifier la priorité d'exécution d'une règle pour le paquet réseau, exécutez l'une des commandes suivantes :

- `kesl-control --move-rule --name <nom de la règle> --at <indice>`
- `kesl-control --move-rule --index <indice> --at <indice>`

où :

- `--name <nom de la règle>` est le nom de la règle de paquet réseau.
- `--index <index>` est l'index actuel de la règle dans la liste des règles pour les paquets réseau.
- `--at <index>` est le nouvel index de la règle dans la liste des règles pour les paquets réseau.

Configuration des zones réseau sur la ligne de commande

Pour ajouter une adresse réseau à la zone, exécutez la commande suivante :

```
kesl-control --add-zone <zone> --address <adresse>
```

où :

- `<zone>` est le nom prédéfini de la zone réseau. Valeurs possibles : `Public`, `Local`, `Trusted`.
- `<adresse>` est l'adresse réseau ou le sous-réseau.

Pour supprimer une adresse réseau d'une zone, exécutez l'une des commandes suivantes :

- `kesl-control --del-zone <zone> --address <adresse>`
- `kesl-control --del-zone <zone> --index <index d'adresse dans la zone>`

Si une zone contient plusieurs éléments porteur de la même adresse réseau, la commande `--del-zone` n'est pas exécutée.

Si l'adresse réseau ou l'index indiqués n'existent pas, un message d'erreur s'affiche.

Protection contre les menaces Internet

Le module Protection contre les menaces Internet vous permet d'analyser le trafic entrant transmis via les protocoles HTTP, HTTPS et FTP, les sites et les adresses IP, d'empêcher le téléchargement de fichiers malveillants depuis Internet et de bloquer l'accès au phishing, à la publicité et à d'autres sites dangereux. La Protection contre les menaces Internet utilise le port 9879 pour intercepter les connexions. Si le port 9879 est utilisé, l'application sélectionne automatiquement un port disponible pour intercepter les connexions.

L'arrêt ou le démarrage d'une application ou du module Protection contre les menaces Internet entraîne l'interruption des connexions sur les ports interceptés, tels que HTTPS.

Par défaut, la pProtection contre les menaces Internet est désactivée. En même temps, il est activé automatiquement si la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » dans les propriétés de la stratégie n'est pas installé) et l'un des fichiers exécutables suivants du navigateur, notamment format snap, est détecté dans le système :

- chrome ;
- chromium ;
- chromium-browser ;
- firefox ;
- firefox-esr ;
- google-chrome ;
- opera ;
- yandex-browser.

Vous pouvez activer et désactiver la Protection contre les menaces Internet et configurer les paramètres de protection :

- Sélectionnez l'action que l'application effectuera sur la ressource Web sur laquelle un objet dangereux est détecté.
- Configurez une liste d'adresses Internet fiables. L'application n'analyse pas le contenu des sites Internet dont l'adresse figure dans cette liste.
- Sélectionnez les objets que l'application détectera lors de l'analyse du trafic entrant.
- Configurez l'analyse des connexions chiffrées pour vérifier le trafic HTTPS.

  Pour analyser le trafic FTP, les paramètres d'analyse du trafic réseau doivent être configurés pour contrôler tous les ports réseau.

Lorsque vous ouvrez un site, l'application effectue les opérations suivantes :

1. Vérifie la sécurité du site à l'aide des bases de l'application téléchargées.
2. Vérifie la sécurité du site à l'aide d'une **analyse heuristique**, si cette fonction est activée.

   Lors de l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique peut détecter les objets dangereux pour lesquels il n'y a actuellement aucun enregistrement dans les bases de données de Kaspersky Endpoint Security.
3. Vérifie la fiabilité d'un site à l'aide des bases de données de réputation de Kaspersky, si Kaspersky Security Network est activé.

   Il est recommandé d'activer l'utilisation de Kaspersky Security Network pour augmenter l'efficacité de la protection contre les menaces Internet.
4. Bloque ou autoriser l'ouverture du site.

Lors d'une tentative d'ouverture d'un site dangereux, l'application effectue les opérations suivantes :

- Pour le trafic HTTP ou FTP, l'application bloque l'accès et affiche un message d'avertissement.
- Pour le trafic HTTPS, un navigateur affiche une page d'erreur.

La suppression des certificats de l'application peut entraîner un fonctionnement incorrect du module de protection contre les menaces Internet.

Si vous avez configuré des exclusions de l'interception du trafic par l'application Kaspersky Endpoint Security, elles affectent le fonctionnement du module Protection contre les menaces Internet.

Configuration de la protection contre les menaces internet dans Web Console

Dans Web Console, vous pouvez gérer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (**Paramètres de l'application → Communication et protection Internet → Protection contre les menaces Internet**).

Configuration de la protection contre les menaces internet dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale → Protection contre les menaces Internet**).

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Activer la Protection contre les menaces Internet	Cette case active ou désactive le module Protection contre les menaces Internet. La case est décochée par défaut.
Adresses Internet de confiance	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre Adresses Internet de confiance dans laquelle vous pouvez établir une liste d'adresses Internet de confiance. L'application n'analyse pas le contenu des sites Internet dont l'adresse figure dans cette liste.
Action en cas de détection d'une menace	Action que l'application effectue sur les ressources Internet où un objet dangereux a été détecté : • **Bloquer** l'accès à tout objet dangereux détecté dans le trafic Internet, affiche une notification concernant la tentative d'accès bloqué et enregistre les informations sur l'objet dangereux dans le journal (valeur par défaut). • **Informer** l'utilisateur lorsqu'un objet dangereux est détecté dans le trafic Internet. La Protection contre les menaces Internet autorise le téléchargement de cet objet sur l'appareil. Dans ce cas, l'application consigne des informations sur l'objet dangereux et ajoute des informations relatives à ce dernier dans la liste des menaces actives.
Paramètres d'analyse	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre Paramètres d'analyse dans laquelle vous pouvez configurer les paramètres d'analyse du trafic entrant.

Fenêtre Adresses Internet de confiance

Cette fenêtre permet d'ajouter des adresses et des pages Internet au contenu desquelles vous faites confiance.

Vous pouvez ajouter uniquement des adresses Internet de confiance HTTP/HTTPS à cette liste. Vous pouvez utiliser des **masques** pour spécifier des adresses Internet. L'utilisation de masques dans le but de définir des adresses IP n'est pas prise en charge. Par défaut, la liste est vide. Vous pouvez ajouter, modifier et supprimer des adresses Internet dans la liste.

Lors de la création d'un masque d'adresse, vous pouvez saisir l'astérisque (*) comme caractère générique pour un ou plusieurs caractères. Si vous saisissez ainsi le masque d'adresse *abc*, il sera appliqué à toutes les ressources Internet contenant la séquence abc (par exemple, www.virus.com/download_virus/page_0-9abcdef.html). Pour inclure l'astérisque dans le masque d'adresse en tant que caractère et non en tant que masque, saisissez deux fois le caractère * (par exemple, www.virus.com/**/page_0-9abcdef.html signifie www.virus.com/*/page_0-9abcdef.html).

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse du trafic entrant pendant le fonctionnement du module Protection contre les menaces Internet.

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Détecter les objets malveillants	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet malveillantes. La case est cochée par défaut.
Détecter les liens de phishing	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet de phishing. La case est cochée par défaut.
Détecter les liens de phishing à l'aide de l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique pour la détection des liens de phishing. Cette case est disponible si la case **Détecter les liens de phishing** est cochée et elle est sélectionnée par défaut.

Paramètre	Description
Détecter les applications publicitaires	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet d'applications publicitaires. La case est décochée par défaut.
Détecter les applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données	Cette case active ou désactive la vérification des liens par rapport aux bases de données des applications légitimes qui pourraient être détournées par des individus malintentionnés pour nuire aux appareils ou aux données. La case est décochée par défaut.

Configuration de la Protection contre les menaces Internet sur la ligne de commande

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces Internet à l'aide de la tâche prédéfinie Protection contre les menaces Internet (*Web_Threat_Protection*).

La tâche s'exécute automatiquement si l'un des navigateurs pris en charge est détecté sur le système et que la gestion locale des paramètres de protection contre les menaces Internet est autorisée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » n'est pas défini dans les propriétés de la stratégie). Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la protection contre les menaces Internet en modifiant les paramètres de la tâche prédéfinie Protection contre les menaces Internet.

Paramètres de la tâche de protection contre les menaces Internet

Paramètre	Description	Valeurs
`ActionOnDetect`	Spécifie l'action à effectuer lors de la détection d'un objet infecté dans le trafic Internet.	`Notify` : autorise le téléchargement de l'objet détecté, affiche une notification concernant la tentative d'accès bloqué et crée une entrée de journal avec des informations sur l'objet infecté. `Block` (valeur par défaut) : bloque l'accès à l'objet détecté, affiche une notification concernant la tentative d'accès bloqué et crée une entrée de journal avec des informations sur l'objet infecté.
`CheckMalicious`	Active ou désactive l'analyse des liens par rapport aux bases de données d'adresses Internet malveillantes.	`Yes` (valeur par défaut) : vérifie si les liens sont répertoriés dans la base de données des adresses Internet malveillantes. `No` : ne vérifie pas si les liens sont répertoriés dans la base de données des adresses Internet malveillantes.
`CheckPhishing`	Active ou désactive l'analyse des liens par rapport aux bases de données d'adresses Internet de phishing.	`Yes` (valeur par défaut) : vérifie si les liens figurent dans la base de données des adresses Internet de phishing. `No` : ne vérifie pas si les liens figurent dans la base de données des adresses Internet de phishing.
`UseHeuristicForPhishing`	Active ou désactive l'utilisation de l'analyse heuristique pour vérifier les pages Web à la recherche de liens de phishing.	`Yes` (valeur par défaut) : détecte les liens de phishing à l'aide de l'analyse heuristique. Si cette valeur est spécifiée, le niveau de l'analyse heuristique est `Light` (faible) (l'analyse la moins approfondie avec une charge minimale sur le système). Vous ne pouvez pas modifier le niveau de l'analyse heuristique pour la tâche de protection contre les menaces Internet. `No` : ne détecte pas les liens de phishing à l'aide de l'analyse heuristique.
`CheckAdware`	Active ou désactive l'analyse des liens par rapport aux bases de données d'adresses Internet publicitaires.	`Yes` : vérifie si les liens sont répertoriés dans la base de données des adresses Internet publicitaires. `No` (valeur par défaut) : ne vérifie pas si les liens sont répertoriés dans la base de données des adresse Internet publicitaires.

Paramètre	Description	Valeurs
`CheckOther`	Active ou désactive la vérification des liens par rapport à une base de données d'adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.	`Yes` : vérifie si des liens sont répertoriés dans les bases de données d'adresses Internet contenant des applications légitimes pouvant être utilisées par des criminels pour endommager vos appareils ou vos données. `No` (valeur par défaut) : ne vérifie pas si des liens sont répertoriés dans les bases de données d'adresses Internet contenant des applications légales pouvant être utilisées par des criminels pour endommager vos appareils ou vos données.
`UseTrustedAddresses`	Active ou désactive l'utilisation d'une liste d'adresses Internet de confiance. L'application ne vérifie pas les adresses Internet de confiance à la recherche de virus et autres objets malveillants. Vous pouvez spécifier des adresses Internet approuvées à l'aide du paramètre `TrustedAddresses.item_#`.	`Yes` (valeur par défaut) : utilise une liste d'adresses Internet de confiance. `No` : n'utilise pas de liste d'adresses Internet de confiance.
`TrustedAddresses.item_#`	Adresses Internet de confiance.	La valeur par défaut n'est pas définie. Vous pouvez utiliser des **masques** pour spécifier des adresses Internet. Lors de la création d'un masque d'adresse, vous pouvez saisir l'astérisque (*) comme caractère générique pour un ou plusieurs caractères. Si vous saisissez ainsi le masque d'adresse *abc*, il sera appliqué à toutes les ressources Internet contenant la séquence abc (par exemple, www.virus.com/download_virus/page_0-9abcdef.html). Pour inclure l'astérisque dans le masque d'adresse en tant que caractère et non en tant que masque, saisissez deux fois le caractère * (par exemple, www.virus.com/**/page_0-9abcdef.html signifie www.virus.com/*/page_0- 9abcdef.html). L'utilisation de masques dans le but de définir des adresses IP n'est pas prise en charge.

Analyse du trafic réseau

Les paramètres d'analyse du trafic réseau sont utilisés dans le fonctionnement des modules Protection contre les menaces Internet, Protection contre les menaces réseau, Protection contre les menaces par emails et Contrôle Internet. Les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet peuvent déchiffrer et analyser le trafic réseau. Par défaut, l'analyse des connexions chiffrées est activée.

Vous pouvez configurer les paramètres d'analyse du trafic réseau suivants :

- Activer ou désactiver l'analyse des connexions chiffrées.
- Sélectionner l'action que l'application entreprend lorsqu'elle détecte un certificat non approuvé.
- Sélectionner l'action que l'application entreprend lorsqu'une erreur de validation du trafic réseau se produit sur un site.
- Activer ou désactiver l'utilisation d'Internet lors de la vérification des certificats.
- Afficher et configurer une liste de domaines de confiance. L'application n'analysera pas les connexions établies lors de la visite de domaines spécifiés.
- Configurer une liste de certificats que l'application considérera comme fiables lors de la vérification des connexions chiffrées.
- Configurer les exclusions d'interception du trafic Vous pouvez spécifier les connexions que l'application exclura de l'interception du trafic. Une connexion exclue est définie par les paramètres suivants :
  - Sens de circulation : entrant ou sortant.
  - Adresse IP de l'appareil à distance : l'adresse IP vers laquelle ou depuis laquelle le trafic est exclu de l'interception (selon la direction du trafic).
  - Port de destination : un port sur un appareil protégé (exclu de l'interception du trafic entrant) ou un port sur un appareil à distance (exclu de l'interception du trafic sortant).

Les exclusions d'interception du trafic s'appliquent uniquement aux connexions TCP et n'affectent pas le fonctionnement des règles de paquets réseau. Les exclusions d'interception du trafic affectent le fonctionnement des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet.

Vous pouvez également configurer des exclusions pour l'interception du trafic pour l'application Kaspersky Endpoint Security à l'aide des outils du système d'exploitation.

- Configurez la liste des ports réseau contrôlés par l'application. Vous pouvez spécifier certains ports réseaux ou certaines plages de ports réseaux à analyser.

  Si vous souhaitez intercepter les connexions réseau vers un serveur NFS, vous devez vous assurer que le serveur NFS est démarré avec l'option `insecure` (afin qu'il accepte les connexions provenant de ports situés en dehors de la plage 1-1024), sinon le serveur NFS peut rejeter ces connexions.

- Sélectionner le mode d'interception du trafic utilisé par l'application.

Lors de la modification des paramètres d'analyse du trafic réseau, l'application génère l'événement *NetworkSettingsChanged*.

À propos des modes d'interception du trafic réseau

L'application peut utiliser l'un des deux modes d'interception du trafic réseau suivants :

- *Utiliser la technologie eBPF*. Si ce mode est sélectionné, l'application utilise la technologie eBPF pour intercepter le trafic. Si l'application ne peut pas utiliser la technologie eBPF pour intercepter le trafic réseau, l'utilitaire iptables est utilisé à la place.

- *Utiliser l'utilitaire iptables*. Si ce mode est sélectionné, l'application utilise l'utilitaire iptables pour intercepter le trafic. Ce mode est sélectionné par défaut.

En mode **Utiliser la technologie eBPF**, l'application crée son propre espace de noms réseau distinct (network linux namespace), où elle redirige les paquets réseau à l'aide de programmes eBPF liés aux files d'attente `tc` (linux traffic control) des interfaces réseau locales. Le trafic réseau redirigé est ensuite analysé en fonction des tâches réseau actives, puis renvoyé à l'interface réseau d'origine.

Pour échanger des données entre espaces de noms réseau, des paires d'interfaces réseau virtuelles `veth` sont utilisées (chaque extrémité de la paire se trouve dans son propre espace de noms réseau) :

- La paire kesl_in – kesl_worm_in transmet le trafic réseau des connexions entrantes.

- La paire kesl_out – kesl_worm_out transmet le trafic réseau des connexions sortantes.

Par l'intermédiaire de ces paires d'interfaces, le trafic réseau est acheminé pour inspection de l'espace de noms par défaut vers l'espace de noms créé par l'application, puis renvoyé après analyse.

Le trafic réseau atteint ces interfaces depuis d'autres interfaces réseau du système uniquement si l'application est en cours d'exécution et que l'interception réseau est activée. Ils ne peuvent pas être utilisés pour transférer des données sur un réseau entre des appareils distants.

Si votre appareil est sensible aux attaques par énumération de ports (par exemple, si l'appareil local possède un pare-feu de système d'exploitation configuré avec un filtrage de ports), il n'est pas recommandé de sélectionner le mode **Utiliser la technologie eBPF**. Il est également déconseillé d'utiliser ce mode d'interception du trafic sur les appareils situés à la périphérie du réseau d'une organisation.

Si l'appareil est situé dans un segment de réseau isolé, dans un réseau local ou à l'intérieur du périmètre réseau de l'organisation, il est permis de sélectionner le mode d'interception du trafic **Utiliser la technologie eBPF**.

Vous pouvez sélectionner le mode d'interception du trafic dans Web Console, dans la Console d'administration et dans la ligne de commande.

Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.

Configuration de l'analyse du trafic réseau dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres d'analyse du trafic réseau dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres du réseau** et **Paramètres de l'application** → **Zone de confiance**).

Configuration de l'analyse du trafic réseau dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres d'analyse du trafic réseau dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Paramètres réseau**).

Paramètres d'analyse des connexions chiffrées

Paramètre	Description
Activer l'analyse des connexions chiffrées.	Cette case active ou désactive l'analyse des connexions chiffrées. La case est cochée par défaut.

Paramètres des connexions chiffrées	Le groupe contient les paramètres d'analyse des connexions chiffrées :
	• **Accéder à un domaine dont le certificat n'est pas fiable** : l'action que l'application effectuera lors du passage à un domaine avec un certificat non approuvé :
	  • **Autoriser** (valeur par défaut) : autoriser la connexion à un domaine avec un certificat douteux.
	  • **Bloquer** : bloquer la connexion à un domaine avec un certificat douteux.
	• **Accès à un domaine avec une erreur lors de l'analyse du trafic réseau** : l'action que l'application effectuera lors du passage à un domaine avec une erreur d'analyse du trafic réseau :
	  • **Autoriser et ajouter un domaine aux exclusions** (valeur par défaut) : ajouter le domaine qui a généré l'erreur à la liste des domaines comportant des erreurs d'analyse et ne pas surveiller le trafic réseau chiffré lors de la visite de ce domaine.
	  • **Bloquer** : bloquer la connexion à un domaine avec une erreur d'analyse.
	• **Stratégie de vérification du certificat** : la manière dont l'application valide les certificats :
	  • **Vérification locale** : l'application n'utilise pas Internet pour vérifier un certificat.
	  • **Vérification complète** (valeur par défaut) : l'application utilise Internet pour vérifier et télécharger les chaînes manquantes qui sont nécessaires pour vérifier un certificat.

Domaines de confiance	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre Domaines de confiance dans laquelle vous pouvez configurer une liste de noms de domaine de confiance.
Certificats racines de confiance	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce lien pour ouvrir la fenêtre Certificats racine de confiance. Dans cette fenêtre, vous pouvez configurer une liste de certificats racine que Kaspersky Endpoint Security considérera comme fiables lors de l'analyse des connexions chiffrées.

Paramètre	Description
Exclusions de l'interception du trafic	Le groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions de l'interception du trafic**. Dans cette fenêtre, vous pouvez configurer les paramètres des connexions dont l'application exclut le trafic de l'interception.
Paramètres des ports réseau	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Ports contrôlés**.
Paramètres avancés	Le groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Mode d'interception du trafic**. Dans cette fenêtre, vous pouvez configurer le mode d'interception du trafic utilisé par l'application : • **Utiliser la technologie eBPF**. si cette option est sélectionnée, l'application utilise la technologie eBPF pour intercepter le trafic. • **Utiliser l'utilitaire iptables** (valeur par défaut). Si cette option est sélectionnée, l'application utilise l'utilitaire iptables pour intercepter le trafic. Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.

Fenêtre Domaines de confiance

Cette liste contient les noms de domaine et les masques de nom de domaine qui seront exclus de l'analyse. L'application n'analyse pas les connexions établies lors de la visite de domaines spécifiés.

Exemple : `*example.com`. Par exemple, `*example.com/*` n'est pas une valeur valide car elle nécessite une adresse de domaine et non une page Internet.

Par défaut, la liste est vide. Vous pouvez ajouter, modifier et supprimer des domaines dans la liste des domaines de confiance.

Fenêtre Certificats de confiance

Vous pouvez configurer la liste des certificats racines que l'application Kaspersky Endpoint Security considérera comme fiables. La liste des certificats racine de confiance est utilisée lors de l'analyse des connexions chiffrées.

Les informations suivantes sont affichées pour chaque certificat :

- Objet du certificat
- Numéro de série du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- empreinte digitale du certificat SHA256.

Par défaut, la liste des certificats est vide.

Vous pouvez ajouter et supprimer des certificats.

Cliquer sur le bouton **Ajouter** ouvre une fenêtre permettant d'ajouter un certificat à la liste des certificats de confiance de l'une des manières suivantes :

- Spécifier le chemin d'accès au fichier de certificat. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Spécifiez le chemin d'accès au fichier au format DER ou PEM contenant le certificat.
- Copiez le contenu du fichier de certificat dans le champ **Saisir les détails du certificat**.

Fenêtre Exclusions de l'interception du trafic

Le tableau contient les paramètres de connexion que l'application exclut de l'interception du trafic :

- **Adresse IP à distance** : l'adresse IP vers laquelle ou depuis laquelle le trafic est exclu de l'interception (selon la direction du trafic).
- **Port de destination** : un port sur un appareil protégé (exclu de l'interception du trafic entrant) ou un port sur un appareil à distance (exclu de l'interception du trafic sortant).
- **Direction du trafic** : la direction du trafic dans la connexion : entrant ou sortant.

Vous pouvez ajouter, modifier et supprimer des exclusions.

Fenêtre Exclusion de l'interception du trafic

Dans cette fenêtre, vous pouvez ajouter une exclusion à l'interception du trafic. Pour ce faire, vous devez spécifier les paramètres de connexion suivants :

- **Adresse IP à distance** : l'adresse de l'appareil à distance au format IPv4 ou IPv6. Selon le sens du trafic, le trafic provenant de l'adresse IP spécifiée (exclusion du trafic entrant) ou le trafic vers l'adresse IP spécifiée (exclusion de trafic sortant) sera exclu.
- **Port de destination** : selon la direction de circulation :
  - Port sur l'appareil protégé (sauf pour le trafic entrant). Le trafic vers ce port provenant des appareils à distance sera exclu de l'interception.
  - Port sur l'appareil à distance (sauf pour le trafic sortant). Le trafic vers ce port provenant de l'appareil protégé sera exclu de l'interception.
- **Direction du trafic** : la direction du trafic dans la connexion exclue. Vous pouvez configurer une exclusion pour le trafic entrant ou pour le trafic sortant.

Fenêtre Ports contrôlés

Paramètres des ports réseau

Paramètre	Description
Surveiller tous les ports réseau	Si cette option est sélectionnée, l'application surveille tous les ports réseau.
Contrôler uniquement les ports réseau sélectionnés	Si cette option est sélectionnée, l'application surveille uniquement les ports réseau renseignés dans le tableau. Cette option est sélectionnée par défaut.
Paramètres des ports réseau	Le tableau contient les ports réseaux que l'application contrôlera quand l'option **Contrôler uniquement les ports indiqués** est sélectionnée. Le tableau contient deux colonnes : • **Port** : le port contrôlé. • **Description** : description du port contrôlé. Par défaut, le tableau affiche une liste des ports réseau normalement utilisés pour la transmission des emails et du trafic réseau. Cette liste de ports réseau est incluse dans le paquet de l'application. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Configuration de l'analyse du trafic réseau dans la ligne de commande

La ligne de commande fournit des commandes de gestion spéciales pour gérer les paramètres d'analyse du trafic réseau. À l'aide des commandes de gestion des paramètres d'analyse du trafic réseau, vous pouvez :

- Configurer les paramètres d'analyse du trafic réseau.
- Afficher les exclusions depuis l'analyse des connexions chiffrées.
- Effacer la liste des domaines que l'application a automatiquement exclus de l'analyse.
- Configurer la liste des certificats racines de confiance que l'application utilise lors de la vérification des connexions chiffrées.
- Configurer et consulter les exclusions de l'interception du trafic.

Affichage et modification des paramètres de vérification du trafic réseau

À l'aide des commandes spéciales de gestion des paramètres d'analyse du trafic réseau, vous pouvez :

- Afficher les valeurs actuelles des paramètres d'analyse du trafic réseau vers la console ou vers un fichier de configuration. Vous pouvez utiliser ce fichier pour modifier les paramètres.
- Modifier tous les paramètres d'analyse du trafic réseau à l'aide du fichier de configuration. Vous pouvez obtenir le fichier de configuration à l'aide de la commande d'affichage des paramètres d'analyse du trafic réseau.
- Modifiez les paramètres individuels à l'aide d'options de ligne de commande au format `< nom du paramètre >= < valeur du paramètre >`. Vous pouvez obtenir les valeurs actuelles des paramètres à l'aide de la commande pour afficher les paramètres d'analyse du trafic réseau.

Pour afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à la console, exécutez la commande suivante :

```
kesl-control --get-net-settings [--json]
```

où `--json` est spécifié pour afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à un fichier, exécutez la commande suivante :

```
kesl-control --get-net-settings --file < chemin d'accès au fichier de configuration > [--
json]
```

où :

- `--file < chemin d'accès au fichier de configuration >` est le chemin d'accès au fichier de configuration dans lequel vous souhaitez enregistrer les paramètres d'analyse du trafic réseau. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Pour modifier les valeurs des paramètres d'analyse du trafic réseau à l'aide d'un fichier de configuration :

1. Générez les paramètres de l'analyse du trafic réseau dans le fichier de configuration comme décrit ci-dessus.
2. Modifiez les valeurs des paramètres requis dans le fichier et enregistrez les modifications.
3. Exécutez la commande :

   ```
   kesl-control --set-net-settings --file < chemin d'accès au fichier de configuration > [-
   -json]
   ```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration contenant les paramètres d'analyse du trafic réseau.
- `--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Toutes les valeurs des paramètres d'analyse du trafic réseau spécifiées dans le fichier seront importées dans l'application.

Pour modifier les paramètres d'analyse du trafic réseau à l'aide de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-net-settings <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

où `<nom du paramètre>=<valeur du paramètre>` correspond au nom et à la valeur de l'un des paramètres d'analyse du trafic réseau.

Les valeurs des paramètres spécifiés seront modifiées.

Affichage des exclusions liées à l'analyse des connexions chiffrées

Vous pouvez afficher les listes suivantes d'exclusions à l'analyse des connexions chiffrées :

- liste des exclusions ajoutées par l'utilisateur ;
- liste des exclusions ajoutées par l'application ;
- une liste des exclusions reçues des bases de données de l'application.

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées qui ont été ajoutées par une application, exécutez la commande suivante :

```
kesl-control -N --query user
```

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées qui ont été ajoutées par une application, exécutez la commande suivante :

```
kesl-control -N --query auto
```

Pour consulter la liste des exclusions de l'analyse des connexions chiffrées reçues des bases de données de l'application, exécutez la commande suivante :

```
kesl-control -N --query kl
```

Pour effacer une liste de domaines que l'application a automatiquement exclus d'une analyse, exécutez la commande suivante :

```
kesl-control [-N] --clear-web-auto-excluded
```

Gestion de la liste des certificats racines de confiance

Pour ajouter un certificat à la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --add-certificate <chemin d'accès au certificat>
```

où :

`<chemin d'accès au certificat>` est le chemin d'accès au fichier de certificat que vous voulez ajouter (au format PEM ou DER).

Pour supprimer un certificat de la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --remove-certificate <objet du certificat>
```

Pour consulter la liste des certificats racines de confiance, exécutez la commande suivante :

```
kesl-control --list-certificates
```

Les informations suivantes sont affichées pour chaque certificat :

- Objet du certificat
- numéro de série du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- empreinte digitale du certificat SHA256.

Configuration et affichage des exclusions à l'interception du trafic

Pour ajouter une exclusion à l'interception du trafic, exécutez la commande :

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <adresse IP distante> --dst-port <port de destination>
```

où :

- `<in|out>` correspond au sens du trafic dans la connexion exclue. Vous pouvez configurer une exclusion pour le trafic entrant ou pour le trafic sortant.
- `< adresse IP distante >` est l'adresse IPv4 ou IPv6 de l'appareil distant. Selon le sens du trafic, le trafic provenant de l'adresse IP spécifiée (exclusion du trafic entrant) ou le trafic vers l'adresse IP spécifiée (exclusion de trafic sortant) sera exclu.
- `< port de destination >`, selon le sens du trafic :
  - Port sur l'appareil protégé (sauf pour le trafic entrant). Le trafic vers ce port provenant des appareils à distance sera exclu de l'interception.
  - Port sur l'appareil à distance (sauf pour le trafic sortant). Le trafic vers ce port provenant de l'appareil protégé sera exclu de l'interception.

Vous pouvez spécifier uniquement l'adresse IP de l'appareil à distance ou uniquement le port de destination dans l'exclusion.

Si vous spécifiez uniquement l'adresse IP de l'appareil à distance (sans spécifier le port sur l'appareil protégé) dans l'exclusion pour le trafic entrant, tout le trafic provenant de l'appareil à distance est exclu de l'interception. Il est recommandé de configurer une telle exclusion uniquement pour le trafic provenant d'appareils auxquels vous faites confiance.

Pour afficher la liste des exclusions configurées à partir de l'interception du trafic, exécutez la commande :

```
kesl-control --list-bypass-endpoints
```

Les informations suivantes sont affichées pour chaque exclusion :

- numéro de série de l'exclusion ;
- direction de circulation dans la connexion ;
- Adresse IP de l'appareil à distance ;
- numéro de port.

Pour supprimer l'exclusion à l'interception du trafic, exécutez la commande :

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip < adresse IP
distante > --dst-port < port de destination >
```

où :

- `<in|out>` correspond au sens du trafic dans la connexion exclue.
- `< adresse IP distante >` est l'adresse IPv4 ou IPv6 de l'appareil distant dont le trafic est exclu de l'interception (selon le sens du trafic).
- `< port de destination >` est un port de l'appareil protégé (exclusion pour le trafic entrant) ou un port de l'appareil distant (exclusion pour le trafic sortant).

Exclusions à l'interception du trafic par le système d'exploitation

Dans les paramètres de l'application Kaspersky Endpoint Security, vous pouvez configurer des exclusions de l'interception du trafic en fonction de sa direction, de l'adresse IP et du port de destination. Si ces exclusions ne permettent pas de résoudre un conflit de communication réseau entre Kaspersky Endpoint Security et les applications client, vous pouvez utiliser la chaîne de règles spéciale kesl_bypass.

Cette chaîne est une liste de règles que Kaspersky Endpoint Security crée dans le tableau mangle du pare-feu du système d'exploitation (iptables/ip6tables). Les règles de la chaîne kesl_bypass permettent d'empêcher l'interception du trafic par l'application Kaspersky Endpoint Security. La chaîne kesl_bypass est ajoutée en premier lors du traitement des paquets réseau ; par conséquent, les règles kesl_bypass sont traitées avant toutes les autres règles iptables.

Si l'application utilise la technologie eBPF pour intercepter le trafic, les règles kesl_bypass ne sont pas appliquées.

Contrairement aux exclusions, que vous pouvez configurer dans les paramètres de Kaspersky Endpoint Security, la chaîne kesl_bypass vous permet de configurer des exclusions non seulement par direction du trafic, adresse IP et port de destination, mais aussi en utilisant d'autres paramètres de connexion.

La modification des règles de la chaîne kesl_bypass s'opère à l'aide des outils du système d'exploitation.

Par exemple, vous pouvez ajouter une règle à la chaîne kesl_bypass en exécutant la commande suivante : `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Cette règle empêche Kaspersky Endpoint Security d'intercepter le trafic HTTP entrant et sortant sur le port 80 et pour toute adresse IP. Cela permet d'éviter d'éventuels conflits avec les services web de confiance.

Si des règles d'exclusion de trafic sont configurées dans la chaîne, elles affectent le fonctionnement des modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet.

Lors de la suppression de l'application, la chaîne de règles kesl_bypass dans iptables et ip6tables est supprimée uniquement si elle était vide.

Protection contre les menaces réseau

Le module Protection contre les menaces réseau vous permet d'analyser le trafic réseau entrant à la recherche d'actions typiques des attaques réseau.

L'application analyse le trafic entrant pour les ports TCP dont l'application Kaspersky Endpoint Security obtient le numéro dans les bases de l'application à jour. La Protection contre les menaces réseau utilise le port 9789 pour intercepter les connexions.

Pour vérifier le trafic réseau, le module Protection contre les menaces réseau accepte les connexions sur tous les ports dont les numéros lui sont communiqués par les bases de données de l'application. Lors du contrôle du réseau, un port peut sembler ouvert sur l'appareil, même si aucune application du système ne l'écoute. Il est recommandé de fermer les ports non utilisés à l'aide d'un pare-feu.

Les connexions actuelles pour les ports TCP interceptés sont réinitialisées lorsque la protection contre les menaces réseau est activée.

Si la protection contre les menaces réseau est activée, lorsqu'une tentative d'attaque réseau sur un appareil protégé est détectée, l'application bloque l'activité réseau de l'appareil attaquant et génère un événement *Attaque réseau détectée*. L'événement contient des informations sur l'appareil attaquant. Par défaut, le trafic réseau provenant de l'appareil attaquant est bloqué pendant une heure. Une fois le délai de blocage expiré, l'application débloque l'appareil.

Par défaut, la Protection contre les menaces réseau est désactivée.

Vous pouvez activer et désactiver la protection contre les menaces réseau, ainsi que configurer les paramètres de protection :

- Sélectionner l'action que l'application entreprendra lorsqu'elle détectera une activité réseau typique des attaques réseau.
- Activer ou désactiver le blocage de l'activité réseau en cas de détection d'une tentative d'attaque réseau.
- Définir la durée de blocage de l'appareil attaquant.
- Configurer une liste d'adresses IP dont l'activité réseau n'est pas bloquée par l'application.

À l'aide des commandes de gestion des appareils verrouillés dans la ligne de commande, vous pouvez afficher une liste des appareils verrouillés et déverrouiller manuellement ces appareils. Kaspersky Security Center ne dispose pas d'outils de surveillance et d'administration des appareils bloqués, à l'exclusion des événements *Attaque réseau détectée*.

Si vous avez configuré des exclusions de l'interception du trafic par l'application Kaspersky Endpoint Security, elles affectent le fonctionnement du module Protection contre les menaces réseau.

Configuration de la protection contre les menaces réseau dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de la Protection contre les menaces réseau dans les propriétés de la stratégie (**Paramètres de l'application** → **Communication et protection Internet** → **Protection contre les menaces réseau**).

Configuration de la protection contre les menaces réseau dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces réseau dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale** → **Protection contre les menaces réseau**).

Paramètres du module Protection contre les menaces réseau

Paramètre	Description
Activer la Protection contre les menaces réseau	La case active ou désactive la Protection contre les menaces réseau. La case est décochée par défaut.
Action en cas de détection d'une menace	Actions à entreprendre en cas de détection d'une activité réseau caractéristique des attaques réseau : • **Informer** l'utilisateur. L'application autorise l'activité réseau, consigne dans le journal les informations sur l'activité réseau détectée. • **Bloquer** l'activité réseau de l'appareil attaquant et consigner les informations sur l'activité réseau détectée (valeur par défaut) dans le journal.
Bloquer les hôtes attaquants	La case active ou désactive le blocage de l'activité réseau en cas de détection d'une tentative d'attaque réseau. La case est cochée par défaut.
Bloquer l'hôte attaquant pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un appareil attaquant (en minutes). Une fois le délai spécifié écoulé, l'application Kaspersky Endpoint Security autorise l'activité réseau en provenance de cet appareil. Valeurs disponibles : entier de 1 à 32768. Valeur par défaut : 60.
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**, qui ouvre la fenêtre **Exclusions**, dans laquelle vous pouvez spécifier une liste d'adresses IP. Les attaques réseau provenant de ces adresses IP ne seront pas bloquées.

Fenêtre Exclusions

Cette fenêtre permet d'ajouter les adresses IP qui ne seront pas bloquées en cas d'attaques réseau.

Par défaut, la liste est vide.

Vous pouvez ajouter, modifier et supprimer des adresses IP dans la liste. Vous pouvez spécifier des adresses IP aux formats IPv4 et IPv6.

Configuration de la Protection contre les menaces réseau sur la ligne de commande

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces réseau à l'aide de la tâche prédéfinie Protection contre les menaces réseau (*Network_Threat_Protection*).

Par défaut, la tâche de protection contre les menaces réseau n'est pas lancée. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la protection contre les menaces réseau en modifiant les paramètres de la tâche prédéfinie Protection contre les menaces réseau.

Paramètres de la tâche de protection contre les menaces réseau

Paramètre	Description	Valeurs
`ActionOnDetect`	Action exécutée en cas de détection d'une activité réseau caractéristique des attaques réseau. La modification de ce paramètre de `Block` à `Notify` efface la liste des appareils bloqués.	`Notify` : autorise l'activité réseau, consigne dans le journal les informations sur l'activité réseau détectée. Si cette valeur est spécifiée, la valeur du paramètre `BlockAttackingHosts` est ignorée. `Block` (valeur par défaut) : bloquer l'activité réseau et consigne dans le journal les informations la concernant.
`BlockAttackingHosts`	Blocage de l'activité réseau à partir des appareils attaquants.	`Yes` (valeur par défaut) : bloquer l'activité réseau de l'appareil attaquant. `No` – ne pas bloquer l'activité réseau de l'appareil attaquant. Si cette valeur est spécifiée et que le paramètre `ActionOnDetect` est défini sur `Block`, l'application bloque l'activité réseau de l'appareil attaquant, mais n'ajoute pas l'appareil à la liste des appareils bloqués.
`BlockDurationMinutes`	Spécifie la durée de blocage des attaques contre les appareils (en minutes).	1 – 32768 Valeur par défaut : 60.
`UseExcludeIPs`	Utilisation d'une liste d'adresses IP dont l'activité réseau ne sera pas bloquée en cas de détection d'une attaque réseau. L'application enregistrera dans le journal uniquement les informations sur les activités malveillante de ces applications. Vous pouvez ajouter des adresses IP à la liste d'exclusion à l'aide du paramètre `ExcludeIPs.item_#`.	`Yes` : utilise une liste d'exclusion d'adresses IP. `No` : (valeur par défaut) : n'utilise pas de liste d'exclusion d'adresses IP.
`ExcludeIPs.item_#`	Spécifie une adresse IP dont l'activité réseau ne sera pas bloquée par l'application. Par défaut, la liste est vide.	`d.d.d.d` : adresse IPv4 où d est un nombre décimal compris entre 0 et 255. `d.d.d.d/p` : sous-réseau d'adresses IPv4 où p est un nombre compris entre 0 et 32. `x:x:x:x:x:x:x:x` : adresses IPv6, où x est un nombre hexadécimal compris entre 0 et ffff. `x:x:x:x::0/p` : sous-réseau d'adresses IPv6 où p est un nombre compris entre 0 et 64. La valeur par défaut n'est pas définie.

Protection contre les menaces par emails

La Protection contre les menaces par emails analyse les pièces jointes des messages entrants et sortants à la recherche de virus et d'autres pièces jointes malveillantes. Ce module protège votre appareil grâce aux bases antivirus, au service Kaspersky Security Network et à 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 et IMAP dans tous les clients de messagerie et les versions étendues de protocole (POP3S, SMTPS et IMAPS) dans les clients de messagerie MyOffice Mail et P7-Office Organizer. La Protection contre les menaces par emails ne prend pas en charge d'autres protocoles.

Pour que la Protection contre les menaces par emails fonctionne, les ports réseau 25, 465, 587, 110, 995, 143 et 993 doivent être surveillés dans les paramètres réseau. Ces ports sont ajoutés par défaut à la liste des ports surveillés. Leur suppression de la liste peut perturber le fonctionnement du module.

Par défaut, le module Protection contre les menaces par emails est activé. Vous pouvez activer, désactiver et configurer les paramètres de Protection contre les menaces par emails via Web Console, la Console d'administration et la ligne de commande.

Configuration de la protection contre les menaces par emails dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de la protection contre les menaces par emails dans les propriétés de la stratégie (**Paramètres de l'application** → **Communication et protection Internet** → **Protection contre les menaces par emails**).

Configuration de la protection contre les menaces par emails dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces par emails dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale** → **Protection contre les menaces par emails**).

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Protection contre les menaces par emails	La case active ou désactive le module Protection contre les menaces par emails. Le module est activé par défaut.
Configurer (Paramètres de la protection)	Cliquer sur le bouton ouvre la fenêtre **Paramètres de la Protection contre les menaces par emails**, où vous pouvez configurer la zone de protection contre les menaces par emails et les paramètres d'analyse des fichiers composés.
Configurer (Filtre de pièces jointes)	Cliquer sur le bouton ouvre la fenêtre **Filtre de pièces jointes**, où vous pouvez configurer le filtrage des pièces jointes de vos emails.

Paramètre	Description
Utiliser l'analyse heuristique **Niveau de l'analyse heuristique**	La case active ou désactive l'utilisation de l'analyseur heuristique. Lors de l'analyse des fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions exécutées dépend du niveau d'analyseur heuristique sélectionné. Celui-ci définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse heuristique. Par défaut, l'analyse heuristique est activée avec le niveau moyen.
Actions en cas de détection d'une menace	Action effectuée par la Protection contre les menaces par emails lorsqu'une menace est détectée dans un email : • **Désinfecter ; supprimer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. Cette action est sélectionnée par défaut. • **Désinfecter ; bloquer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. • **Bloquer**. Si un objet infecté est détecté dans un message entrant, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine.

Fenêtre Paramètres de la protection contre les menaces par emails

Cette fenêtre permet de configurer la zone de protection contre les menaces par emails et les paramètres d'analyse des fichiers composés.

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Zone de protection	*Zone de protection* : les objets que le module vérifie pendant son fonctionnement : messages entrants et sortants ou uniquement messages entrants. Par défaut, l'option **Messages entrants et sortants** est sélectionnée.
Analyser les archives jointes	Active et désactive la vérification des archives jointes. Analyse des 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 l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). La case est cochée par défaut.
Analyser les fichiers joints des applications Office	Active ou désactive la vérification des fichiers joints aux formats Office. L'application analyse les fichiers au format Office de moins de 1 Mo, quel que soit l'état de la case. La case est cochée par défaut.
Ne pas analyser les archives de plus de (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 dépasse celle spécifiée. Si cette case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques. La case est décochée par défaut.
Limiter le temps d'analyse des archives à (sec.)	Si la case est cochée, la durée d'analyse des archives jointes aux messages est limitée à la période spécifiée. La case est décochée par défaut.

Fenêtre Filtre des pièces jointes

Dans cette fenêtre, vous pouvez configurer le filtrage des pièces jointes aux emails.

Paramètres de filtrage des pièces jointes

Paramètre	Description
Ne pas appliquer le filtre	Si cette option est sélectionnée, la Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques.
Renommer les pièces jointes de types spécifiés	Lorsque cette option est sélectionnée, la Protection contre les menaces par emails remplace le dernier caractère de l'extension des fichiers joints des types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir. Sélectionné par défaut.
Supprimer les pièces jointes des types spécifiés	Lorsque cette option est sélectionnée, la Protection contre les menaces par emails supprime les pièces jointes des types de fichiers spécifiés des messages électroniques. Vous pouvez spécifier les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Tableau des types de pièces jointes	Le tableau indique les types de pièces jointes qui doivent être renommées ou supprimées des messages électroniques. Vous pouvez ajouter, modifier et supprimer des types de pièces jointes à l'aide des boutons du même nom.

Configuration de la protection contre les menaces par emails dans la ligne de commande

À partir de la ligne de commande, vous pouvez gérer la protection contre les menaces par emails à l'aide de la tâche prédéfinie Protection contre les menaces par emails (*Mail_Monitoring*).

La tâche Protection contre les menaces par emails est lancée par défaut. Vous pouvez démarrer et arrêter cette tâche manuellement.

Les privilèges du rôle Administrateur sont nécessaires pour arrêter et démarrer la tâche Protection contre les menaces par emails à partir de la ligne de commande.

Vous pouvez configurer les paramètres de la protection contre les menaces par emails en modifiant les paramètres de la tâche prédéfinie Protection contre les menaces par emails.

Le tableau ci-dessous décrit les valeurs disponibles et les valeurs par défaut pour les paramètres que vous pouvez définir pour la tâche Protection contre les menaces par emails.

Paramètres de la tâche Protection contre les menaces par emails

Paramètre	Description	Valeurs
`CheckIncomingMessagesOnly`	*Zone de protection* : les objets que le module vérifie pendant son fonctionnement : messages entrants et sortants ou uniquement messages entrants.	`Yes` : l'application vérifie uniquement les messages entrants. `No` (par défaut) : l'application vérifie les messages entrants et sortants.
`ScanFileArchive`	Active et désactive la vérification des archives jointes. Analyse des 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 l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive).	`Yes` (par défaut) : l'application analyse les archives jointes. `No` : l'application n'analyse pas les archives jointes.
`ScanFileOffice`	Active ou désactive la vérification des fichiers joints aux formats Office.	`Yes` (par défaut) : l'application analyse les fichiers Office joints. `No` : l'application n'analyse pas les fichiers Office joints.
`UseSizeLimit`	Limite la taille des archives jointes analysées.	`Yes` : l'application exclut de l'analyse les archives jointes aux emails dont la taille dépasse la limite spécifiée par l'argument `SizeLimit`. `No` (par défaut) : l'application analyse les archives jointes aux emails, quelle que soit leur taille.
`SizeLimit`	Spécifie la taille maximale des archives jointes analysées.	1 à 9 999 Mo.
`UseTimeLimit`	Limite la durée maximale d'analyse des archives jointes.	`Yes` : l'application termine l'analyse des archives jointes après le délai spécifié par l'argument `TimeLimit`. `No` (par défaut) : aucune limite de temps n'est appliquée à l'analyse des archives jointes.
`TimeLimit`	Spécifie la durée maximale d'analyse des archives jointes.	1 à 9 999 secondes.
`ExtensionFilter`	Configure le filtrage des pièces jointes.	`Disable` : l'application ne filtre pas les fichiers joints aux emails. `Rename` (par défaut) : l'application remplace le dernier caractère de l'extension des fichiers joints de types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir. `Delete` : l'application supprime les fichiers joints de types spécifiés des emails.

`ExtensionMasks`	Spécifie les extensions des pièces jointes à renommer ou à supprimer des emails.	Une liste d'extensions multiples est spécifiée comme suit :
		`[ExtensionMasks.item_0000]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.txt`
		`[ExtensionMasks.item_0001]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.run`
		`[ExtensionMasks.item_0002]`
		`UseExtensionMask=Yes`
		`ExtensionMask=*.exe`
		`...`
		Par défaut, les fichiers avec les extensions suivantes sont traités : TXT, RUN, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH.
		Pour modifier la liste des extensions, exportez les paramètres de la tâche dans un fichier INI, puis modifiez la liste dans ce fichier et importez le fichier INI dans l'application.

`UseAnalyzer`	Active ou désactive l'utilisation de l'analyseur heuristique.	`Yes` (par défaut) : analyseur heuristique est activé. `No` : analyseur heuristique est désactivé.

Paramètre	Description	Valeurs
`AnalyzerLevel`	Lors de l'analyse des fichiers à la recherche de code malveillant, l'analyseur heuristique exécute des instructions dans les fichiers exécutables. Le nombre d'instructions exécutées dépend du niveau d'analyseur heuristique sélectionné. Celui-ci définit l'équilibre entre la minutie de la recherche de nouvelles menaces, la charge sur les ressources du système d'exploitation et la durée de l'analyse heuristique.	`Light` : analyse la moins complète, charge système minimale. `Medium` (par défaut) : niveau de détail moyen pendant analyse, charge équilibrée sur le système. `Deep` : analyse la plus complète, charge système maximale.
`ActionOnThreat`	L'action que prend la Protection contre les menaces par emails lorsqu'elle détecte une menace dans les messages électroniques entrants. Le paramètre `ActionOnThreat` ne s'applique pas aux messages sortants. Si un objet infecté est détecté dans un message sortant, l'application bloque son envoi.	`DisinfectDeleteIfNotPossible` (par défaut) : désinfecter ; supprimer si la désinfection est impossible. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. Cette action est sélectionnée par défaut. `DisinfectBlockIfNotPossible` : Désinfecter ; bloquer si la désinfection est impossible. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine. `Block` : bloquer Si un objet infecté est détecté dans un message entrant, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès au message avec la pièce jointe d'origine.

Protection BadUSB

Certains virus modifient l'application interne des appareils USB afin que le système d'exploitation considère l'appareil USB comme un clavier. Le virus peut ainsi exécuter des commandes sous votre compte, comme le téléchargement d'un logiciel malveillant.

Le module Protection BadUSB empêche la connexion des appareils USB infectés imitant un clavier.

Lorsqu'un appareil USB détecté comme clavier par le système d'exploitation est connecté, l'application invite l'utilisateur à saisir un code numérique généré par l'application à l'aide du clavier physique ou du clavier virtuel (le cas échéant). C'est ce qu'on appelle l'autorisation du clavier.

Si le code est saisi correctement, l'application enregistre les paramètres d'identification du clavier (VID/PID et numéro de port) 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.

Lorsqu'un clavier autorisé est connecté à un autre port USB de l'appareil, l'application demande à nouveau l'autorisation.

Si le code numérique est saisi incorrectement, l'application en génère un nouveau. Vous pouvez configurer le nombre de tentatives de saisie du code numérique. Si le code numérique est saisi incorrectement à plusieurs reprises ou si la fenêtre d'autorisation de clavier est fermée, l'application bloque la saisie provenant de 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.

Par défaut, le module Protection BadUSB est désactivé. Vous pouvez activer, désactiver et configurer les paramètres de Protection BadUSB via Web Console, la Console d'administration et la ligne de commande.

Configuration de la protection BadUSB dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de la protection BadUSB dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Protection BadUSB**).

Configuration de la protection BadUSB dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les menaces Internet dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection principale** → **Protection BadUSB**).

Paramètres du module Protection BadUSB

Paramètre	Description
Activer la protection BadUSB	La case active ou désactive le module Protection BadUSB. Le module est désactivé par défaut.
Nombre maximal de tentatives d'autorisation de l'appareil USB	Bloque automatiquement un appareil USB si le code d'autorisation est saisi incorrectement un nombre de fois spécifié. 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 affichera la durée de verrouillage de l'appareil USB. Une fois ce délai écoulé, vous disposez encore une fois de cinq tentatives pour saisir le code d'autorisation. Valeur par défaut : 5.
Verrouillage de l'appareil lorsque le nombre maximal de tentatives d'autorisations 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 autorisées vont de 1 à 180 minutes. Valeur par défaut : 5.
Interdire l'utilisation du clavier virtuel pour autoriser les appareils USB	Si la case est cochée, l'application bloque l'utilisation du clavier virtuel pour autoriser l'appareil USB à partir duquel la saisie du code d'autorisation est impossible. La case est décochée par défaut.

Configuration de la protection BadUSB dans la ligne de commande

À partir de la ligne de commande, vous pouvez gérer la protection BadUSB à l'aide de la tâche prédéfinie Protection BadUSB (*Bad_USB*).

La tâche Protection BadUSB n'est pas lancée par défaut. Vous pouvez démarrer et arrêter cette tâche manuellement.

Les privilèges du rôle Administrateur sont nécessaires pour arrêter et démarrer la tâche Protection BadUSB à partir de la ligne de commande.

Vous pouvez configurer les paramètres de la Protection BadUSB en modifiant les paramètres de la tâche prédéfinie Protection BadUSB.

Le tableau ci-dessous décrit les valeurs disponibles et les valeurs par défaut pour les paramètres que vous pouvez définir pour la tâche Protection BadUSB.

Paramètres de la tâche Protection BadUSB

Paramètre	Description	Valeurs
`MaxAuthAttempts`	Le nombre maximal de tentatives d'authentification de l'appareil USB après lesquelles l'application bloque l'appareil USB et toutes les tentatives d'authentification suivantes pendant la durée spécifiée par le paramètre `TimeoutAfterAttempts`.	Valeurs possibles : 1 à 10. Valeur par défaut : 5.
`TimeoutAfterAttempts`	La durée de verrouillage de l'appareil USB après le nombre de tentatives infructueuses de saisie du code d'autorisation défini par le paramètre `MaxAuthAttempts`.	Valeurs possibles : 1 – 180 (min). Valeur par défaut : 5 minutes.
`ProhibitOnScreenKeyboard`	Activation ou désactivation de l'interdiction d'utiliser le clavier virtuel pour l'autorisation de clavier des appareils USB.	`Yes` : l'application interdit l'utilisation du clavier virtuel pour autoriser les appareils USB à partir desquels il est impossible de saisir un code d'autorisation de clavier. `No` (par défaut) : l'application n'interdit pas l'utilisation du clavier virtuel pour autoriser les appareils USB à partir desquels il est impossible de saisir un code d'autorisation de clavier.

Protection contre le chiffrement malveillant à distance

La module Protection contre le chiffrement permet de protéger vos fichiers dans les répertoires locaux accessibles sur le réseau via les protocoles SMB/NFS contre le chiffrement malveillant à distance.

Pour utiliser le module, vous devez posséder la licence qui couvre cette fonction.

Si la protection contre le chiffrement est activée, Kaspersky Endpoint Security vérifie les actions des appareils à distance avec des ressources de fichiers situées dans les répertoires réseau partagés de l'appareil protégé pour détecter la présence d'un chiffrement malveillant. Si une application interprète les actions d'un appareil distant accédant aux partages réseau comme un chiffrement malveillant, l'application crée et active une règle de pare-feu du système d'exploitation qui bloque le trafic réseau provenant de l'appareil compromis. L'appareil compromis est ajouté à la liste des appareils non fiables et l'accès aux répertoires réseau partagés pour tous les appareils non fiables est bloqué. L'application génère un événement *Chiffrement détecté*, qui contient des informations sur l'appareil compromis.

Par défaut, l'application bloque l'accès des hôtes douteux aux ressources de fichier réseau pendant 30 minutes. Une fois le délai de blocage expiré, l'application supprime l'appareil compromis de la liste des appareils non fiables et l'accès de l'appareil aux ressources de fichiers réseau est automatiquement restauré.

Les règles de pare-feu créées par le module Protection contre le chiffrement ne peuvent pas être supprimées à l'aide de l'utilitaire iptables, car l'application restaure l'ensemble des règles toutes les minutes.

Par défaut, la protection contre le chiffrement malveillant à distance est désactivée.

Vous pouvez activer ou désactiver la protection contre le chiffrement malveillant, et également configurer les paramètres de la protection :

- Choisissez l'action que l'application entreprendra lorsque le chiffrement sera détecté : informer l'utilisateur ou bloquer l'appareil effectuant un chiffrement malveillant.

  Si l'action *Informer* est sélectionné, l'application analyse malgré tout les actions des appareils distants sur les ressources de fichiers réseau afin d'identifier d'éventuels chiffrements malveillants lorsque la protection contre le chiffrement est activée. Si un chiffrement malveillant est détecté, un événement *Chiffrement détecté* est généré, mais l'appareil compromis n'est pas bloqué.

- Définir la durée de blocage d'un appareil non fiable.

- Spécifiez les fichiers et répertoires que l'application protège contre le chiffrement malveillant.

- Spécifiez les fichiers et répertoires qui sont exclus de la protection contre le chiffrement malveillant.

  L'application ne considère pas les actions comme du chiffrement si une activité de chiffrement est détectée dans des répertoires exclus de la protection contre le chiffrement.

À l'aide des commandes de gestion des appareils verrouillés dans la ligne de commande, vous pouvez afficher une liste des appareils verrouillés et déverrouiller manuellement ces appareils. Kaspersky Security Center ne dispose pas d'outils de surveillance et de gestion des appareils bloqués, à l'exclusion des événements *Chiffrement détecté*.

Pour que le module Protection contre le chiffrement fonctionne correctement, il faut installer au moins un des services suivants dans le système d'exploitation : Samba ou NFS. Pour le service NFS, le paquet rpcbind doit être installé.

Le module Protection contre le chiffrement fonctionne sans problème avec les protocoles SMB1, SMB2, SMB3, NFS3, TCP / UDP et IP / IPv6. Les protocoles NFS2 et NFS4 ne sont pas pris en charge. Il est conseillé de configurer le serveur de telle sorte que les protocoles NFS2 et NFS4 ne puissent pas être utilisés pour monter des ressources.

L'application Kaspersky Endpoint Security ne bloque pas l'accès aux ressources de fichiers réseau tant que les actions de l'appareil n'ont pas été considérées comme malveillantes. Autrement dit, au moins un fichier doit être chiffré avant que l'application ne détecte une activité malveillante.

Configuration de la protection contre le chiffrement dans Web Console

Dans Web Console, vous pouvez gérer les paramètres de la Protection contre le chiffrement dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre le chiffrement**).

Configuration de la protection contre le chiffrement dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre le chiffrement dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection avancée** → **Protection contre le chiffrement**).

Paramètres du module Protection contre le chiffrement

Paramètre	Description
Activer la protection contre le chiffrement	La case active ou désactive la protection des fichiers des répertoires locaux avec accès réseau par protocoles SMB/NFS contre le chiffrement à distance malveillant. La case est décochée par défaut.
Zones de protection	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration de la zone d'analyse et des paramètres de la protection.
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets de l'analyse sur la base d'un masque de nom.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone d'analyse

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Dans cette fenêtre, vous pouvez ajouter ou configurer la zone de protection du module Protection contre le chiffrement.

Paramètres de la zone de protection

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone de protection. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application traite cette zone de protection pendant le fonctionnement du module. Si cette case est décochée, l'application ne traite pas cette zone de protection pendant le fonctionnement du module. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement du module en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'analyse. Cette liste déroulante des fichiers système permet de sélectionner le type de système de fichiers : • **Local** : répertoires locaux. • **Partagé** affiche les ressources du système de fichiers du serveur accessibles via le protocole Samba ou NFS. • **Tous les éléments partagés** (valeur par défaut) : affiche les ressources du système de fichiers du serveur accessibles via les protocoles Samba et NFS.
	Si **Partagé** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez inclure dans la zone de protection. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide.
Masques	La liste contient les masques des noms des objets analysés par l'application pendant le fonctionnement du module Protection contre le chiffrement. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Paramètres de la protection

Paramètres de la protection

Paramètre	Description
Action en cas de détection d'un chiffrement	Action que Kaspersky Endpoint Security effectuera lorsqu'un chiffrement malveillant est détecté : • **Informer** l'utilisateur. Kaspersky Endpoint Security ne bloque pas l'appareil effectuant le chiffrement ; il enregistre uniquement l'événement de détection d'un chiffrement malveillant dans le journal des événements. • **Bloquer** l'appareil effectuant le chiffrement (par défaut).
Bloquer un appareil douteux pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un appareil douteux (en minutes). À l'expiration du délai indiqué, l'application Kaspersky Endpoint Security retire les hôtes douteux de la liste des appareils bloqués. L'accès de l'hôte aux ressources de fichier réseau est automatiquement restauré une fois qu'il a été supprimé de la liste d'hôtes douteux. Si un hôte compromis est bloqué et si vous modifiez cette valeur de paramètre, la durée de blocage de cet hôte ne change pas. La durée de blocage n'est pas une valeur dynamique et se calcule au moment du blocage. Valeurs disponibles : entier de 1 à 2147483647. Valeur par défaut : 30.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion de l'analyse.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone d'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone de l'analyse pendant son fonctionnement. Si la case est cochée, l'application inclut cette zone dans l'analyse pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres permet de définir la zone d'exclusion. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires exclus de l'analyse : • **Local** : répertoires locaux. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers de l'appareil indiquées dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au répertoire que vous souhaitez ajouter à la zone d'exclusion. Vous pouvez utiliser des **masques** et des **tags** pour spécifier le chemin. Vous pouvez utiliser des tags spéciaux pour spécifier un conteneur ou une image : • `[container-id:<id>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<id>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` Où : `<id>` est l'ID du conteneur. `<name>` est le nom du conteneur `<path to local directory>` est le chemin d'accès au répertoire local. Vous pouvez également utiliser des combinaisons uniques de tags : `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]` et `[image-name:<name>]/path to local directory>`. Toute combinaison de tags uniques de 1 à 4 dans une même zone est possible. L'ordre de liste n'a pas d'importance. Par exemple : • `[container-name:<name>][image-name:<name>]/path to local directory>` • `[container-id:<id>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<id>]/<path to local directory>` • `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>` Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et les identifiants. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.

Paramètre	Description
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter à la zone d'exclusion. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Les masques sont appliqués aux objets uniquement à l'intérieur du répertoire indiqué dans le champ de saisie du chemin. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Configuration de la Protection contre le chiffrement sur la ligne de commande

Depuis la ligne de commande, vous pouvez gérer la protection contre le chiffrement à l'aide de la tâche Protection contre le chiffrement (*Anti_Cryptor*).

Par défaut, la tâche Protection contre le chiffrement n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres de protection contre le chiffrement en modifiant les paramètres de la tâche prédéfinie de protection contre le chiffrement.

Paramètres de la tache de Protection contre le chiffrement

Paramètre	Description	Valeurs
`ActionOnDetect`	Active les blocages des appareils douteux.	`Block` (valeur par défaut) : active le blocage des hôtes douteux. `Notify` : désactiver le blocage des appareils douteux.
`BlockTime`	Durée de blocage d'un appareil non fiable en minutes. Si un appareil compromis est bloqué et si vous modifiez la valeur du paramètre `BlockTime`, la durée de blocage de cet appareil ne change pas. La durée de blocage n'est pas une valeur dynamique et se calcule au moment du blocage.	Entier entre 1 et 4294967295. Valeur par défaut : 30.
`UseExcludeMasks`	Active l'exclusion, de la zone de protection, des objets définis à l'aide du paramètre `ExcludeMasks.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de protection les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de protection les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion, de la zone de protection, des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone de protection indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Si vous souhaitez définir plusieurs masques, indiquez chaque masque sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.
La section **[ScanScope.item_#]** contient les zones protégées par l'application. Pour la tâche Protection contre le chiffrement, il faut indiquer au moins une zone de protection. Seuls les répertoires partagés peuvent être indiqués. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de protection contient des informations complémentaires sur la zone de protection.	Valeur par défaut : `All shared directories`.
`UseScanArea`	Active la protection de la zone définie. Pour exécuter la tâche, il faut inclure au moins une zone de protection.	`Yes` (valeur par défaut) : protège la zone définie. `No` : ne protège pas une zone définie.
`AreaMask.item_#`	Restriction de la zone de protection. Dans la zone de protection, l'application protège uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (protéger tous les objets)

Paramètre	Description	Valeurs
`Path`	Chemin d'accès au répertoire contenant les objets protégés.	`< chemin d'accès au répertoire local >` — Protéger un répertoire local accessible via SMB/NFS. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. `AllShared` (valeur par défaut) : protège toutes les ressources partagées via SMB/NFS. `Shared:SMB` — Protéger les ressources accessibles via SMB. `Shared:NFS` — Protéger les ressources accessibles via NFS.
La section **[ExcludedFromScanScope.item_#]** contient les objets à exclure de toutes les sections [ScanScope.item_#]. Les objets qui satisfont aux règles de n'importe quelle section [ExcludedFromScanScope.item_#] ne sont pas analysés. Le format d'une section [ExcludedFromScanScope.item_#] est identique au format d'une section [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion de la protection contient des informations complémentaires sur la zone d'exclusion.	Valeur par défaut : `All objects`.
`UseScanArea`	Exclusion de la zone de protection indiquée.	`Yes` (valeur par défaut) : exclut une zone définie de la protection. `No` : n'exclut pas la zone définie de la protection.
`AreaMask.item_#`	Restriction de la zone d'exclusion de la protection. Dans la zone d'exclusion, l'application exclut uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets).

Paramètre	Description	Valeurs
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la protection.	`< chemin d'accès au répertoire local >` — Exclure de la protection les objets du répertoire indiqué. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. `Mounted:NFS` : exclure de la protection les répertoires distants montés sur l'appareil client via le protocole NFS. `Mounted:SMB` : exclure de la protection les répertoires distants montés sur l'appareil client via le protocole Samba. `AllRemoteMounted` : exclut de la protection tous les répertoires distants montés sur l'appareil distant via les protocoles Samba et NFS.

Gestion des appareils bloqués

Tout en protégeant un appareil contre les menaces réseau et contre le chiffrement malveillant à distance, Kaspersky Endpoint Security peut bloquer les appareils distants dont les actions sont considérées comme malveillantes :

- Si un chiffrement malveillant est détecté, l'application bloque l'accès de l'appareil distant aux répertoires réseau partagés de l'appareil protégé.
- Lorsqu'une tentative d'attaque réseau sur un appareil protégé est détectée, l'application bloque le trafic réseau provenant de l'appareil attaquant.

Vous pouvez modifier la durée de blocage dans les paramètres de protection contre les menaces réseau et protection contre le chiffrement malveillant à distance. Après la période spécifiée, l'application débloquera l'appareil.

Si vous gérez une application à l'aide de la ligne de commande, vous pouvez utiliser les commandes d'administration des appareils verrouillés pour afficher une liste des appareils verrouillés suite à l'exécution de l'application sur l'appareil et déverrouiller manuellement ces appareils avant l'expiration du délai de verrouillage. Kaspersky Security Center ne dispose pas d'outils de surveillance et d'administration des appareils bloqués, à l'exclusion des événements *Attaque réseau détectée* et *Chiffrement détecté*.

Pour consulter la liste des appareils bloqués, exécutez la commande suivante :

```
kesl-control --get-blocked-hosts
```

À la suite de l'exécution de la commande, l'application affiche une liste des appareils bloqués sur la console.

Pour débloquer des appareils, saisissez la commande suivante :

```
kesl-control --allow-hosts <adresse>
```

où `<adresse>` correspond à une ou plusieurs adresses IP des appareils ou des sous-réseaux (IPv4/IPv6, y compris les adresses abrégées). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

À la suite de l'exécution de la commande, l'application débloque les appareils spécifiés.

Exemples :
Adresses IPv4 :
```
dec - 192.168.0.1
dec - 192.168.0.0/24
```
Adresses IPv6 :
```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

Contrôle des applications

Le module Contrôle des applications permet de contrôler le lancement des applications sur les appareils protégés. Le contrôle des applications réduit le risque d'infection des appareils en limitant l'accès des utilisateurs aux applications. Vous pouvez obtenir des informations sur les applications installées sur les appareils protégés à l'aide de la tâche Inventaire.

Pour utiliser le module, vous devez posséder la licence qui couvre cette fonction.

Les *règles du Contrôle des applications* sont les éléments qui permettent de régir le lancement des applications.

Le module Contrôle des applications peut fonctionner dans l'un des deux modes suivants :

- *Liste de refus*. Dans ce mode, l'application Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. Par défaut, le module Contrôle des applications fonctionne dans ce mode.

- *Liste d'autorisation*. Dans ce mode, l'application Kaspersky Endpoint Security interdit à tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.

En cas d'application de règles du Contrôle des applications les plus complètes, Kaspersky Endpoint Security interdit le lancement de toute nouvelle application que l'administrateur du réseau local de l'organisation n'a pas encore vérifiée, mais elle garantit le fonctionnement du système d'exploitation et des applications vérifiées dont l'utilisateur a besoin pour remplir ses fonctions.

L'administrateur de Kaspersky Security Center ou un utilisateur local avec le rôle admin attribué dans l'application peut interdire ou autoriser l'exécution de processus sous le compte root à l'aide de Contrôle des applications.

Par défaut, le contrôle des applications est désactivé. Vous pouvez activer ou désactiver le Contrôle des applications, ainsi que configurer les paramètres de fonctionnement du module :

- Sélectionner le mode du module Contrôle des applications : la *liste des autorisés* ou la *liste des bloqués*.

- Créer des règles de Contrôle des applications pour chaque mode du module.

- Sélectionner l'action que l'application Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles. Kaspersky Endpoint Security peut *appliquer des règles* et exécuter les actions spécifiées dans les règles, ou *tester les règles* et informer uniquement d'une tentative de lancement d'une application qui satisfait aux règles.

- Exporter et importer les paramètres configurés du Contrôle des applications.

Le Contrôle des applications ne prend pas en charge le contrôle de lancement des applications Snap, Flatpak et AppImage.

Contrôle des applications ne contrôle pas le lancement des scripts depuis des interprètes qui ne sont pas compatibles avec Kaspersky Endpoint Security, ni le lancement des scripts transmis à l'interprète par une méthode autre que la ligne de commande. Kaspersky Endpoint Security prend en charge les interprètes suivants : python, perl, bash, ssh.

Si les règles du Contrôle des applications autorise le lancement de l'interprète, Kaspersky Endpoint Security ne bloque pas le script lancé depuis cet interprète. Si les règles du Contrôle des applications interdisent le lancement d'au moins un des scripts indiqués dans la ligne de commande de l'interprète, alors Kaspersky Endpoint Security interdit tous les scripts repris dans la ligne de commande de l'interprète. Exclusion : cat script.py | python.

À propos des règles du contrôle des applications

Une règle de contrôle des applications est un ensemble de paramètres qui contiennent les conditions de déclenchement de la règle et les actions du module Contrôle des applications lorsque la règle est déclenchée (autorisant ou interdisant aux utilisateurs de lancer l'application) :

- Application appartenant à la catégorie application. Une *catégorie d'applications* est un groupe d'applications qui ont quelque chose en commun. Il peut s'agir, par exemple, d'une catégorie qui reprend les fichiers exécutables des applications installées ou les applications indispensables au travail, comme peuvent l'être les applications standard que les entreprises utilisent. Vous ne pouvez utiliser une catégorie dans une seule règle.

  L'utilisation des catégories KL de l'application Kaspersky Security Center n'est pas prise en charge par l'application Kaspersky Endpoint Security.

- Autorisation ou interdiction du lancement de l'application pour des utilisateurs et/ou groupes d'utilisateurs sélectionnés. Vous pouvez choisir l'utilisateur et/ou le groupe d'utilisateurs qui pourra lancer ou non une application appartenant à la catégorie indiquée.

- Condition de déclenchement de la règle. La condition est une équivalence entre "type de condition - critère de condition - valeur de la condition". La condition de déclenchement de la règle de l'application Kaspersky Endpoint Security détermine si la règle va être appliquée ou non à l'application. Les règles utilisent des conditions d'inclusion et d'exclusion :

  - *Conditions d'inclusion*. Kaspersky Endpoint Security applique la règle à l'application si celle-ci satisfait à au moins une condition d'inclusion.

  - *Conditions d'exclusion*. Kaspersky Endpoint Security n'applique pas la règle à l'application si celle-ci satisfait à au moins une condition d'exclusion ou si elle ne satisfait à aucune règle d'inclusion.

  Les critères suivants permettent de définir les conditions de déclenchement de la règle :

  - nom du fichier exécutable de l'application ;

  - nom du dossier contenant le fichier exécutable de l'application ;

  - hachage du fichier exécutable de l'application. Seul SHA256 est autorisé.

  Vous devez attribuer une valeur à chaque critère utilisé dans une condition.

Les **masques** peuvent servir à définir des noms de fichiers et de répertoires.

Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Si les paramètres de l'application en cours de lancement répondent aux critères spécifiés dans la condition d'activation, la règle est déclenchée. Dans ce cas, Kaspersky Endpoint Security exécute l'action spécifiée dans la règle. Si les paramètres de l'application répondent aux critères spécifiés dans la condition d'exclusion, Kaspersky Endpoint Security ne contrôle pas le lancement de l'application.

Les règles du Contrôle des applications peuvent avoir l'un des *états de fonctionnement* suivants :

- *Activé* : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le contrôle des applications.
- *Inactif* : la règle est désactivée et n'est pas appliquée au Contrôle des applications.
- *Essai* : l'application Kaspersky Endpoint Security autorise le lancement des applications qui satisfont aux conditions de la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

La priorité de l'état de fonctionnement de la règle est supérieure à l'action indiquée dans la règle.

Mode de test des règles du Contrôle des applications

Pour vous assurer que les règles du Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est recommandé d'activer le *mode de test des règles du Contrôle des applications*. Dans ce mode, Kaspersky Endpoint Security ne bloquera pas l'exécution des applications tierces, mais enverra des notifications sur leur lancement au Serveur d'administration.

Par défaut, le Contrôle des applications autorise l'exécution de toutes les applications tierces, sauf celles interdites par les règles.

Test des règles du Contrôle des applications

1. **Créer les règles du Contrôle des applications**

   Configurez et activez les règles du Contrôle des applications que vous souhaitez tester. Par exemple, vous pouvez créer des règles qui empêchent l'exécution de toutes les applications tierces, à l'exception des applications des catégories « Image de référence » et « Applications de travail ».

2. **Activer le Contrôle des applications en mode test**

Comment activer le mode de test du Contrôle des applications 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 des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
6. Dans la section **Action lors du démarrage des applications**, sélectionnez l'action **Informer** pour le Contrôle des applications.
7. Pour appliquer la stratégie aux ordinateurs, fermez les icônes de cadenas et enregistrez vos modifications.

Comment activer le mode de test du Contrôle des applications sur la ligne de commande

Pour sélectionner le mode test pour le Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 AppControlRulesAction=TestRules
```

3 Examiner les résultats du test

Examinez le rapport du Contrôle des applications et les événements du module envoyés à Kaspersky Security Center.

Comment consulter le rapport du Contrôle des applications 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 des applications**.
5. Assurez-vous que le commutateur du module est en position **Contrôle des applications ACTIVÉ**.
6. Dans le tableau des règles du Contrôle des applications, cliquez sur le bouton **Consulter le rapport**.
7. La fenêtre **Rapport sur les applications interdites en mode test** s'ouvre.
8. Examinez les informations relatives au lancement des applications interdites en mode test.

Comment consulter les événements résultant d'un fonctionnement test du Contrôle des applications

1. Dans la fenêtre principale de Web Console, sélectionnez **Surveillance → Sélections d'événements**.
2. Cliquez sur **Ajouter**.

3. Dans la fenêtre **Nouvelle sélection d'événements** qui s'ouvre, indiquez un nom pour la sélection. Par exemple, « Test des règles du Contrôle des applications ».

4. Accédez à la section **Événements** et gérez les paramètres suivants :

   - **Nom de l'application** – Kaspersky Endpoint Security for Linux.
   - **Niveau de gravité** – **Information**.
   - Choisissez l'option **Inclure les événements généraux sélectionnés**.
   - Cochez les cases en regard des événements **Le lancement de l'application est interdit en mode test** et **Le lancement de l'application est autorisé en mode test**.

5. Si nécessaire, configurez les autres paramètres.

6. Enregistrez vos modifications.

7. Cliquez sur le nom de la sélection pour consulter le résultat de la sélection d'événements.

4 **Ajuster les règles**

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, modifiez les paramètres des règles que vous avez créées, créez des règles supplémentaires ou supprimez les règles existantes.

Configuration du contrôle des applications dans Web Console

Dans Web Console, vous pouvez gérer les paramètres du Contrôle des applications dans les propriétés de la stratégie (**Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle des applications**).

Configuration du contrôle des applications dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle des appareils dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Contrôle des applications**).

Paramètres du module Contrôle des applications

Paramètre	Description
Activer le module Contrôle des applications	Cette case permet d'activer le module Contrôle des applications. La case est décochée par défaut.
Action à réaliser en cas de tentative de lancement de l'application	Action que Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles configurées : • **Appliquer les règles** (valeur par défaut). Si vous choisissez cette option, l'application Kaspersky Endpoint Security applique les règles du Contrôle des applications et exécute l'action définie. • **Tester les règles**. Lorsque vous sélectionnez cette option, Kaspersky Endpoint Security teste les règles et génère un événement concernant une tentative de lancement d'une application qui correspond aux règles.
Mode Contrôle des applications	Mode de fonctionnement du module Contrôle des applications : • **Liste d'autorisation**. Si vous choisissez cette option, l'application Kaspersky Endpoint Security interdit à tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. • **Liste de refus** (valeur par défaut). Si vous choisissez cette option, l'application Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.
Règles du Contrôle des applications	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Règles du Contrôle des applications**.
Application des règles	Dans la liste déroulante, vous pouvez choisir comment ajouter des règles : • **Remplacer les règles locales par les règles depuis la stratégie**. Lorsque vous sélectionnez cet élément de la liste, l'application applique uniquement les règles spécifiées dans la stratégie. • **Ajouter des règles depuis la stratégie aux règles locales** (valeur par défaut). Si vous choisissez cette option, l'application applique les règles configurées dans la stratégie en même temps que les règles locales configurées sur l'appareil protégé.

Fenêtre Règles du Contrôle des applications

Le tableau **Règles du Contrôle des applications** contient les règles utilisées par le module Contrôle des applications. Par défaut, le tableau des règles du contrôle des applications est vide.

Paramètres des règles du contrôle des applications

Paramètre	Description
nom de la catégorie ;	Le nom de la catégorie des applications qui est utilisée par la règle.
État	État de fonctionnement de la règle du Contrôle des applications. • *Activé* : la règle est activée, le Contrôle des applications applique cette règle pendant son fonctionnement. • *Inactif* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle des applications. • *Essai* : le Contrôle des applications autorise le lancement des applications qui satisfont aux conditions de la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport. Vous pouvez modifier l'état d'une règle dans la fenêtre **Ajouter une nouvelle règle**.

Vous pouvez ajouter, modifier et supprimer des règles de contrôle des applications.

Fenêtre Ajouter une nouvelle règle

Cette fenêtre permet de configurer les paramètres de la règle du Contrôle des applications.

Ajout de la règle du Contrôle des applications

Paramètre	Description
Description	Description de la règle du Contrôle des applications.
État de la règle	La liste déroulante permet de sélectionner l'état du fonctionnement des règles du contrôle des applications : • *Activé* : la règle est activée, le Contrôle des applications applique cette règle pendant son fonctionnement. • *Inactif* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle des applications. • *Essai* : le Contrôle des applications autorise le lancement des applications qui satisfont aux conditions de la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.
Catégorie	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Catégories des applications**.
Utilisateurs et leurs droits	Le tableau contient une liste d'utilisateurs ou de groupes d'utilisateurs auxquels s'applique la règle de contrôle des applications ainsi que les types d'accès qui leur sont attribués et il se compose des colonnes suivantes : • **Nom d'utilisateur ou de groupe** : les noms d'utilisateurs ou les noms de groupes d'utilisateurs affectés par la règle de contrôle des applications. • **Accès** : type d'accès : **Autoriser** l'exécution des applications ou **Bloquer** leur exécution. Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.

Fenêtre Catégories d'applications

Cette fenêtre vous permet d'ajouter une nouvelle catégorie ou de configurer les paramètres de catégorie pour une règle du Contrôle des applications.

L'utilisation des catégories KL de l'application Kaspersky Security Center n'est pas prise en charge par l'application Kaspersky Endpoint Security.

Catégories du Contrôle des applications

Paramètre	Description
nom de la catégorie ;	Liste des catégories du Contrôle des applications ajoutées.
Ajouter	Cliquez sur ce bouton pour lancer l'assistant de création d'une catégorie. Suivez les instructions de l'Assistant. Pour plus d'informations sur la création d'une catégorie, consultez l'aide de Kaspersky Security Center.
Modifier	Cliquez sur le bouton pour ouvrir la fenêtre des propriétés des catégories qui permet de modifier les paramètres des catégories. La catégorie **Golden Image (locale)** ne peut pas être modifiée.

Fenêtre Utilisateur ou groupe

Cette fenêtre permet d'indiquer l'utilisateur local ou de domaine ou le groupe d'utilisateurs pour lequel vous souhaitez configurer la règle.

Ajout de la règle du Contrôle des applications

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.
Accès	Type d'accès : **Autoriser** le lancement des applications ou **Bloquer** le lancement des applications.

Configuration du Contrôle des applications sur la ligne de commande

À partir de la ligne de commande, vous pouvez gérer le contrôle des applications à l'aide de la tâche prédéfinie du contrôle des applications (*Application_Control*).

Par défaut, la tâche Contrôle des applications n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du contrôle des applications sur votre appareil en modifiant les paramètres de la tâche prédéfinie du contrôle des applications.

Si vous modifiez la liste des applications autorisées ou interdisez le lancement de toutes les applications ou des applications affectant le fonctionnement de Kaspersky Endpoint Security, alors, lors de la modification des paramètres de la tâche à l'aide du fichier de configuration ou de l'utilisation des options de ligne de commande, exécutez la commande `kesl-control --set-settings` avec l'option `--accept`.

Vous pouvez également configurer les paramètres du Contrôle des applications à l'aide des commandes de gestion du Contrôle des applications :

- Créer et modifier les listes des catégories.
- Consulter une liste des catégories créées dans l'application.
- Configurer une liste des règles du Contrôle des applications.

Paramètres de la tâche Contrôle des applications

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Contrôle des applications.

Paramètres de la tâche Contrôle des applications

Paramètre	Description	Valeurs
`AppControlMode`	Mode de fonctionnement du module Contrôle des applications.	`AllowList` : Kaspersky Endpoint Security interdit pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications. `DenyList` (valeur par défaut) : Kaspersky Endpoint Security autorise pour tous les utilisateurs le lancement de n'importe quelle application, à l'exception de celles reprises dans les règles du Contrôle des applications.
`AppControlRulesAction`	Action que l'application Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles configurées :	`ApplyRules` (valeur par défaut) : Kaspersky Endpoint Security applique les règles du contrôle des applications et exécute l'action définie. `TestRules` : Kaspersky Endpoint Security teste les règles et génère un événement concernant la détection d'une application correspondant à la règle.
La section **[Categories.item_#]** contient les paramètres suivants :		

Paramètre	Description	Valeurs
`Name`	Nom de la catégorie d'applications à laquelle la règle va s'appliquer.	
`UseIncludes`	Utilisation de conditions d'inclusion pour le déclenchement de la règle.	`Yes` : appliquer la règle à l'application si celle-ci satisfait à au moins une condition d'inclusion. `No` (valeur par défaut) : ne pas appliquer la règle à l'application, même si celle-ci satisfait à la condition d'inclusion.
`IncludeFileNames.item_#`	Nom du fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des **masques** pour spécifier des noms de fichier Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire. Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`. Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.
`IncludeFolders.item_#`	Nom du répertoire contenant le fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des **masques** pour spécifier des noms de répertoire. Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire. Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`. Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.
`IncludeHashes.item_#`	Hachage SHA256 du fichier exécutable pour le déclenchement de la règle.	Seul SHA256 est autorisé.
`UseExcludes`	Utilisation de conditions d'exclusion pour le déclenchement de la règle.	`Yes` : ne pas appliquer la règle à l'application si celle-ci satisfait à au moins une condition d'exclusion ou si elle ne satisfait à aucune règle d'inclusion. `No` (valeur par défaut) : appliquer la règle à l'application, même si celle-ci satisfait à la condition d'exclusion.
`ExcludeFileNames.item_#`	Nom du fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des **masques** pour spécifier des noms de fichier Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire. Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`. Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.
`ExcludeFolders.item_#`	Nom du répertoire contenant le fichier exécutable pour le déclenchement de la règle.	Vous pouvez utiliser des **masques** pour spécifier des noms de répertoire. Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire. Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`. Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Paramètre	Description	Valeurs
`ExcludeHashes.item_#`	Hachage SHA256 du fichier exécutable pour le déclenchement de la règle.	Seul SHA256 est autorisé.
La section **[AllowListRules.item_#]** contient la liste des règles du Contrôle des applications pour le mode de fonctionnement *Liste d'autorisation* (*AllowList*). Chaque section [AllowListRules.item_#] contient les paramètres suivants :		
`Description`	Description de la règle du Contrôle des applications.	
`AppControlRuleStatus`	État de fonctionnement de la règle du Contrôle des applications.	`On` (valeur par défaut) : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le Contrôle des applications. `Off` : la règle n'est pas utilisée pour contrôler les applications. `Test` : l'application Kaspersky Endpoint Security autorise le lancement des applications soumises à l'action de la règle, mais consigne les informations relatives au lancement de ces applications dans le rapport.
`Category`	Nom de la catégorie des applications à laquelle la règle s'applique. Vous pouvez indiquer en guise de catégorie la catégorie d'applications "Golden Image".	
La section **[AllowListRules.item_#.ACL.item_#]** contient la liste des utilisateurs qui ont le droit ou non de lancer des applications.		
`Access`	Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.	`Allow` (valeur par défaut) : autorise le lancement d'applications. `Block` : interdit le lancement d'applications.
`Principal`	Utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.	`\Everyone` (valeur par défaut) : la règle s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom de l'utilisateur auquel la règle s'applique. `@< nom de groupe >` est le nom du groupe d'utilisateurs auquel la règle s'applique.
La section **[DenyListRules.item_#]** contient la liste des règles du Contrôle des applications pour le mode de fonctionnement *Liste de refus* (*DenyList*). Chaque section [DenyListRules.item_#] contient les paramètres suivants :		
`Description`	Description de la règle du Contrôle des applications.	
`AppControlRuleStatus`	État de fonctionnement de la règle du Contrôle des applications.	`On` (valeur par défaut) : la règle est activée, et Kaspersky Endpoint Security applique cette règle pour le Contrôle des applications. `Off` : la règle n'est pas utilisée pour contrôler les applications. `Test` : l'application Kaspersky Endpoint Security autorise le lancement des applications soumises à l'action de la règle, mais consigne les informations relatives au lancement de ces applications dans le rapport.
`Category`	Nom de la catégorie d'applications créée à laquelle la règle s'applique. Vous pouvez indiquer en guise de catégorie la liste d'application "Golden Image".	
La section **[DenyListRules.item_#.ACL.item_#]** contient la liste des utilisateurs qui ont le droit ou non de lancer des applications.		
`Access`	Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.	`Allow` : autoriser le lancement des applications. `Block` (valeur par défaut) : interdit le lancement des applications.
`Principal`	Utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.	`\Everyone` (valeur par défaut) : la règle s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom de l'utilisateur auquel la règle s'applique. `@< nom de groupe >` est le nom du groupe d'utilisateurs auquel la règle s'applique.

Créer et modifier une liste des catégories

Vous pouvez créer une nouvelle catégorie de deux manières :

- en utilisant la commande kesl --set-settings et le fichier de configuration pour les paramètres de la tâche Contrôle des applications (Application_Control) ;
- en utilisant la commande kesl --set-categories et le fichier de configuration des paramètres de la catégorie.

Pour créer des catégories des applications, exécutez la commande suivante :

```
kesl-control --set-categories --file <chemin d'accès au fichier de configuration>
```

où :

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration contenant les paramètres de la catégorie.

Le fichier avec les paramètres de la catégorie doit avoir la structure suivante :

```
[
    {
        "Exclude" : [ "(FilePath like <chemin d'accès complet au fichier exécutable de
  l'application>)", "(FileHash == <hachage du fichier exécutable>)" ],
        "GUID" : "<ID unique de catégorie>",
        "Include" : [ "(FilePath like <chemin d'accès complet au fichier exécutable de
  l'application>)", "(FileHash == <hachage du fichier exécutable>)" ],
        "Name" : "<nom de la catégorie 1>"
    },
  {
        "Exclude" : [ "(FilePath like <chemin d'accès complet au fichier exécutable de
  l'application>)", "(FileHash == <hachage du fichier exécutable>)" ],
        "GUID" : "<ID unique de catégorie>",
        "Include" : [ "(FilePath like <chemin d'accès complet au fichier exécutable de
  l'application>)", "(FileHash == <hachage du fichier exécutable>)" ],
        "Name" : "<nom de la catégorie 2>"
    }
]
```

Pour spécifier le nom du fichier dans les champs `Exclude` et `Include`, vous pouvez utiliser les **masques**.

Vous pouvez utiliser le caractère * (toute séquence de caractères) ou le ? (n'importe quel caractère) pour former un masque pour un nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/*/file*/` ou `/dir/file*/`.

Pouvez-vous préciser le symbole ? au lieu d'un seul caractère (y compris le symbole `/`) dans un nom de fichier ou de répertoire.

Le paramètre `Name` est requis. Si vous ne spécifiez pas le nom de la catégorie, elle ne sera pas créée ou sera supprimée. Le paramètre `GUID` est également requis. Si vous ne le spécifiez pas, un message d'erreur s'affiche et la catégorie n'est pas créée. Le paramètre `GUID` doit être spécifié sans tirets.

Pour modifier la liste des catégories des applications créées, exécutez la commande suivante :

```
kesl-control --set-categories [--names <nom de la catégorie 1> <nom de la catégorie 2> … <nom de la catégorie N>] --file <chemin d'accès au fichier de configuration>
```

où :

- `<nom de la catégorie 1> <nom de la catégorie 2> … <nom de la catégorie N>` sont les noms des catégories dont vous souhaitez modifier les informations. Si vous souhaitez modifier les informations sur plusieurs catégories, spécifiez les noms de catégories séparés par un espace. Si vous ne spécifiez pas de nom de catégorie, les catégories existantes seront supprimées et de nouvelles catégories seront créées à partir du fichier spécifié.
- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration contenant les paramètres de la catégorie.

Consultation de la liste des catégories

À partir de la ligne de commande, vous pouvez afficher une liste des catégories créées des applications à l'aide de la commande de gestion par le contrôle des applications `kesl-control --get-categories`.

La liste des catégories créées contient les catégories suivantes :

- catégories créées dans Kaspersky Security Center ;
- catégories ajoutées dans les paramètres de la tâche Contrôle des applications via la ligne de commande ;
- catégorie "GoldenImage" créée à l'aide de la tâche Inventaire (dans Kaspersky Security Center ou via la ligne de commande).

Pour afficher la liste de toutes les catégories des applications créées, exécutez la commande suivante :

```
kesl-control --get-categories [--file <chemin d'accès au fichier de configuration>] [--json]
```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration JSON dans lequel les paramètres seront écrits.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas la clé --json, les paramètres seront affichés au format INI.

Kaspersky Endpoint Security affiche les informations suivantes sur chaque catégorie des applications :

- identifiant unique (GUID) de la catégorie ;
- nom de la catégorie ;
- une liste des conditions qui incluent les conditions de déclenchement de la règle ;
- Liste des conditions d'exclusion pour le déclenchement de la règle.

Pour afficher la liste des catégories distinctes des applications, exécutez la commande suivante :

```
kesl-control --get-categories [--names <nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>] [--file <chemin d'accès au fichier de configuration>] [--json]
```

où :

- `<nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>` désignent les noms des catégories pour lesquelles vous souhaitez consulter les informations. Si vous souhaitez consulter des informations sur plusieurs catégories, saisissez les noms des catégories séparés par un espace.
- `--file <chemin d'accès au fichier de configuration>` – chemin d'accès complet au fichier de configuration JSON dans lequel la liste des catégories sera exportée.
- `--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas la clé --json, les paramètres seront affichés au format INI.

Si, dans les paramètres de la tâche Contrôle des applications, dans la section `[Categories.item_#]`, vous avez spécifié des liens symboliques vers le fichier d'application ou vers le répertoire contenant les fichiers exécutables pour les conditions d'inclusion ou d'exclusion du déclencheur de règles, le chemin d'origine auquel le lien symbolique est référencé s'affichera lors de l'affichage de la liste des catégories pour ces conditions.

Configuration de la liste des règles du Contrôle des applications

Pour afficher la liste des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --get-settings 21 [--file <path to configuration file>] [--json]
```

où :

- `--file <path to configuration file>` est le chemin d'accès complet au fichier de configuration vers lequel vous souhaitez exporter les paramètres.
- `--json` : afficher les données au format JSON.

Kaspersky Endpoint Security affichera les informations suivantes sur les règles du Contrôle des applications :

- Mode de fonctionnement du module Contrôle des applications.
- Action que le Contrôle des applications effectue lors de la détection d'une tentative de lancement d'une application qui correspond à la règle configurée.
- Description de la règle du Contrôle des applications (le cas échéant).
- État de la règle du Contrôle des applications
- Nom de la catégorie d'applications à laquelle la règle s'applique
- Type d'accès attribué à l'utilisateur ou à un groupe d'utilisateurs.
- Utilisateur ou groupe d'utilisateurs auquel s'applique la règle du Contrôle des applications :

Pour modifier la liste des catégories des applications et des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 [--file <path to configuration file>] [--json]
```

où :

- `--file <path to configuration file>` est le chemin d'accès complet au fichier de configuration à partir duquel vous souhaitez importer les paramètres.
- `--json` : importer les données d'un fichier au format JSON.

Pour supprimer la liste des catégories des applications et des règles du Contrôle des applications, exécutez la commande suivante :

```
kesl-control --set-settings 21 --set-to-default
```

Exportation et importation des paramètres du Contrôle des applications

Pour simplifier la configuration du module Contrôle des applications sur les appareils des utilisateurs, vous pouvez exporter et importer les paramètres du Contrôle des applications ainsi qu'une liste de catégories des applications.

Exportation et importation des paramètres du Contrôle des applications dans Web Console

Dans Web Console, vous pouvez exporter et importer les paramètres du Contrôle des applications et la liste des catégories des applications dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Contrôle des applications**).

Cliquer sur le bouton **Exporter** dans le groupe **Paramètres du Contrôle des applications** ouvre une fenêtre permettant de spécifier le fichier dans lequel enregistrer les paramètres configurés. Cliquer sur le bouton **Importer** dans le groupe **Paramètres du Contrôle des applications** ouvre une fenêtre permettant de spécifier le fichier à partir duquel importer les paramètres.

Cliquer sur le bouton **Exporter** dans le groupe **Catégories des applications** ouvre une fenêtre vous permettant de spécifier le fichier dans lequel enregistrer les catégories ajoutées des applications. Cliquer sur le bouton **Importer** dans le groupe **Catégories des applications** ouvre une fenêtre vous permettant de spécifier le fichier à partir duquel importer les catégories des applications.

Exportation et importation des paramètres du Contrôle des applications dans la Console d'administration

Dans la Console d'administration, vous pouvez également exporter et importer les paramètres du Contrôle des applications et la liste des catégories des applications dans les propriétés d'un appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → <nom de l'application> → bouton **Propriétés** → fenêtre **Paramètres de <nom de l'application>** → section **Contrôle des applications**).

Cliquer sur le bouton **Exporter** dans le groupe **Paramètres du Contrôle des applications** ouvre une fenêtre permettant de spécifier le fichier dans lequel enregistrer les paramètres configurés. Cliquer sur le bouton **Importer** dans le groupe **Paramètres du Contrôle des applications** ouvre une fenêtre permettant de spécifier le fichier à partir duquel importer les paramètres.

Cliquer sur le bouton **Exporter** dans le groupe **Catégories des applications** ouvre une fenêtre vous permettant de spécifier le fichier dans lequel enregistrer les catégories ajoutées des applications. Cliquer sur le bouton **Importer** dans le groupe **Catégories des applications** ouvre une fenêtre vous permettant de spécifier le fichier à partir duquel importer les catégories des applications.

Exportation et importation des paramètres du Contrôle des applications dans la ligne de commande

Dans la ligne de commande, vous pouvez exporter et importer les paramètres du Contrôle des applications ainsi qu'une liste de catégories des applications à l'aide des commandes d'administration du Contrôle des applications.

Inventaire

La tâche Inventaire permet d'obtenir des informations sur tous les fichiers exécutables des applications conservés sur les appareils clients. L'obtention d'informations relatives aux applications installées sur les appareils peut être utile dans la création des règles de Contrôle des applications par exemple.

Pour utiliser la tâche, vous devez posséder la licence qui couvre cette fonction.

Vous pouvez configurer les paramètres d'inventaire suivants :

- Sélectionnez les types d'objets que l'application détectera sur l'appareil lors de l'inventaire (fichiers, scripts).
- Configurez les zones d'inventaire (chemins d'accès aux répertoires dans lesquels rechercher les fichiers exécutables de l'application).
- Configurez les exclusions de l'inventaire.
- Sélectionner l'action que l'application Kaspersky Endpoint Security effectue sur la catégorie des applications « Golden Image » à la fin de la tâche Inventaire. Vous pouvez ajouter les applications trouvées sur l'appareil à la suite de la tâche à la catégorie, laisser la catégorie inchangée ou la supprimer.
- Activer ou désactiver la transmission au Serveur d'administration de Kaspersky Security Center des informations sur les applications détectées sur l'appareil suite à l'exécution de la tâche Inventaire. Si les informations sur les applications de l'appareil sont transmises au Serveur d'administration, elles peuvent être utilisées pour configurer les catégories des applications via Kaspersky Security Center, sur la base desquelles les règles du module de Contrôle des applications sont créées.

Configuration de l'inventaire dans Web Console

Dans Web Console, vous pouvez effectuer un inventaire des applications sur un appareil protégé à l'aide de la tâche *Inventaire*.

Vous pouvez créer et lancer des tâches d'inventaire personnalisées. Vous pouvez configurer les paramètres d'inventaire en modifiant les paramètres de ces tâches.

Les bases de données de l'application Kaspersky Security Center peuvent conserver les informations relatives à 150 000 fichiers traités. Une fois ce chiffre atteint, les nouveaux fichiers ne seront pas traités. Afin de rétablir le fonctionnement de la tâche d'inventaire, il convient de supprimer sur l'appareil doté de l'application Kaspersky Endpoint Security tous les fichiers comptabilisés antérieurement dans la base de données de Kaspersky Security Center suite à l'analyse de l'inventaire.

Paramètres de la tâche d'inventaire

Paramètre	Description
Action avec la catégorie Golden Image une fois la tâche terminée	Dans la liste déroulante, vous pouvez sélectionner l'action que Kaspersky Endpoint Security effectue avec la catégorie des applications « Golden Image » une fois la tâche Inventaire terminée : • **Laisser inchangé** : ne pas modifier la catégorie des applications « Golden Image » une fois l'inventaire terminé. Cette valeur est sélectionnée par défaut. • **Mettre à jour ou créer (si n'est pas créé)** : ajouter les applications trouvées sur l'appareil par la tâche Inventaire à la catégorie des applications « Golden Image ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. • **Supprimer** : supprimer la catégorie des applications « Golden Image » après avoir effectué l'inventaire. Vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles de contrôle des applications.
Analyser tous les fichiers exécutables	La case active ou désactive l'analyse des fichiers exécutables. La case est cochée par défaut.
Analyser les fichiers binaires	La case active ou désactive l'analyse des fichiers binaires (avec l'extension .elf, .java et .pyc). La case est cochée par défaut.
Analyser les scripts	La case active ou désactive l'analyse des scripts. La case est cochée par défaut.
Zones d'inventaire	Un tableau contenant les zones d'inventaire vérifiées par l'application. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'inventaire : /usr/bin. Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'inventaire dans le tableau. Vous pouvez également importer une liste des zones d'inventaire à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones d'inventaire vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones d'inventaire ou à ajouter des zones d'inventaire à une liste existante.

Fenêtre d'ajout d'une zone d'analyse

Cette fenêtre permet d'ajouter ou de modifier une zone d'analyse pour la tâche Inventaire.

Paramètres de la zone d'inventaire

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone d'inventaire. Ce nom sera affiché dans le tableau de la section **Paramètres d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant l'exécution de la tâche. Si la case est cochée, l'application traite cette zone d'inventaire au moment de l'exécution de la tâche. Si cette case est décochée, l'application ne traite pas cette zone d'inventaire au moment de l'exécution de la tâche. Par la suite, vous pouvez inclure cette zone dans les paramètres de la tâche en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'inventaire. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local.

Paramètre	Description
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution de la tâche. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Zones d'exclusion

La section **Zones d'exclusion** de la tâche d'inventaire permet de configurer les zones d'exclusion de l'analyse.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Fenêtre d'ajout d'une zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion de l'analyse pour la tâche Inventaire.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'exclusion de cette zone pendant l'exécution de la tâche. Si cette case est cochée, l'application exclut cette zone au moment de l'exécution de la tâche. Si cette case est décochée, l'application inclut cette zone au moment de l'exécution de la tâche. Par la suite, vous pouvez exclure cette zone de l'analyse après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion d'inventaire. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Vous pouvez ajouter, modifier et supprimer des masques.

Configuration de l'inventaire dans la Console d'administration

Dans la Console d'administration de Kaspersky Security Center, vous pouvez effectuer un inventaire des applications sur l'appareil protégé à l'aide de la tâche *Inventaire*.

Vous pouvez créer et lancer des tâches d'inventaire personnalisées. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Les bases de données de l'application Kaspersky Security Center peuvent conserver les informations relatives à 150 000 fichiers traités. Une fois ce chiffre atteint, les nouveaux fichiers ne seront pas traités. Afin de rétablir le fonctionnement de la tâche d'inventaire, il convient de supprimer sur l'appareil doté de l'application Kaspersky Endpoint Security tous les fichiers comptabilisés antérieurement dans la base de données de Kaspersky Security Center suite à l'analyse de l'inventaire.

Paramètres de la tâche d'inventaire

Paramètre	Description
Action avec la catégorie Golden Image une fois la tâche terminée	Dans la liste déroulante, vous pouvez sélectionner l'action que Kaspersky Endpoint Security effectue avec la catégorie des applications « Golden Image » une fois la tâche Inventaire terminée : • **Laisser inchangé** : ne pas modifier la catégorie des applications « Golden Image » une fois l'inventaire terminé. Cette valeur est sélectionnée par défaut. • **Mettre à jour ou créer (si n'est pas créé)** : ajouter les applications trouvées sur l'appareil par la tâche Inventaire à la catégorie des applications « Golden Image ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. • **Supprimer** : supprimer la catégorie des applications « Golden Image » après avoir effectué l'inventaire. Vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles de contrôle des applications.
Analyser tous les fichiers exécutables	La case active ou désactive l'analyse des fichiers exécutables. La case est cochée par défaut.
Analyser les fichiers binaires	La case active ou désactive l'analyse des fichiers binaires (avec l'extension .elf, .java et .pyc). La case est cochée par défaut.
Analyser les scripts	La case active ou désactive l'analyse des scripts. La case est cochée par défaut.
Zones d'inventaire	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'analyse**.

La section **Exclusions** de la tâche Inventaire permet de configurer les zones d'exclusion de l'analyse.

Fenêtre Zones d'analyse

Le tableau contient les zones d'analyse. L'application analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone d'analyse : /usr/bin.

Paramètres de la zone d'analyse de la tâche Inventaire

Paramètre	Description
Nom de la zone	Nom de la zone d'analyse.
Chemin	Chemin au répertoire que l'application analyse.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de modifier une zone d'analyse pour la tâche Inventaire.

Paramètres de la zone d'inventaire

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone d'analyse. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant l'exécution de la tâche. Si la case est cochée, l'application traite cette zone d'analyse au moment de l'exécution de la tâche. Si cette case est décochée, l'application ne traite pas cette zone d'analyse au moment de l'exécution de la tâche. Par la suite, vous pouvez inclure cette zone dans les paramètres de la tâche en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'analyse. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution de la tâche. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Cliquer sur ce bouton ouvre la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion du contrôle.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de zone d'exclusion

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion de l'analyse pour la tâche Inventaire.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'exclusion de cette zone pendant l'exécution de la tâche. Si cette case est cochée, l'application exclut cette zone au moment de l'exécution de la tâche. Si cette case est décochée, l'application inclut cette zone au moment de l'exécution de la tâche. Par la suite, vous pouvez exclure cette zone de l'analyse après avoir coché la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion d'inventaire. Vous pouvez utiliser des **masques** pour spécifier le chemin. Le champ ne peut être vide. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.
Masques	La liste contient les masques des noms des objets exclus de l'analyse par l'application. Vous pouvez ajouter, modifier et supprimer des masques.

Configuration de l'inventaire dans la ligne de commande

Depuis la ligne de commande, vous pouvez faire l'inventaire des applications de l'appareil protégé des manières suivantes :

- Utilisation de la tâche prédéfinie Inventaire (*Inventory_Scan*). Vous pouvez démarrer et arrêter cette tâche et configurer la planification de son exécution. Vous pouvez configurer les paramètres d'analyse en modifiant les paramètres de cette tâche.
- À l'aide de tâches d'inventaire utilisateur (tâches de type *InventoryScan*). Vous pouvez démarrer, arrêter, suspendre et reprendre les tâches d'utilisateur manuellement et configurer la planification de lancement de la tâche.

Vous pouvez afficher la liste des applications découvertes sur un appareil suite à la tâche Inventaire à l'aide des commandes de gestion par le contrôle des applications.

Paramètres de la tâche d'inventaire

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez définir pour la tâche Inventaire.

Paramètres de la tâche d'inventaire

Paramètre	Description	Valeurs
`ScanScripts`	Activation de l'analyse des scripts.	`Yes` (valeur par défaut) : analyser les scripts. `No` : ne pas analyser les scripts.
`ScanBinaries`	Activation de l'analyse des fichiers binaires (elf, java, et pyc).	`Yes` (valeur par défaut) : analyser les fichiers binaires. `No` : ne pas analyser les fichiers binaires.
`ScanAllExecutable`	Activation de l'analyse des fichiers avec un bit exécutable.	`Yes` (valeur par défaut) : analyser les fichiers avec un bit exécutable. `No` : ne pas analyser les fichiers avec un bit exécutable.

Paramètre	Description	Valeurs
`GoldenImageAction`	L'action que l'application Kaspersky Endpoint Security effectue sur la catégorie des applications « Golden Image » à la fin de la tâche Inventaire : Vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles de contrôle des applications.	`DoNothing` (valeur par défaut) : ne pas modifier la catégorie des applications « Golden Image » une fois l'inventaire effectué. `Create` : ajouter les applications détectées à la catégorie d'applications « Golden Image ». Si la catégorie n'existe pas, elle sera créée. Si la catégorie existe, la liste des applications qu'elle contient sera mise à jour. `Remove` : supprimer la catégorie des applications « Golden Image » après avoir effectué l'inventaire.
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	Description de la zone d'inventaire. La longueur maximale la ligne définie par ce paramètre est de 4 096 caractères.	Valeur par défaut : `All objects`.
`UseScanArea`	Activation de l'analyse de la zone d'inventaire. Pour exécuter la tâche, il faut activer l'analyse d'au moins une zone d'inventaire.	`Yes` (valeur par défaut) : analyser la zone d'inventaire indiquée. `No` : ne pas analyser la zone d'inventaire indiquée.
`AreaMask.item_#`	Restriction de la zone d'inventaire. Dans la zone d'inventaire, l'application analyse uniquement les fichiers renseignés à l'aide de masques au format "shell". Si le paramètre n'est pas défini, l'application analyse tous les objets de la zone d'inventaire. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (analyser tous les objets).
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` — analyser les objets dans le répertoire indiqué. Valeur par défaut : `/usr/bin`
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	Description de la zone d'exclusion de l'inventaire.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone d'inventaire indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée. `No` : n'exclut pas la zone indiquée.
`AreaMask.item_#`	Restriction de la zone d'exclusion d'inventaire selon des masques au format shell. Si le paramètre n'est pas défini, l'application exclut tous les objets de la zone d'inventaire. Vous pouvez définir plusieurs valeurs de ce paramètre.	Valeur par défaut : `*` (exclure tous les objets).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`< chemin d'accès au répertoire local >` exclut les objets du répertoire indiqué de l'analyse. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Consultation de la liste des applications détectées

Pour consulter la liste des applications détectées sur l'appareil, exécutez la commande suivante :

```
kesl-control --get-app-list [--json]
```

où `--json` : afficher les données au format JSON.

Kaspersky Endpoint Security affiche les informations suivantes sur les applications détectées :

- **Date et heure d'inventaire**. Date et heure d'exécution de la tâche d'inventaire.
- **Nombre d'applications**. Le nombre d'applications trouvées sur l'appareil.
- Liste des applications contenant les informations suivantes :
  - **Chemin d'accès**. Chemin d'accès à l'application.
  - **Hash**. La somme de hash de l'application.
  - **Type**. Type d'application. Par exemple : `Script`, `Executable`.
  - **Catégories**. Les catégories auxquelles l'application appartient (si elles ont été créées auparavant). Vous pouvez consulter la liste des catégories d'applications générées avec la commande `kesl-control --get-categories`.

Lorsqu'une nouvelle catégorie est ajoutée, ses informations dans la liste des applications ne sont pas automatiquement mises à jour. Pour mettre à jour la liste des applications, la tâche Inventaire doit être exécutée à nouveau.

Contrôle des appareils

Le module *Contrôle des appareils* permet de contrôler l'accès des utilisateurs aux appareils installés ou connectés à l'appareil client (par exemple, disques durs, caméras ou modules Wi-Fi). Le contrôle d'accès aide à protéger l'appareil client contre les infections lors de la connexion des appareils externes et empêche la perte ou la fuite de données.

Le module Contrôle des appareils est activé automatiquement avec les paramètres par défaut lorsque vous lancez l'application Kaspersky Endpoint Security.

Le contrôle des appareils gère l'accès aux niveaux suivants :

- **Type d'appareil** selon la classification du module Contrôle des appareils (par exemple, imprimantes, lecteurs amovibles, lecteurs de CD/DVD). Pour chaque type d'appareil, l'un des modes d'accès suivants peut être utilisé :
  - *Autoriser* pour octroyer un accès aux appareils de ce type.
  - *Bloquer* : bloque l'accès aux appareils de ce type.
  - *En fonction du bus de connexion* : autoriser ou refuser l'accès aux appareils en fonction du mode d'accès du bus via lequel l'appareil est connecté.
  - *Par règles* : autoriser ou refuser l'accès aux appareils en fonction des règles d'accès aux appareils. Une *règle d'accès à l'appareil* est un ensemble de paramètres qui définissent quels utilisateurs et à quelle heure peuvent accéder aux appareils installés ou connectés à l'appareil client. Ce mode d'accès ne peut être spécifié que pour les appareils de stockage (disques durs, disques amovibles, disquettes, lecteurs de CD/DVD). Lorsque vous connectez un appareil dont l'accès est interdit, l'application refuse aux utilisateurs spécifiés dans la règle l'accès à cet appareil et affiche une notification. Lors d'une tentative de lecture et d'écriture sur cet appareil, l'application refuse la lecture/écriture aux utilisateurs spécifiés dans la règle sans afficher de notification. Si, lorsque vous tentez d'effectuer une opération sur un appareil pour lequel le mode d'accès *En fonction des règles* est défini, aucune règle n'est active au moment de l'accès, l'opération avec l'appareil sera interdite.
  - *Lecture seule* : autoriser l'accès en lecture seule aux appareils du type sélectionné, mais l'écriture sera interdite. Ce mode d'accès ne peut être spécifié que pour les appareils de stockage (disques durs, disques amovibles, disquettes, lecteurs de CD/DVD). Si le type d'accès à l'appareil est défini sur lecture seule, lorsque vous attribuez un appareil deconfiance à un utilisateur spécifique, l'utilisateur attribué est ignoré et l'appareil devient accessible en écriture par tous les utilisateurs.
- **Bus de connexion**. Le *bus de connexion* est l'interface via laquelle les appareils sont connectés à l'appareil client (par exemple, USB, FireWire). L'un des modes d'accès suivants peut être utilisé pour les bus de connexion :
  - *Autoriser* : donner accès aux appareils connectés via ce bus de connexion.
  - *Bloquer* : refuser l'accès aux appareils connectés via ce bus de connexion.

  Par exemple, l'accès à tous les appareils connectés via USB peut être refusé.

Par défaut, le mode d'accès *Dépend du bus de connexion* est sélectionné pour tous les types d'appareils. Le mode d'accès *Autoriser* est sélectionné pour les bus de connexion. Sur la base de ces paramètres, le Contrôle des appareils donne aux utilisateurs un accès complet à tous les appareils.

Lors de sa première activation, le Contrôle des appareils génère un événement *Appareil autorisé* pour tous les appareils détectés dont le type d'appareil ou le type de bus est connu. Aucun événement répété n'est généré lors des exécutions ultérieures du module, sauf si les paramètres de contrôle de ces appareils ont été modifiés.

Lorsque vous désactivez le module Contrôle des appareils, l'application déverrouille l'accès aux appareils bloqués.

Le contrôle des appareils ne bloque pas les disques système. Si l'application ne parvient pas à détecter automatiquement le disque système, le module Contrôle des appareils échoue avec une erreur.

Le blocage des appareils par type d'appareil et par bus de connexion via le pilote système de l'appareil n'est pas pris en charge sur les noyaux du système d'exploitation Linux : 3.10, 5.14, 5.15, 5.17, 6.1, 6.8. Sur ces noyaux et en mode d'accès *Par règles*, seules l'ouverture de fichiers et la lecture de répertoires (c'est-à-dire l'obtention de noms de fichiers et de répertoires) sont bloquées. Sur les systèmes qui ne prennent pas en charge la technologie fanotify, le verrouillage de la lecture du répertoire n'est pas pris en charge.

Le contrôle des appareils ignore les exclusions de points de montage. L'accès à un appareil monté sur un point de montage exclu peut être limité conformément aux paramètres configurés de contrôle des appareils.

Vous pouvez activer ou désactiver le Contrôle des appareils, ainsi que configurer les paramètres de fonctionnement du module :

- Sélectionnez le mode de fonctionnement de l'application lorsque vous tentez d'accéder à un appareil dont l'accès est interdit conformément aux paramètres de contrôle des appareils : bloquer ou informer uniquement d'une tentative d'accès à l'appareil.
- Sélectionnez le mode d'accès des appareils en fonction de leur type.
- Sélectionner le mode d'accès aux appareils en fonction du bus via lequel les appareils sont connectés.
- Excluez des appareils individuels de la zone d'action du Contrôle des appareils en les ajoutant à la liste des appareils de confiance. *Les appareils de confiance* sont des appareils auxquels les utilisateurs ont un accès complet. Par exemple, vous pouvez également autoriser l'accès à des appareils USB spécifiques ou uniquement à des clés USB, tandis que l'accès à d'autres appareils USB sera refusé. De plus, vous pouvez spécifier des utilisateurs ou des groupes d'utilisateurs pour lesquels les appareils seront approuvés.

  Vous pouvez gérer la liste des appareils de confiance via la ligne de commande ou à l'aide de Kaspersky Security Center.

  Vous pouvez ajouter des appareils à la liste des appareils de confiance par ID ou masque d'ID d'appareil. Vous pouvez obtenir des informations sur les appareils installés ou connectés aux appareils clients à l'aide de la ligne de commande sur l'appareil client ou à l'aide de Kaspersky Security Center. Le transfert d'informations vers le Serveur d'administration de Kaspersky Security Center est activé par défaut.

  > Les informations sur les appareils sont transférées si l'appareil client est sous le contrôle d'une stratégie active et si la synchronisation avec l'Agent d'administration est effectuée (effectuée à la fréquence spécifiée dans les propriétés de la stratégie de l'Agent d'administration, par défaut - toutes les 15 minutes).

  Si vous administrez l'application à l'aide de Kaspersky Security Center, pour ajouter des appareils à la liste des appareils approuvés, vous pouvez également utiliser :

  - Liste des appareils détectés sur les appareils clients administrés. La liste s'affiche dans les propriétés de la stratégie dans Web Console ou dans la Console d'administration.
  - Liste des appareils générée à partir des événements du Contrôle des appareils dans Kaspersky Security Center. Vous pouvez créer cette liste dans les propriétés de la stratégie dans la Console d'administration.

Dans la Console d'administration, vous pouvez aussi exporter la liste configurée des appareils de confiance vers un fichier et importer la liste des appareils à partir d'un fichier.

- Configurer un calendrier d'accès pour les appareils de stockage (disques durs, lecteurs amovibles, disquettes, lecteurs CD/DVD).

  Si le blocage d'accès aux fichiers pendant l'analyse est désactivé dans les paramètres généraux de l'application, vous ne pouvez pas bloquer l'accès aux appareils à l'aide d'un calendrier d'accès aux appareils.

- Configurez les règles d'accès pour les appareils en fonction de leur type. Vous pouvez autoriser ou refuser l'accès à des utilisateurs spécifiés à des heures spécifiées.

- Autoriser l'utilisateur demander un accès temporaire à un appareil bloqué et fournir à l'utilisateur l'accès à l'appareil.

  L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.2 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.

Configuration du contrôle des appareils dans Web Console

Dans Web Console, vous pouvez configurer les paramètres du contrôle des applications dans les propriétés de la stratégie (**Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle des appareils**).

Configuration du contrôle des appareils dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle des appareils dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Contrôle des appareils.**).

Paramètres du contrôle des appareils

Paramètre	Description
Activer le contrôle des appareils	Cette case active ou désactive le module Contrôle des appareils. La case est cochée par défaut.
Appareils de confiance	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur ce lien pour ouvrir la fenêtre **Appareils de confiance**. Dans cette fenêtre, vous pouvez ajouter un appareil à la liste des appareils de confiance.
Mode de fonctionnement du Contrôle des appareils	Mode de fonctionnement de l'application lors de la tentative d'accès à un appareil dont l'accès est interdit conformément aux paramètres du Contrôle des appareils : • **Informer**. Si vous sélectionnez cette option, Kaspersky Endpoint Security teste le mode d'accès sélectionné et génère un événement relatif à la tentative détectée d'accès à un appareil. • **Bloquer** (valeur par défaut). Si vous sélectionnez cette option, Kaspersky Endpoint Security applique le mode d'accès défini pour l'appareil ou le bus.
Paramètres du Contrôle des appareils	Le groupe de paramètres contient les boutons qui, lorsqu'ils sont cliqués, ouvrent des fenêtres dans lesquelles vous pouvez configurer le mode d'accès aux appareils en fonction de leur type et le mode d'accès aux bus de connexion.

Paramètre	Description
Autoriser les demandes d'accès temporaire	Si la case est cochée, l'utilisateur peut demander un accès temporaire à un appareil verrouillé via l'interface graphique ou la ligne de commande de l'application.
Modèles de messages	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Modèles de messages**.

Fenêtre Appareils de confiance

Le tableau contient la liste des appareils de confiance. Par défaut, le tableau est vide.

Paramètres de l'appareil de confiance.

Paramètre	Description
ID de l'appareil	ID d'un appareil de confiance.
Nom de l'appareil	Nom d'un appareil de confiance.
Type d'appareil.	Type d'un appareil de confiance (par exemple, Disque dur ou Lecteur de carte intelligente).
Nom d'hôte	Nom de l'appareil client auquel se connecte un appareil de confiance.
Utilisateur ou groupe	Le nom d'utilisateur ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé.
Commentaire	Commentaire lié à un appareil de confiance.

Vous pouvez ajouter des appareils à la liste des appareils de confiance à l'aide du bouton **Ajouter** en procédant comme suit :

- Spécifier l'identifiant de l'appareil ou le masque de l'identifiant (**Ajouter** → **Ajouter un appareil par identifiant ou masque**).
- Sélectionner l'appareil souhaité dans la liste des appareils détectés sur les appareils administrés (**Ajouter** → **Sélectionner l'appareil dans la liste des appareils détectés sur les appareils clients**).
- Sélectionner l'appareil nécessaire dans la liste des appareils détectés dans les événements du Contrôle des appareils de Kaspersky Security Center (**Ajouter** → **Ajouter un appareil en fonction des événements**).

Vous pouvez modifier et supprimer des appareils de confiance dans le tableau.

Vous pouvez également exporter la liste des appareils ajoutés dans un fichier en cliquant sur le bouton **Avancés** → **Exporter les éléments sélectionnés** ou sur le bouton **Avancés** → **Exporter tout** et importer une liste d'appareils à partir d'un fichier JSON à l'aide du bouton **Avancés** → **Importer**.

Trois modes d'importation sont disponibles :

- **Fusionner avec ceux qui existent** : fusionne les listes d'appareils de confiance lors de l'importation. Si le fichier contient déjà un enregistrement pour un appareil avec le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figuraient pas auparavant dans la liste.
- **Ajouter à ceux qui existent** : compléter la liste des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.
- **Remplacer ceux qui existent** : remplacer la liste des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste du fichier.

Fenêtre Appareil de confiance (ID de l'appareil)

Cette fenêtre permet d'ajouter un appareil à la liste des appareils de confiance sur la base de son ID.

Ajout d'un appareil par ID

Paramètre	Description
ID de l'appareil	Champ de saisie d'ID ou de masque d'ID de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance. Pour indiquer un identifiant, vous pouvez utiliser des masques * (toute séquence de caractères) ou ? (n'importe quel caractère). Par exemple, vous pouvez indiquer un masque USBSTOR* pour autoriser l'accès à toutes les clés USB.
Recherche sur les appareils	Un clic sur le bouton affiche les appareils trouvés par l'identifiant ou le masque spécifié sur les appareils clients connectés. Le bouton est disponible quand le champ **ID de l'appareil** contient une valeur.
Appareils trouvés	Ce tableau contient les colonnes suivantes : • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **ID de l'appareil** : identifiant de l'appareil trouvé. • **Nom de l'appareil** : nom de l'appareil trouvé. • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé.
Commentaire	Champ de saisie de commentaires au sujet de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance (facultatif).
Autoriser l'accès aux utilisateurs et/ou aux groupes d'utilisateurs	Un champ qui affiche le nom de l'utilisateur et/ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé. La valeur par défaut est **\Everyone** (tous les utilisateurs).
Configurer	Cliquer sur le bouton ouvre la fenêtre Accès à un appareil de confiance.

Fenêtre Appareils sur les appareils clients

Dans cette fenêtre, vous pouvez ajouter un appareil à une liste d'appareils de confiance en sélectionnant dans une liste d'appareils découverts sur les appareils clients administrés.

Les informations sur les appareils existants sont disponibles uniquement si une stratégie active est créée et s'il y a eu une synchronisation avec l'Agent d'administration (fonctionne dans les limites spécifiées dans la stratégie de l'Agent d'administration, 15 minutes par défaut).

Lorsque vous créez une stratégie inactive, la liste sera vide.

Ajout d'appareils à partir de la liste des appareils détectés sur les appareils clients administrés

Paramètre	Description
Nom d'hôte	Champ de saisie du nom ou du masque du nom de l'appareil administré pour lequel vous souhaitez trouver les appareils connectés. Le masque par défaut est *, qui représente tous les appareils administrés.
Type d'appareil.	Cette liste déroulante permet de définir le type d'appareil connecté à rechercher (par exemple, Disques durs ou Lecteurs de carte intelligente). L'option sélectionnée par défaut est **Tous les appareils**.
ID de l'appareil	Champ de saisie de l'ID ou du masque d'ID de l'appareil que vous souhaitez trouver. Le masque par défaut est *, qui représente tous les appareils.
Recherche sur les appareils	Cliquez sur ce bouton pour que l'application lance une recherche d'appareils selon les paramètres indiqués. Les résultats de la recherche sont repris dans le tableau inférieur.
Liste des appareils détectés	Ce tableau contient les colonnes suivantes : • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé. • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **Nom de l'appareil** : nom de l'appareil trouvé. • **ID de l'appareil** : identifiant de l'appareil trouvé.

Fenêtre Liste des appareils en fonction des événements du Contrôle des appareils

Dans cette fenêtre, vous pouvez créer une liste des appareils détectés lors des événements du Contrôle des appareils dans Kaspersky Security Center. Les appareils de cette liste peuvent ensuite être ajoutés à la liste des appareils de confiance.

Vous pouvez sélectionner un ou plusieurs appareils à ajouter à la liste des appareils de confiance.

Les informations sur les appareils sont disponibles si le Contrôle des appareils est activé, s'il existe une stratégie active et s'il y a eu une synchronisation avec l'Agent d'administration (fonctionne dans les limites spécifiées dans la stratégie de l'Agent d'administration, 15 minutes par défaut).

Lorsque vous créez une stratégie inactive, la liste sera vide.

Ajout d'appareils à partir de la liste des appareils détectés dans les événements de Kaspersky Security Center

Paramètre	Description
Types d'événements	Vous pouvez cocher les cases pour sélectionner les types d'événements du Contrôle des appareils envoyés à Kaspersky Security Center. La liste inclut les appareils détectés dans les événements du type spécifié. Toutes les cases sont cochées par défaut.
Groupe d'administration	Champ du saisie du nom du groupe d'administration contenant les appareils clients auxquels les appareils détectés sont connectés. La liste inclut uniquement les appareils connectés aux appareils clients du groupe d'administration spécifié. Vous pouvez spécifier une partie du nom du groupe. Par défaut, la liste inclut les appareils connectés aux appareils clients de n'importe quel groupe d'administration.
Période de formation des événements	Utilisez la liste déroulante pour sélectionner la période pendant laquelle les événements se sont produits. La liste inclut les appareils détectés dans les événements envoyés à Kaspersky Security Center pendant la période spécifiée. Par défaut, la liste inclut les appareils détectés dans les événements du mois dernier.
Recherche d'appareils	Cliquez sur ce bouton pour que l'application lance une recherche d'appareils selon les paramètres indiqués. Les résultats de la recherche sont repris dans le tableau inférieur.
Appareils trouvés	Ce tableau contient les colonnes suivantes : • **Type d'appareil** : type d'appareil trouvé (par exemple, Disque dur ou Lecteur de carte à puce). • **ID de l'appareil** : identifiant de l'appareil trouvé. • **Nom de l'appareil** : nom de l'appareil trouvé. • **Nom de l'appareil client** : nom de l'appareil client auquel se connecte un appareil trouvé. • **Date de connexion** : date à laquelle l'appareil détecté a été connecté. • **Groupe d'administration** : nom du groupe d'administration contenant l'appareil client auquel l'appareil détecté est connecté.
Commentaire	Champ de saisie de commentaires au sujet de l'appareil que vous souhaitez ajouter à la liste des appareils de confiance (facultatif).
Autoriser l'accès aux utilisateurs et/ou aux groupes d'utilisateurs	Un champ qui affiche le nom de l'utilisateur et/ou le nom du groupe d'utilisateurs pour lesquels l'appareil est approuvé. La valeur par défaut est **\Everyone** (tous les utilisateurs).
Configurer	Cliquer sur le bouton ouvre la fenêtre Accès à un appareil de confiance.

Fenêtre Accès à un appareil de confiance

Dans cette fenêtre, vous pouvez configurer l'accès des utilisateurs ou des groupes d'utilisateurs à l'appareil de confiance sélectionné.

Accès à un appareil de confiance

Paramètre	Description
Utilisateurs et/ou groupes d'utilisateurs	Liste des utilisateurs et des groupes pour lesquels l'appareil ajouté sera approuvé. Par défaut, le tableau contient l'élément **\Tous** (tous les utilisateurs). Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier un utilisateur ou un groupe d'utilisateurs pour lesquels l'appareil sera approuvé.

Paramètres de l'appareil de confiance.

Paramètre	Description
Type	L'**Utilisateur** ou le **Groupe** pour lesquels l'appareil sera approuvé.
Utilisateur ou groupe	Le nom d'un utilisateur local ou de domaine (sans spécifier le nom complet avec le domaine, si le système permet de saisir des noms d'utilisateur dans ce format, ou dans le format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`) ou le nom d'un groupe d'utilisateurs pour lesquels l'appareil sera approuvé.

Fenêtre Type d'appareil

Cette fenêtre permet de configurer des modes d'accès pour différents types d'appareil.

Modes d'accès pour les types d'appareil

Paramètre	Description
Type d'appareil.	Types d'appareil (par exemple, Disques durs, Imprimantes).
Mode d'accès	Mode d'accès à l'appareil. Un clic droit sur la souris ouvre un menu contextuel dans lequel vous pouvez sélectionner l'une des options suivantes : • **Autoriser** pour octroyer l'accès aux appareils du type sélectionné. • **Bloquer** pour interdire l'accès aux appareils du type sélectionné. • **Dépend du bus** (valeur par défaut) pour autoriser ou interdire l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion. • **En fonction des règles** pour autoriser ou interdire l'accès aux appareils, selon une règle d'accès et sa planification. Cette option de menu est uniquement disponible pour les appareils de stockage (disques durs, lecteurs amovibles, disquettes, lecteurs CD/DVD). • **Lecture seule** : autoriser l'accès en lecture seule aux appareils du type sélectionné. Cette option de menu est uniquement disponible pour les appareils de stockage (disques durs, lecteurs amovibles, disquettes, lecteurs CD/DVD).

Vous pouvez configurer les règles et les horaires d'accès dans la fenêtre **Configuration de la règle d'accès aux appareils**, qui s'ouvre en double-cliquant sur le nom du type d'appareil.

Fenêtre Configuration de la règle d'accès aux appareils

Cette fenêtre permet configurer les règles d'accès et la planification pour les types d'appareil sélectionnés.

Pour ouvrir cette fenêtre, double-cliquez sur le nom du type d'appareil dans la fenêtre **Type d'appareil**.

Règles et planifications d'accès aux appareils

Paramètre	Description
Utilisateurs et/ou groupes d'utilisateurs	Liste des utilisateurs et des groupes pour lesquels vous pouvez configurer des planifications d'accès. Par défaut, le tableau contient l'élément **\Tous** (tous les utilisateurs). Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs.
Règles d'accès aux appareils	Ce tableau contient les planifications d'accès pour les utilisateurs et les groupes d'utilisateurs. Il comporte les colonnes suivantes : • **Planification d'accès** : noms des planifications d'accès en vigueur. La case à côté de la planification indique si cette planification est utilisée par le module. • **Accès** : type d'accès pour la planification : **Autoriser** (octroyer l'accès aux appareils du type sélectionné) ou **Bloquer** (interdire l'accès aux appareils du type sélectionné). Vous pouvez configurer des planifications uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs CD/DVD. Le tableau contient par défaut une planification d'accès intitulée **Par défaut**. Celle-ci garantit l'accès intégral aux appareils pour tous les utilisateurs (sélection de l'option **\Tous** dans la liste **Utilisateurs et/ou groupes d'utilisateurs**) à tout moment, même si l'accès via le bus de connexion est autorisé pour ce type d'appareil. Vous pouvez ajouter, modifier et supprimer des planifications d'accès pour les utilisateurs sélectionnés. Il est impossible de modifier ou de supprimer la planification **Par défaut**.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier l'utilisateur ou le groupe d'utilisateurs auquel s'applique la règle d'accès à l'appareil.

Configuration de la règle d'accès aux appareils

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Le nom d'un utilisateur local ou de domaine (sans spécifier le nom complet avec le domaine, si le système permet de saisir des noms d'utilisateur dans ce format, ou dans le format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`) ou le nom d'un groupe d'utilisateurs auquel la règle s'applique.

Fenêtre Planification d'accès

Cette fenêtre permet de configurer les planifications d'accès aux appareils.

Planifier l'accès aux appareils

Paramètre	Description
Nom	Champ de saisie du nom de la planification d'accès.
Intervalles de temps	Tableau qui permet de préciser des intervalles de temps pour la planification (jours et heures). Les intervalles surlignés en vert sont inclus dans la planification. Pour exclure un intervalle de la planification, cliquez sur les cellules correspondantes. Les intervalles exclus de la planification sont surlignés en gris. Par défaut, tous les intervalles (24/7) sont inclus dans la planification.

Fenêtre Bus de connexion

Cette fenêtre permet de configurer le mode d'accès pour les bus de connexion.

Mode d'accès pour les bus de connexion

Paramètre	Description
Bus de connexion	Le bus de connexion via lequel les appareils sont connectés à l'appareil client : • **FireWire** • **USB**
Mode d'accès	Mode d'accès pour les bus de connexion. Un clic droit sur la souris ouvre un menu contextuel dans lequel vous pouvez sélectionner l'une des options suivantes : • **Autoriser** (valeur par défaut) permet d'accéder aux appareils connectés à l'aide de ce bus de connexion. • **Bloquer** : refuser l'accès aux appareils connectés via ce bus de connexion.

Configuration du modèle de message du Contrôle des appareils

Lorsqu'un utilisateur tente d'accéder à un appareil verrouillé, l'application affiche un message indiquant que l'accès à l'appareil est refusé ou que les opérations sur l'appareil sont interdites.

Un modèle est fourni pour les messages de refus d'accès, décrivant les raisons du blocage. Il existe des variables spéciales pour le texte du modèle de message (par exemple, %USER_NAME%). Les variables vous permettent d'utiliser un seul modèle de message pour différents appareils. Lors de la génération d'un message, l'application insère dans celui-ci les valeurs des variables correspondant à un appareil, un utilisateur et un événement spécifiques.

Vous pouvez modifier le contenu du modèle de message.

Pour modifier le modèle de message dans Web Console :

1. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Paramètres de l'application** → **Contrôle de sécurité** → **Contrôle des appareils**.

2. Dans la section **Modèles de messages**, cliquez sur le lien **Messages de verrouillage de l'appareil**.

3. Dans la fenêtre **Modèles de messages** qui s'ouvre, configurez le modèle de message du Contrôle des appareils sous l'onglet **Message à l'utilisateur**.

   Vous pouvez ajouter des variables et des liens au texte du message adressé à l'utilisateur à l'aide des boutons **Ajouter une variable** et **Ajouter un lien**. Pour ajouter une variable au texte du modèle, placez le curseur à l'endroit souhaité dans le texte, cliquez sur le bouton **Ajouter une variable** et sélectionnez la variable souhaitée dans la liste déroulante. Pour ajouter un lien au texte du modèle, placez le curseur à l'endroit souhaité dans le texte et cliquez sur le bouton **Ajouter un lien**.

   Vous pouvez aussi restaurer le texte du modèle de message en cliquant sur le bouton **Restaurer par défaut**.

4. Cliquez sur le bouton **OK**.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Pour modifier le modèle de message dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de sécurité** → **Contrôle des appareils**.

5. Dans la section **Modèles** de messages, cliquez sur le bouton **Configurer**.

6. Dans la fenêtre **Modèles de messages** qui s'ouvre, configurez le modèle de message du Contrôle des appareils sous l'onglet **Message sur le blocage**.

   Vous pouvez ajouter des variables et des liens au texte d'un message destiné à un utilisateur à l'aide des boutons **Variable** et **Lien**. Pour ajouter une variable au texte du modèle, placez le curseur à l'endroit souhaité dans le texte, cliquez sur le bouton **Variable** et sélectionnez la variable souhaitée dans la liste déroulante. Pour ajouter un lien au texte du modèle, placez le curseur à l'endroit souhaité dans le texte et cliquez sur le bouton **Lien**.

   Vous pouvez aussi restaurer le texte du modèle de message en cliquant sur le bouton **Par défaut**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Appliquer**.

Configuration du Contrôle des appareils dans la ligne de commande

À partir de la ligne de commande, vous pouvez gérer le contrôle des appareils à l'aide de la tâche prédéfinie Contrôle des appareils (*Device_Control*).

La tâche Contrôle des appareils n'est pas lancée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de contrôle des appareils en modifiant les paramètres de la tâche prédéfinie Contrôle des appareils.

À l'aide des commandes d'administration du Contrôle des appareils, vous pouvez également :

- afficher et exporter la liste des appareils connectés dans un fichier ;
- afficher et modifier la liste des appareils de confiance.

Paramètres du Contrôle des appareils

Le tableau décrit toutes les valeurs possibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche Contrôle des appareils.

Paramètre	Description	Valeurs
`OperationMode`	Mode de fonctionnement de l'application lors de la tentative d'accès à un appareil dont l'accès est interdit conformément aux paramètres du Contrôle des appareils.	`Block` (valeur par défaut) : l'application applique le mode d'accès spécifié pour l'appareil ou le bus. `Notify` : l'application teste le mode d'accès sélectionné et génère un événement sur la détection d'une tentative d'accès à l'appareil.
`AllowToRequestTemporaryAccess`	Autorisation de demander un accès temporaire à un appareil verrouillé. L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.1 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.	`Yes` : autoriser l'utilisateur demander un accès temporaire à un appareil verrouillé via l'interface graphique ou la ligne de commande de l'application. `No` (valeur par défaut) : interdire l'utilisateur à demander un accès temporaire à un appareil verrouillé.
La section **[DeviceClass]** contient les modes d'accès aux appareils en fonction de leur type.		
`HardDrive`	Spécifie le mode d'accès pour les disques durs connectés à l'appareil client.	`Allow` : l'accès à tous les disques durs est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au disque dur dépend du mode d'accès du bus de connexion sur lequel le disque est connecté. `Block` : l'accès à tous les disques durs (à l'exclusion des disques durs système, qui ne sont jamais bloqués par le Contrôle des applications) est bloqué pour les utilisateurs. `ByRule` : l'accès aux disques durs dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux disques durs, l'écriture est interdite.
`RemovableDrive`	Spécifie le mode d'accès aux disques amovibles connectés à l'appareil client.	`Allow` : l'accès à tous les disque amovibles est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à un disque amovible dépend du mode d'accès du bus de connexion sur lequel le disque est connecté. `Block` : l'accès à tous les disques amovibles est bloqué pour les utilisateurs. `ByRule` : l'accès aux disques amovibles dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux disques amovibles, l'écriture est interdite.
`FloppyDrive`	Spécifie le mode d'accès aux lecteurs de disquettes connectés à l'appareil client. L'application ne bloque pas les lecteurs de disquette connectés à un appareil client via le bus ISA.	`Allow` : l'accès à tous les lecteurs de disquette est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de disquette dépend du mode d'accès du bus de connexion sur lequel la disquette est connectée. `Block` : l'accès à tous les lecteurs de disquette est bloqué pour les utilisateurs. `ByRule` : l'accès aux lecteurs de disquette dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux lecteurs de disquettes uniquement, l'écriture est interdite.

Paramètre	Description	Valeurs
`OpticalDrive`	Spécifie le mode d'accès pour les lecteurs CD/DVD connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs CD/DVD est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de CD/DVD dépend du mode d'accès du bus de connexion via lequel le lecteur de CD/DVD est connecté. `Block` : l'accès à tous les lecteurs de CD / DVD est bloqué pour les utilisateurs. `ByRule` : l'accès aux lecteurs CD/DVD dépend des règles d'accès. `ReadOnly` : les utilisateurs sont autorisés à accéder en lecture seule aux lecteurs de CD/DVD, l'écriture est interdite.
`SerialPortDevice`	Spécifie le mode d'accès aux appareils connectés à l'appareil client via un port série. L'application ne bloque pas les appareils connectés à l'appareil client via un port série via le bus ISA.	`Allow` : l'accès aux appareils connectés via un port série est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil connecté via un port série dépend du mode d'accès pour le bus de connexion. `Block` : l'accès aux appareils connectés via un port série est bloqué pour les utilisateurs.
`ParallelPortDevice`	Spécifie le mode d'accès aux appareils connectés à l'appareil client via un port parallèle.	`Allow` : l'accès aux appareils connectés via un port parallèle est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil connecté via un port parallèle dépend du mode d'accès pour le bus de connexion. `Block` : l'accès aux appareils connectés via un port parallèle est bloqué pour les utilisateurs.
`Printer`	Spécifie le mode d'accès aux imprimantes connectées à l'appareil client.	`Allow` : l'accès à toutes les imprimantes est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'imprimante dépend du mode d'accès du bus de connexion via lequel l'imprimante est connectée. `Block` : l'accès à toutes les imprimantes est bloqué pour les utilisateurs.
`Modem`	Spécifie le mode d'accès aux modems connectés à l'appareil client.	`Allow` : l'accès à tous les modems est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au modem dépend du mode d'accès du bus de connexion via lequel le modem est connecté. `Block` : l'accès à tous les modems est bloqué pour les utilisateurs.
`TapeDrive`	Spécifie le mode d'accès aux lecteurs de bande connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs de bande est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au streamer dépend du mode d'accès du bus de connexion via lequel le streamer est connecté. `Block` : l'accès à tous les lecteurs de bande est bloqué pour les utilisateurs.
`MultifuncDevice`	Spécifie le mode d'accès aux dispositifs multifonctions connectés à l'appareil client.	`Allow` : l'accès à tous les appareils multifonctions est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil multifonction dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils multifonctions est bloqué pour les utilisateurs.
`SmartCardReader`	Spécifie le mode d'accès aux lecteurs de cartes à puce connectés à l'appareil client.	`Allow` : l'accès à tous les lecteurs de cartes à puce est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès au lecteur de carte à puce dépend du mode d'accès au bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les lecteurs de cartes à puce est bloqué pour les utilisateurs.

Paramètre	Description	Valeurs
`WiFiAdapter`	Spécifie le mode d'accès aux adaptateurs Wi-Fi connectés à l'appareil client.	`Allow` : l'accès à tous les adaptateurs Wi-Fi est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur Wi-Fi dépend du mode d'accès pour le bus de connexion. `Block` : l'accès à tous les adaptateurs Wi-Fi est bloqué pour les utilisateurs.
`NetworkAdapter`	Spécifie le mode d'accès aux adaptateurs réseau connectés à l'appareil client.	`Allow` : l'accès à toutes les cartes réseau est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur réseau externe dépend du mode d'accès au bus de connexion sur lequel l'adaptateur est connecté. Le Contrôle des appareils ne vous permet pas de refuser l'accès aux adaptateurs réseau externes pour éviter de déconnecter votre appareil client du réseau.
`PortableDevice`	Spécifie le mode d'accès aux appareils mobiles connectés à l'appareil client.	`Allow` : l'accès à tous les appareils portables est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil portable dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils portables est bloqué pour les utilisateurs.
`BluetoothDevice`	Spécifie le mode d'accès aux dispositifs Bluetooth connectés à l'appareil client.	`Allow` : l'accès à tous les appareils Bluetooth est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil Bluetooth dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils Bluetooth est bloqué pour les utilisateurs.
`ImagingDevice`	Spécifie le mode d'accès aux appareils d'imagerie connectés à l'appareil client.	`Allow` : l'accès à tous les appareils de traitement d'images est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil d'imagerie dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils de traitement d'images est bloqué pour les utilisateurs.
`SoundAdapter`	Spécifie le mode d'accès aux cartes sons connectées à l'appareil client.	`Allow` : l'accès à toutes les cartes audio est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'adaptateur audio dépend du mode d'accès au bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à toutes les cartes audio est interdit pour les utilisateurs.
`InputDevice`	Spécifie le mode d'accès aux appareils de saisie (claviers, souris, pavé tactile et autres) connectés à l'appareil client.	`Allow` : l'accès à tous les appareils d'entrée est autorisé pour les utilisateurs. `DependsOnBus` (valeur par défaut) : l'accès à l'appareil de saisie dépend du mode d'accès du bus de connexion sur lequel l'appareil est connecté. `Block` : l'accès à tous les appareils d'entrée est bloqué pour les utilisateurs.
La section **[DeviceBus]** contient les modes d'accès aux bus de connexion.		
`USB`	Mode d'accès pour les appareils connectés à l'appareil client via l'interface USB.	`Allow` (valeur par défaut) : l'accès à tous les appareils USB est autorisé pour les utilisateurs. `Block` : l'accès à tous les appareils USB est bloqué pour les utilisateurs.

Paramètre	Description	Valeurs
`FireWire`	Mode d'accès pour les appareils connectés à l'appareil client via l'interface FireWire.	`Allow` (valeur par défaut) : l'accès aux appareils connectés via l'interface FireWire est autorisé pour les utilisateurs. `Block` : l'accès aux appareils connectés via l'interface FireWire est bloqué pour les utilisateurs.
La section **[TrustedDevices.item_#]** contient les appareils de confiance.		
`DeviceId`	Spécifie l'ID ou le masque d'ID d'un appareil de confiance.	Vous pouvez utiliser le caractère générique * (n'importe quelle séquence de caractères) ou ? (n'importe quel caractère) pour indiquer l'ID de l'appareil. Exemples : *Pour refuser l'accès à tous les appareils USB à l'exception de celui que vous définissez, indiquez les paramètres suivants :* Dans la section `[DeviceBus]`, le paramètre `USB=Block` Dans la section `[TrustedDevices.item_#]`, indiquez `DeviceId=<identifiant de l'appareil>` *Pour refuser l'accès à tous les appareils USB, mais autoriser l'accès à toutes les clés USB, indiquez les paramètres suivants :* Dans la section `[DeviceBus]`, le paramètre `USB=Block` Dans la section `[TrustedDevices.item_#]`, le paramètre `DeviceId=USBSTOR*`
`Comment`	Commentaire sur l'appareil de confiance spécifié.	—
La section **[TrustedDevices.item_#.Principals.item_#]** contient les règles d'accès à un appareil de confiance.		
`Principal`	L'utilisateur ou le groupe d'utilisateurs pour lesquels l'appareil est approuvé. Si le type d'accès à l'appareil est défini sur lecture seule, lorsque vous attribuez un appareil deconfiance à un utilisateur spécifique, l'utilisateur attribué est ignoré et l'appareil devient accessible en écriture par tous les utilisateurs.	`\Everyone` (valeur par défaut) : l'appareil sera approuvé par tous les utilisateurs. `<nom d'utilisateur>` est le nom d'un utilisateur local ou de domaine pour lequel l'appareil est approuvé (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`). `@<nom de groupe>` est le nom du groupe d'utilisateurs (local ou de domaine) pour lequel l'appareil est approuvé.
La section **[Schedules.item_#]** contient les planifications d'accès pour les appareils. Vous pouvez configurer une programmation uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs CD/DVD.		
`ScheduleName`	Spécifie un nom de planification. Le nom de l'horaire doit être unique.	Valeur par défaut : `Default`. La planification `Default` permet un accès complet aux appareils à tous les utilisateurs à tout moment si l'accès par le bus de connexion est autorisé pour le type d'appareil en question. Vous ne pouvez pas supprimer la planification `Default`.

Paramètre	Description	Valeurs

`DaysHours`	Spécifie des intervalles de temps pour une planification.	`All` (valeur par défaut) : la planification est active 24/7 (aucune limite de temps).
		`< jour de la semaine >` désigne le jour de la semaine. Vous pouvez utiliser les noms complets des jours de la semaine ou leurs abréviations (par exemple, pour lundi, vous pouvez spécifier `Mo`, `Mon` ou `Monday`). Pour les jours de la semaine, vous pouvez spécifier des intervalles ou des jours spécifiques. La semaine commence le dimanche.
		`< heure >` correspond aux heures [0:24]. Pour les heures, vous ne pouvez spécifier que des intervalles.
		Exemples :
		Spécifiez la planification Schedule_1 qui couvre les jours du dimanche au samedi de 0 à 11, de 12 à 15 et de 16 à 24 :
		`[Schedules.item_0001]`
		`ScheduleName=schedule_1`
		`DaysHours=Su-Sa:0..11,12..15,16..24`
		Spécifiez la planification schedule_2 qui couvre les intervalles suivants : les jeudis de 12 à 14 et les vendredis de 2 à 15 et de 16 à 24 :
		`[Schedules.item_0002]`
		`ScheduleName=schedule_2`
		`DaysHours=Th:12..14;Fr:2..15,16..24`
		Spécifiez la planification schedule_3 qui couvre 24 heures/24 et 7 jours par semaine :
		`[Schedules.item_0003]`
		`ScheduleName=schedule_3`
		`DaysHours=All`

La section **[HardDrivePrincipals.item_ #]** contient les règles d'accès aux disques durs. Pour les disques durs, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un disque dur. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom d'un utilisateur local ou de domaine auquel la règle d'accès s'applique (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`). `@< nom de groupe >` est le nom du groupe d'utilisateurs (local ou de domaine) auquel la règle d'accès s'applique.
`[HardDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux disques durs est autorisé. `Block` : l'accès aux disques durs est bloqué.
La section **[RemovableDrivePrincipals.item_ #]** contient les règles d'accès aux disques amovibles. Pour les disques amovibles, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un disque amovible. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		

Paramètre	Description	Valeurs
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom d'un utilisateur local ou de domaine auquel la règle d'accès s'applique (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`). `@< nom de groupe >` est le nom du groupe d'utilisateurs (local ou de domaine) auquel la règle d'accès s'applique.
`[RemovableDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux disques amovibles est autorisé. `Block` : l'accès aux disques amovibles est bloqué.
La section **[FloppyDrivePrincipals.item_ #]** contient les règles d'accès aux disquettes. Pour les lecteurs de disquette, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un lecteur de disquette. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom d'un utilisateur local ou de domaine auquel la règle d'accès s'applique (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`). `@< nom de groupe >` est le nom du groupe d'utilisateurs (local ou de domaine) auquel la règle d'accès s'applique.
`[FloppyDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (par défaut) : l'accès aux lecteurs de disquette est autorisé. `Block` : l'accès aux lecteurs de disquette est bloqué.
La section **[OpticalDrivePrincipals.item_ #]** contient les règles d'accès aux lecteurs CD/DVD. Pour les lecteurs CD/DVD, au moins une planification doit toujours être activée. Vous pouvez attribuer plusieurs règles d'accès à un lecteur CD/DVD. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. En cas de conflits d'accès pour un utilisateur ou un groupe, des droits d'accès minimaux sont accordés.		
`Principal`	Spécifie un utilisateur ou un groupe d'utilisateurs pour lesquels la règle d'accès est appliquée.	`\Everyone` (valeur par défaut) : la règle d'accès s'applique à tous les utilisateurs. `< nom d'utilisateur >` est le nom d'un utilisateur local ou de domaine auquel la règle d'accès s'applique (sans spécifier le nom complet avec le domaine, si le système permet de saisir les noms d'utilisateur dans ce format, ou au format `<nom de domaine>\<nom d'utilisateur>` ou `<nom d'utilisateur>@<nom de domaine>`). `@< nom de groupe >` est le nom du groupe d'utilisateurs (local ou de domaine) auquel la règle d'accès s'applique.
`[OpticalDrivePrincipals.item_#.AccessRules.item_#]` contient les paramètres de la règle d'accès.		
`UseRule`	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'accès est activée. `No` : la règle d'accès est désactivée.

Paramètre	Description	Valeurs
`ScheduleName`	Spécifie la planification définie dans la section `[Schedules.item_#]`.	Valeur par défaut : `Default`.
`Access`	Spécifie le type d'accès.	`Allow` (valeur par défaut) : l'accès aux lecteurs CD/DVD est autorisé. `Block` : l'accès à tous les lecteurs CD/DVD est bloqué.

Afficher et exporter une liste des appareils connectés dans la ligne de commande

Pour consulter la liste des appareils connectés, exécutez la commande suivante :

```
kesl-control --get-device-list [--all] [--json]
```

où :

- `--all` : afficher la liste de tous les appareils connectés.
- `--json` : afficher la liste des appareils connectés au format JSON.

L'application Kaspersky Endpoint Security affiche les informations suivantes sur les appareils connectés :

- **Type d'appareil** Type d'un appareil connecté. Par exemple, `OpticalDrive` ou `HardDrive`.
- **ID**. ID de l'appareil connecté.
- **Nom**. Nom de l'appareil connecté.
- **Chemin d'accès**. Chemin d'accès à l'appareil dans le système d'exploitation virtuel sysfs.
- **Disque système**. Paramètre qui indique si l'appareil connecté est un disque système (oui ou non).
- **Bus**. Bus de connexion. Valeurs possibles : `UnknownBus`, `USB`, `FireWire`.
- **Pilote**. Nom du pilote utilisé, nom lu par le système d'exploitation virtuel sysfs.

Pour exporter la liste des appareils connectés, exécutez la commande suivante :

```
kesl-control --get-device-list --export <fichier>
```

où `<fichier>` est le chemin d'accès complet au fichier JSON dans lequel vous souhaitez enregistrer la liste des appareils connectés.

L'exportation est effectuée au format d'une liste des appareils de confiance.

Administration de la liste des appareils de confiance à partir de la ligne de commande

La liste des appareils de confiance contient des informations sur les appareils dont l'accès est autorisé (pour des utilisateurs ou des groupes spécifiques).

La ligne de commande vous permet de consulter la liste des appareils de confiance, d'y ajouter et d'en supprimer des appareils, et d'importer une liste d'appareils de confiance à partir d'un fichier.

Pour consulter la liste des appareils des confiances, exécutez la commande suivante :

```
kesl-control --trusted-devices --list
```

Pour ajouter un appareil à la liste des appareils de confiance, exécutez la commande suivante :

```
kesl-control --trusted-devices --add <ID>
```

où `<identifiant>` est l'identifiant de l'appareil ou le masque de l'identifiant de l'appareil.

Pour supprimer l'appareil de la liste des appareils de confiance, exécutez la commande suivante :

```
kesl-control --trusted-devices --delete <ID>
```

où `<identifiant>` est l'identifiant de l'appareil ou le masque de l'identifiant de l'appareil.

Pour importer la liste des appareils de confiance à partir d'un fichier, exécutez la commande suivante :

```
kesl-control --trusted-devices --merge|--add|--replace --file <fichier>
```

où :

- `--merge` : fusionner les listes des appareils de confiance lors de l'importation. Si la liste actuelle et la liste importée contiennent des enregistrements pour un appareil ayant le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figurent pas dans la liste actuelle.
- `--add` : compléter la liste actuelle des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.
- `--replace` : remplacer la liste actuelle des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste importée.
- `--file <fichier>` est le chemin complet du fichier JSON à partir duquel la liste des appareils de confiance sera importée.

Autorisation d'accès temporaire à l'appareil

Lors de la configuration du Contrôle des appareils, l'administrateur peut bloquer accidentellement l'accès à un appareil nécessaire au travail d'un utilisateur. Si l'utilisateur pense que l'accès à un appareil ou à son contenu a été bloqué par erreur, il peut demander un accès temporaire à l'appareil bloqué auprès de l'administrateur réseau local de l'organisation.

Il est possible de demander un accès temporaire si l'administrateur a autorisé l'utilisateur à en faire la demande. L'administrateur peut configurer cette autorisation dans les propriétés de la stratégie, soit dans Web Console, soit dans la Console d'administration, soit encore dans les paramètres de la tâche Contrôle des appareils.

La procédure d'autorisation d'accès à un appareil bloqué se déroule comme suit :

1. L'utilisateur crée un *fichier de demande* et le soumet à l'administrateur, par exemple par email ou tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage). L'utilisateur peut demander un accès temporaire à un appareil verrouillé via l'interface graphique ou la ligne de commande de l'application.

2. L'administrateur crée une *clé d'accès* à partir du fichier de requête et la transmet à l'utilisateur, par exemple, par message ou tout autre moyen disponible. L'autorisation d'accès à un appareil bloqué s'effectue dans Web Console.

3. L'utilisateur télécharge la clé d'accès et obtient un accès temporaire à l'appareil verrouillé. L'utilisateur peut télécharger cette clé d'accès via l'interface graphique ou la ligne de commande de l'application.

L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.1 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.

Octroi d'accès à un appareil dans Web Console

L'autorisation d'accéder à un appareil bloqué n'est possible que si Kaspersky Security Center 16.1 est déployé dans l'organisation et que l'appareil client peut établir une connexion avec le Serveur d'administration.

Lorsque l'administrateur reçoit une demande d'accès temporaire d'un utilisateur, il peut créer une clé d'accès à partir du fichier de demande d'accès dans Web Console.

Pour accorder un accès temporaire à un appareil, l'administrateur doit disposer des autorisations de lecture, d'écriture et d'exécution pour la fonction **Chiffrement des données** (**Utilisateurs et rôles** → **Rôles** → <rôle utilisateur> → fenêtre des propriétés du rôle utilisateur → onglet **Droits d'accès** → <nom de l'application> → **Chiffrement des données** → **Lecture/Écriture/Exécution**).

Pour créer une clé d'accès pour un appareil verrouillé :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration qui contient l'appareil dont vous avez besoin et cochez la case en regard de son nom.

3. Au-dessus de la liste des appareils administrés, cliquez sur le bouton **Accorder l'accès à l'appareil en mode hors-ligne**. Si le bouton n'apparaît pas au-dessus de la liste des appareils, cliquez sur le bouton représentant des points de suspension et sélectionnez l'option **Partager cet appareil en mode hors-ligne** dans le menu.

4. Dans la fenêtre **Paramètres de l'application** qui s'ouvre, dans la section **Contrôle des appareils**, cliquez sur le bouton **Parcourir** et chargez le fichier de requête reçu de l'utilisateur.

   Les informations relatives à l'appareil bloqué auquel l'utilisateur a demandé l'accès seront affichées.

5. Si nécessaire, modifiez la valeur en heures dans le champ **Durée d'accès**.

   Par défaut, le champ **Durée d'accès** est défini sur la valeur spécifiée par l'utilisateur lors de la génération du fichier de requête d'accès.

6. Si nécessaire, modifiez la valeur du champ **Spécifiez la période pendant laquelle la clé d'accès peut être utilisée sur l'appareil client**.

   Le champ indique la période pendant laquelle l'utilisateur peut télécharger la clé d'accès.

7. Cliquez sur le bouton **Créer une clé**.

8. Enregistrez le fichier contenant la clé d'accès avec l'extension *.acode.

Obtention d'un accès temporaire à un appareil dans la ligne de commande

Si l'utilisateur estime que le blocage de l'accès à un appareil ou l'interdiction d'une opération sur le contenu de l'appareil s'est produit par erreur, il peut demander un accès temporaire à l'appareil bloqué auprès de l'administrateur du réseau local de l'organisation à l'aide de la commande d'administration du contrôle des appareils `kesl-control --request-temporary-device-access`.

Pour demander un accès temporaire à un appareil verrouillé, exécutez la commande suivante :

```
kesl-control --request-temporary-device-access --device-id <identifiant de l'appareil>
--access-duration <durée d'accès> --path <chemin d'accès au fichier de demande
d'accès>
```

où :

`--device-id <identifiant de l'appareil>` spécifie l'identifiant de l'appareil bloqué auquel vous souhaitez accéder.

`--access-duration <durée d'accès>` spécifie la période pendant laquelle vous souhaitez pouvoir accéder à l'appareil (en heures). Valeurs possibles : 1 à 100.

`--path <chemin d'accès au fichier de demande d'accès>` spécifie le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.

À la suite de l'exécution de la commande, un fichier de demande d'accès sera créé, qui devra être envoyé à l'administrateur, par exemple par courrier électronique ou par tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage).

Après avoir reçu la clé d'accès de l'administrateur, vous devez la charger à l'aide de la commande `kesl-control --upload-temporary-device-access-key` pour obtenir un accès temporaire à l'appareil.

Pour obtenir un accès temporaire à un appareil verrouillé, exécutez la commande suivante :

```
kesl-control --upload-temporary-device-access-key --path <chemin d'accès au fichier contenant la clé d'accès>
```

où :

`--path <chemin d'accès au fichier contenant la clé d'accès>` est le chemin d'accès au fichier contenant la clé d'accès à l'appareil (fichier avec l'extension .acode).

La commande affiche des informations sur l'accès à l'appareil et sur la période pendant laquelle l'accès à cet appareil est accordé.

Contrôle Internet

Le Contrôle Internet gère l'accès des utilisateurs aux ressources Web. Cela vous permet de réduire la consommation de trafic et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur tente d'ouvrir un site dont l'accès est restreint par le Contrôle Internet, Kaspersky Endpoint Security bloque l'accès ou affiche un message d'avertissement indiquant que la visite du site n'est pas recommandée.

Kaspersky Endpoint Security contrôle uniquement le trafic HTTP et HTTPS.

Le Contrôle Internet vous permet de configurer l'accès aux sites des manières suivantes :

- Par catégories de contenu. La catégorisation du contenu des sites est assurée par le service cloud de Kaspersky Security Network, l'analyse heuristique et la base de données de sites connus (qui font partie de la base de données de l'application). Vous pouvez restreindre l'accès des utilisateurs, par exemple, à la catégorie du contenu « Réseaux sociaux » ou à d'autres catégories.

- Par catégories de types de données. Vous pouvez restreindre l'accès des utilisateurs aux données de votre site et, par exemple, masquer les graphiques. L'application détermine le type de données par le format de fichier et non par l'extension.

  L'application n'analyse pas les fichiers dans les archives. Par exemple, si des fichiers image sont archivés, l'application détectera le type de données comme « Archives » plutôt que « Fichiers graphiques ».

- Par adresse Internet. Vous pouvez spécifier une adresse Internet ou un masque d'adresse Internet.

Vous pouvez utiliser plusieurs méthodes pour contrôler l'accès aux sites en même temps. Par exemple, vous pouvez limiter l'accès à la catégorie de type de données « Fichiers des applications Office » à la seule catégorie de contenu « Emails en ligne ».

Par défaut, la *règle par défaut* pour toutes les ressources Web est **Autoriser**. Conformément à cette règle, le Contrôle Internet permet aux utilisateurs d'accéder aux ressources Web à moins que d'autres *règles d'accès aux ressources Web* ne soient spécifiées.

Vous pouvez modifier la règle par défaut du Contrôle Internet, selon laquelle l'application régulera l'accès aux ressources Web qui ne sont pas couvertes par d'autres règles, et définir la *règle par défaut* **Bloquer**. Conformément à cette règle, le Contrôle Internet interdit aux utilisateurs d'accéder aux ressources Web à moins que d'autres *règles d'accès aux ressources Web* ne soient spécifiées.

Si vous avez configuré des exclusions de l'interception du trafic par l'application Kaspersky Endpoint Security, elles affectent le fonctionnement du module Contrôle Internet.

À propos des règles d'accès aux ressources Web

Une *règle d'accès aux ressources Web* est un ensemble de filtres et une action que l'application effectue lorsque les utilisateurs visitent les ressources Web décrites dans la règle à l'heure spécifiée dans le calendrier de la règle. Les filtres vous permettent de spécifier les ressources Web auxquelles le module Contrôle Internet contrôle l'accès.

Les filtres suivants sont disponibles :

- **Filtre par catégorie de contenu**. Le Contrôle Internet peut distribuer des ressources Web dans des catégories de contenu. Vous pouvez contrôler l'accès des utilisateurs aux ressources Web contenant du contenu défini par ces catégories. Lorsque les utilisateurs visitent des ressources Web appartenant à la catégorie de contenu sélectionnée, l'application effectue l'action spécifiée dans la règle.

- **Filtrer par catégories de types de données**. Le Contrôle Internet peut classer les ressources Web en catégories de types de données. Vous pouvez contrôler l'accès des utilisateurs à certains types de données publiées sur les ressources Web. Lorsque les utilisateurs visitent des ressources Web appartenant à la catégorie de type de données sélectionnée, l'application effectue l'action spécifiée dans la règle.

- **Filtrer par adresses de ressources Web**. Vous pouvez contrôler l'accès des utilisateurs à toutes les adresses de ressources Web ou à des adresses de ressources Web individuelles et/ou à des groupes d'adresses de ressources Web.

  Si un filtre par catégories de contenu et/ou catégories de types de données et un filtre par adresses de ressources Web sont spécifiés et que les adresses de ressources Web et/ou groupes d'adresses de ressources Web spécifiés appartiennent aux catégories de contenu ou aux catégories de types de données sélectionnées, l'application contrôle l'accès non pas à toutes les ressources Web de catégories de contenu et/ou de catégories de types de données sélectionnées, mais uniquement à des adresses de ressources Web spécifiées et/ou à des groupes d'adresses de ressources Web.

- **Filtrer par noms d'utilisateurs et groupes d'utilisateurs**. Vous pouvez spécifier des utilisateurs et/ou des groupes d'utilisateurs pour lesquels l'accès aux ressources Web est contrôlé conformément 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**. Vous pouvez définir une planification pour la règle. La planification de la règle détermine l'heure à laquelle l'application contrôle l'accès aux ressources Web spécifiées dans la règle. Par exemple, vous pouvez limiter l'accès à Internet via un navigateur uniquement pendant les heures ouvrables.

Pour chaque règle, vous pouvez spécifier l'action que le Contrôle Internet effectue lorsqu'un utilisateur visite une ressource Web qui répond aux paramètres de la règle :

- *Autoriser.* Le Contrôle Internet permet à l'utilisateur d'accéder à une ressource Web.

- *Bloquer.* Le Contrôle Internet refuse à l'utilisateur l'accès à la ressource Web et affiche un message concernant le refus d'accès. En cliquant sur les liens contenus dans le message de blocage, l'utilisateur peut envoyer un message de réclamation à l'administrateur du réseau local de l'organisation concernant un blocage erroné et demander l'accès à la ressource Web bloquée.

- *Informer.* Le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Web n'est pas recommandée. En cliquant sur les liens contenus dans le message d'avertissement, l'utilisateur peut envoyer un message de réclamation à l'administrateur du réseau local de l'organisation concernant un avertissement erroné. Dans le même temps, l'accès de l'utilisateur à la ressource Web n'est pas bloqué.

Chaque règle a une priorité. Plus une règle figure en haut de la liste, plus sa priorité est élevée. Si un site est ajouté à plusieurs règles, le Contrôle Internet régule l'accès à ce site selon la règle ayant la priorité la plus élevée. Par exemple, une application peut définir un portail d'entreprise comme un réseau social. Pour restreindre l'accès aux réseaux sociaux et fournir l'accès au portail Web d'entreprise, créez deux règles : une règle de refus pour la catégorie du contenu « Réseaux sociaux » et une règle d'autorisation pour le portail Web d'entreprise. La règle d'accès au portail Web d'entreprise doit avoir une priorité plus élevée que la règle d'accès aux réseaux sociaux.

Si aucune règle de refus n'a été créée, le trafic HTTPS n'est pas déchiffré.

Configuration du Contrôle Internet dans Web Console

Dans Web Console, vous pouvez configurer les paramètres du Contrôle Internet dans les propriétés de la stratégie (**Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle Internet**).

Configuration du Contrôle Internet dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle Internet dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Contrôle Internet**).

Paramètres du module Contrôle Internet

Paramètre	Description
Activer le Contrôle Internet	La case active le module Contrôle Internet. La case est décochée par défaut.

Paramètres du Contrôle Internet	Le tableau contient une liste de règles d'accès aux ressources Web. Pendant le fonctionnement, le Contrôle Internet applique les règles dans l'ordre dans lequel elles sont répertoriées dans le tableau.
	Ce tableau contient les colonnes suivantes :
	• **État**. État de fonctionnement de la règle d'accès aux ressources Web :
	  • *Activé* : la règle est activée, le Contrôle Internet applique cette règle pendant son fonctionnement.
	  • *Désactivé* : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle Internet.
	  Vous pouvez cocher ou décocher la case dans le tableau, et vous pouvez cocher ou décocher la case **Utiliser cette règle** dans la fenêtre **Règle du Contrôle Internet**.
	• **Action**. L'action que l'application entreprendra lorsqu'elle détectera une tentative d'accès aux ressources Web qui correspond à la règle.
	• **Nom**. Le nom de la règle d'accès aux ressources Web.
	Vous pouvez ajouter, modifier, supprimer, **déplacer vers le haut** et **déplacer vers le bas** les éléments du tableau.
	Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.
	Ce bouton est accessible si un élément uniquement est sélectionné dans le tableau.
	Vous pouvez également importer la liste des règles d'un fichier à l'aide du bouton **Avancé** → **Importer** et exporter la liste des règles ajoutées vers un fichier à l'aide du bouton **Avancé** → **Exporter les éléments sélectionnés** ou **Avancé** → **Tout exporter**. Lors de l'importation, vous serez invité à remplacer la liste des règles ou à ajouter des règles à une liste existante.

Règle par défaut	Dans la liste déroulante, vous pouvez sélectionner une règle par défaut, selon laquelle l'application régulera l'accès aux ressources Web qui ne sont pas soumises à d'autres règles : • **Autoriser** (valeur par défaut) : autoriser l'accès aux ressources Web. • **Bloquer** : bloque l'accès aux ressources Web.
Modèles de messages	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Modèles de messages**.

Fenêtre Règle du Contrôle Internet

Dans cette fenêtre, vous pouvez configurer les paramètres de la règle d'accès aux ressources Web.

Paramètre	Description
Nom de la règle	Champ de saisie du nom de la règle d'accès aux ressources Web. Le nom de la règle doit être unique.
Utiliser cette règle	La case à cocher active ou désactive l'utilisation de cette règle pendant l'exécution de l'application. Si la case est cochée, la règle est activée, le Contrôle Internet applique cette règle pendant le fonctionnement. Si la case n'est pas cochée, la règle est désactivée et n'est pas utilisée pendant l'exécution du Contrôle Internet. À l'avenir, vous pourrez activer l'utilisation de cette règle par le Contrôle Internet en cochant la case. La case est cochée par défaut.
Filtrer le contenu	Dans la liste déroulante, vous pouvez sélectionner un filtre de contenu de ressource Web : • **Ne pas filtrer** (valeur par défaut). Lorsque vous sélectionnez cet élément de liste, le filtre de contenu des ressources Web n'est pas utilisé. • **Par catégories de contenu**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les catégories de contenu**. • **Par catégories de types de données**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les catégories de types de données**. • **Par catégories de contenu et types de données**. Lorsque vous sélectionnez cet élément de liste, les boutons **Sélectionner** deviennent disponibles. Ces boutons permettent d'ouvrir des fenêtres dans lesquelles vous pouvez sélectionner les catégories nécessaires.
Filtrer les adresses	Dans la liste déroulante, vous pouvez sélectionner un filtre d'adresse de ressource Web : • **Toute adresse** (valeur par défaut). Lorsque cet élément de la liste est sélectionné, le filtre d'adresses des ressources Web n'est pas utilisé ; la règle du Contrôle Internet est appliquée à toutes les adresses des ressources Web. • **Adresses indiquées**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner des adresses** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner des adresses**, dans laquelle vous pouvez sélectionner les adresses des ressources Web nécessaires.
Appliquer aux utilisateurs	Dans la liste déroulante, vous pouvez sélectionner les utilisateurs soumis à la règle d'accès aux ressources web : • **À tous les utilisateurs** (valeur par défaut). Lorsque cet élément de la liste est sélectionné, le filtre des utilisateurs n'est pas utilisé et la règle Contrôle Internet est appliquée à tous les utilisateurs. • **Aux utilisateurs sélectionnés**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner les utilisateurs** devient disponible. Ce bouton permet d'ouvrir la fenêtre **Sélectionner les utilisateurs**.
Horaire des règles	Dans la liste déroulante, vous pouvez configurer le calendrier de la règle d'accès à une ressource Web : • **Toujours** (valeur par défaut). Lorsque vous sélectionnez cet élément de la liste, une règle d'accès personnalisée à une ressource Web est appliquée sans restriction de temps, c'est-à-dire à tout moment. • **<Nom de la planification>**. Lorsque vous sélectionnez cet élément de liste, les boutons **Supprimer** et **Modifier** deviennent disponibles, en cliquant sur lesquels vous pouvez supprimer ou configurer ce calendrier. • **Ajouter un nouvelle planification**. Lorsque vous sélectionnez cet élément de liste, la fenêtre **Planification d'accès** s'ouvre, dans laquelle vous pouvez configurer un nouveau calendrier de fonctionnement de la règle d'accès à la ressource Web.
Action de la règle	Dans la liste déroulante, vous pouvez sélectionner l'action que le Contrôle Internet effectuera lorsqu'il détectera une tentative d'accès à une ressource Web qui correspond à la règle : • **Autoriser** (valeur par défaut) : autoriser l'accès à la ressource Web. • **Bloquer** : bloquer l'accès à la ressource Web et afficher un message concernant le refus d'accès. • **Informer** : afficher un avertissement indiquant que la ressource Web n'est pas recommandée à la visite. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.

Fenêtre Sélectionner les catégories de contenu

Dans cette fenêtre, vous pouvez sélectionner les catégories de contenu dont vous souhaitez contrôler l'accès.

Pour ce faire, cochez les cases à côté des catégories souhaitées.

Toutes les cases sont décochées par défaut.

Lorsque vous cochez les cases en regard de toutes les catégories de sous-contenu, la case en regard de la catégorie de contenu principale qui contient les sous-catégories n'est pas automatiquement sélectionnée.

Fenêtre Sélectionner les catégories de type de données

Cette fenêtre vous permet de sélectionner les catégories de types dont vous souhaitez contrôler l'accès.

Pour ce faire, cochez les cases à côté des catégories souhaitées.

Toutes les cases sont décochées par défaut.

Fenêtre Sélectionner les adresses

Dans cette fenêtre, vous pouvez spécifier les adresses des ressources Web auxquelles vous souhaitez contrôler l'accès des utilisateurs. Vous pouvez spécifier plusieurs adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie. Vous pouvez utiliser des masques pour spécifier des adresses.

Si vous souhaitez spécifier un groupe d'adresses, ouvrez la fenêtre **Sélectionner des groupes d'adresses**, en cliquant sur le bouton **Ajouter un groupe d'adresses**.

Fenêtre Sélectionner un groupe d'adresses

Le tableau contient des groupes d'adresses de ressources Web auxquelles l'accès des utilisateurs est contrôlé par le module Contrôle Internet.

Si vous souhaitez ajouter un groupe d'adresses à la liste des groupes dans la fenêtre **Sélectionner les adresses**, cochez la case en regard du nom du groupe dans le tableau et cliquez sur le bouton **Ajouter** situé sous le tableau.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Si vous souhaitez ajouter un nouveau groupe d'adresses à la liste des groupes de cette fenêtre, ouvrez la fenêtre **Ajout d'un groupe d'adresses** en cliquant sur le bouton **Ajouter** situé au-dessus du tableau.

Par défaut, le tableau est vide.

Fenêtre Ajout d'un groupe d'adresses

Dans cette fenêtre, vous pouvez spécifier des groupes d'adresses de ressources Web auxquels vous souhaitez contrôler l'accès des utilisateurs. Vous pouvez spécifier plusieurs adresses dans un groupe d'adresses ; dans ce cas, indiquez chaque adresse sur une nouvelle ligne pour faciliter la copie. Vous pouvez utiliser des masques pour spécifier des adresses.

Fenêtre Sélectionner les utilisateurs

Le tableau contient les noms et les groupes d'utilisateurs pour lesquels l'accès aux ressources Web est contrôlé conformément à la règle.

Vous pouvez ajouter, modifier ou supprimer des éléments dans le tableau

Si vous souhaitez ajouter un nouvel utilisateur et/ou groupe d'utilisateurs à la liste des utilisateurs de cette fenêtre, en cliquant sur le bouton **Ajouter** situé au dessus du tableau, ouvrez la fenêtre **Utilisateur ou groupe**.

Par défaut, le tableau est vide.

Fenêtre Utilisateur ou groupe

Dans cette fenêtre, vous pouvez spécifier l'utilisateur ou le groupe d'utilisateurs auquel s'applique la règle d'accès aux ressources Web.

Configuration des règles d'accès aux ressources Web

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Utilisateur ou groupe	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle s'applique.

Fenêtre Planification d'accès

Dans cette fenêtre, vous pouvez configurer le calendrier d'accès aux ressources Web.

Calendrier d'accès aux ressources Web

Paramètre	Description
Nom	Champ de saisie du nom de la planification d'accès.
Intervalles de temps	Tableau qui permet de préciser des intervalles de temps pour la planification (jours et heures). Les intervalles surlignés en vert sont inclus dans la planification. Pour exclure un intervalle de la planification, cliquez sur les cellules correspondantes. Les intervalles exclus de la planification sont surlignés en gris. Par défaut, tous les intervalles (24/7) sont inclus dans la planification.

Configuration des modèles de messages du Contrôle Internet

En fonction de l'action spécifiée dans les propriétés des règles du Contrôle Internet, lorsque l'utilisateur tentent d'accéder aux ressources Web, l'application affiche un message (remplace la réponse du serveur HTTP par une page HTML contenant un message) de l'un des types suivants :

- Message d'alerte. Ce message avertit l'utilisateur que la visite de la ressource Web n'est pas recommandée et/ou n'est pas conforme à la politique de sécurité de l'entreprise. L'application affiche un message d'avertissement si l'action **Informer** est sélectionnée dans les paramètres de la règle décrivant cette ressource Web.

  Si, de l'avis de l'utilisateur, l'avertissement est erroné, en utilisant le lien de l'avertissement, l'utilisateur peut envoyer un message de réclamation déjà généré à l'administrateur du réseau local de l'organisation.

- Message de ressource Web bloquée L'application affiche un message sur le blocage d'une ressource Web, si l'action **Bloquer** est sélectionnée dans les paramètres de la règle qui décrit cette ressource Web.

  Si, de l'avis de l'utilisateur, le blocage de l'accès à une ressource Web était erroné, en utilisant le lien du message concernant le blocage de la ressource Web, l'utilisateur peut envoyer un message de réclamation déjà généré à l'administrateur du réseau local de l'organisation.

Des modèles sont fournis pour un message de réclamation, un message concernant le blocage de l'accès à une ressource Web et un message à envoyer à l'administrateur du réseau local de l'organisation. Vous pouvez modifier leur contenu.

Pour modifier le modèle de message dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Stratégies et profils de stratégies**.

   La liste des stratégies s'ouvre.

2. Sélectionnez le groupe d'administration contenant les appareils sur lesquels la stratégie est appliquée. Pour cela, cliquez sur le lien dans le champ Chemin actuel dans la partie supérieure de la fenêtre et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   La liste affichera les stratégies configurées pour le groupe d'administration sélectionné.

3. Cliquez sur le nom de la stratégie souhaitée dans la liste.

   La fenêtre des propriétés de la stratégie s'ouvre.

4. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Paramètres de l'application** → **Security Controls** → **Web Control**.

5. Dans le groupe **Modèles de messages**, configurez les modèles de messages du Contrôle Internet sous les onglets suivants :

   - **Avertissement**. Le champ de saisie contient un modèle de message qui apparaît lorsqu'une règle est déclenchée, avertissant d'une tentative d'accès à une ressource Web non recommandée.

   - **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 champ de saisie contient un modèle de message de réclamation à envoyer à l'administrateur du réseau local de l'organisation si, de l'avis de l'utilisateur, l'accès à la ressource Web a été bloqué par erreur. Lorsqu'un utilisateur demande l'autorisation d'accéder, l'application Kaspersky Endpoint Security envoie à Kaspersky Security Center un événement *Message à l'administrateur concernant l'accès refusé à une page Web*. La description de l'événement contient un message destiné à l'administrateur avec des variables substituées. Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'y a pas de connexion avec le Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Sous les onglets **Avertissement et Notification sur le blocage**, vous pouvez ajouter des variables et des liens aux messages destinés à l'utilisateur en cliquant sur les boutons **Ajouter une variable** et **Ajouter un lien**.

   Vous pouvez restaurer le texte du modèle de message en cliquant sur le bouton **Restaurer défaut**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Pour modifier le modèle de message dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration contenant les appareils requis.

2. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

3. Dans la liste des stratégies, sélectionnez la stratégie souhaitée et ouvrez la **fenêtre Propriétés : <Nom de la stratégie>** par double-clic.

   Vous pouvez également ouvrir la fenêtre des propriétés de la stratégie à l'aide de l'élément **Propriétés** du menu contextuel de la stratégie ou en cliquant sur le lien **Configurer les paramètres de stratégie** situé à droite de la liste des stratégies dans le groupe contenant les paramètres de stratégie.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de sécurité** → **Contrôle Internet**.

5. Dans la section **Modèles** de messages, cliquez sur le bouton **Configurer**.

6. Dans la fenêtre **Modèles de messages** qui s'ouvre, configurez les modèles de messages du Contrôle Internet sous les onglets suivants :

   - **Avertissement**. Le champ de saisie contient un modèle de message qui apparaît lorsqu'une règle est déclenchée, avertissant d'une tentative d'accès à une ressource Web non recommandée.

   - **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.

   - **Plainte auprès de l'administrateur**. Le champ de saisie contient un modèle de message de réclamation à envoyer à l'administrateur du réseau local de l'organisation si, de l'avis de l'utilisateur, l'accès à la ressource Web a été bloqué par erreur. Lorsqu'un utilisateur demande l'autorisation d'accéder, l'application Kaspersky Endpoint Security envoie à Kaspersky Security Center un événement *Message à l'administrateur concernant l'accès refusé à une page Web*. La description de l'événement contient un message destiné à l'administrateur avec des variables substituées. Vous pouvez afficher ces événements dans la Console d'administration de Kaspersky Security Center à l'aide de la sélection prédéfinie **Demandes des utilisateurs**. Si Kaspersky Security Center n'est pas déployé dans votre organisation ou s'il n'y a pas de connexion avec le Serveur d'administration, l'application enverra un message à l'administrateur à l'adresse email indiquée.

   Sous les onglets **Avertissement** et **Message sur le blocage**, vous pouvez ajouter des variables et des liens vers des textes de message destinés à l'utilisateur à l'aide des boutons **Variable** et **Lien**.

   Vous pouvez restaurer le texte du modèle de message en cliquant sur le bouton **Par défaut**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Appliquer**.

Configuration du Contrôle Internet dans la ligne de commande

Sur la ligne de commande, vous pouvez gérer le Contrôle Internet à l'aide de la tâche prédéfinie Contrôle Internet (*Web_Control*).

La tâche Contrôle Internet est arrêtée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du Contrôle Internet, en modifiant les paramètres de la tâche prédéfinie Contrôle Internet.

Vous pouvez également afficher et configurer les paramètres du Contrôle Internet à l'aide des commandes de gestion du Contrôle Internet.

Paramètres de la tâche Contrôle Internet

Le tableau ci-dessous décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez spécifier pour la tâche Contrôle Internet.

Paramètres de la tâche Contrôle Internet

Paramètre	Description	Valeurs
`WebControlDefaultAction`	La règle par défaut, c'est-à-dire l'action que Contrôle Internet effectuera lorsqu'il détectera une tentative d'accès à des ressources Web qui ne sont pas couvertes par d'autres règles.	`Allow` (valeur par défaut) : autoriser l'accès aux ressources Web. `Block` : bloque l'accès aux ressources Web.
`ComplaintRecipient`	L'adresse email de l'administrateur pour lui envoyer un message concernant un blocage erroné d'une ressource Web.	
La section **[Rules.item_#]** contient les paramètres suivants :		
`Name`	Le nom de la règle d'accès aux ressources Web. Le nom de la règle doit être unique.	
`WebControlAction`	Action de la règle que le Contrôle Internet exécutera lorsqu'il détectera une tentative d'accès à une ressource Web qui satisfait à la règle.	`Allow` (valeur par défaut) : autoriser l'accès à la ressource Web. `Block` : interdire l'accès à une ressource Web. `Notify` : afficher un avertissement indiquant que la ressource Web n'est pas recommandée à la visite. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.
`Enabled`	État de fonctionnement de la règle d'accès aux ressources Web.	`Yes` : la règle est activée, le Contrôle Internet applique cette règle pendant son fonctionnement. `No` (valeur par défaut) : la règle est désactivée et n'est pas prise en compte lors du fonctionnement du Contrôle Internet.
`ScheduleId`	Identifiant de calendrier utilisé dans la section `[Schedules.item_#]`.	
`UseUrls`	Utilisation d'un filtre d'adresses de la ressource Web dans une règle.	`Yes` : utiliser un filtre pour les adresses des ressources Web dans une règle. `No` (valeur par défaut) : ne pas utiliser le filtre pour les adresses des ressource Web, appliquer la règle à toutes les adresses des ressources Web.
`Urls.item_#`	L'adresse de la ressource Web, dont l'accès est réglementé par la règle.	Vous pouvez utiliser des masques pour spécifier l'adresse d'une ressource Web.

Paramètre	Description	Valeurs
`UseCategories`	Utilisation de filtres dans une règle par catégories de contenu et par catégories de types de données.	`None` (valeur par défaut) : ne pas utiliser le filtre de contenu des ressources Web. `ContentOnly` : utiliser un filtre par catégories de contenu dans la règle. `FormatOnly` : utiliser un filtre pour les catégories de types de données dans la règle. `ContentAndFormat` : utiliser un filtre dans la règle par catégories de contenu et catégories de types de données.
`[Rules.item_#.ContentCategories.item_#]`	Section pour indiquer la catégorie de contenu.	–
`ContentCategory`	Catégorie de contenu.	`AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITools`
`[Rules.item_#.FormatCategories.item_#]`	Section pour spécifier la catégorie de types de données.	–
`FormatCategories.item_#.FormatCategory`	Catégorie de types de données.	`Video` : vidéo `Audio` : données sonores `OfficeDocument` : fichiers des applications Office `Executable` : fichiers exécutables `Archives` : archives `Images` : fichiers graphiques `Scripts` : scripts
`UsePrincipals`	Utilisation d'un filtre pour les utilisateurs soumis à une règle d'accès aux ressources Web.	`Yes` : utiliser un filtre utilisateur dans la règle. `No` (valeur par défaut) : ne pas utiliser le filtre utilisateur, appliquer la règle à tous les utilisateurs.
`[Rules.item_#.Principals.item_#]`	Section permettant de spécifier les utilisateurs soumis à la règle d'accès aux ressources Web.	
`Name`	Utilisateur ou groupe d'utilisateurs soumis à une règle d'accès aux ressources Web.	`< nom d'utilisateur >` est le nom de l'utilisateur auquel la règle s'applique. `@< nom de groupe >` est le nom du groupe d'utilisateurs auquel la règle s'applique. Valeur par défaut : la règle d'accès aux ressources Web est appliquée à tous les utilisateurs.
La section **[UrlCategories.item_#]** contient les paramètres suivants :		
`Name`	Nom du groupe d'adresses des ressources Web auquel la règle régule l'accès.	

Paramètre	Description	Valeurs
`Urls.item_#`	L'adresse d'une ressource Web incluse dans le groupe.	Vous pouvez utiliser des masques pour spécifier l'adresse d'une ressource Web.
La section **[Schedules.item_#]** contient le calendrier de fonctionnement d'une règle.		
`Id`	Identifiant de calendrier utilisé dans la section `[Rules.item_#]`.	`1 – 999999` `0` : l'identifiant du calendrier `Default` (par défaut) qui garantit que la règle s'exécute sans restriction de temps, c'est-à-dire à tout moment.
`Name`	Spécifie un nom de planification.	
`DaysHours`	Spécifie des intervalles de temps pour une planification.	`< jour de la semaine >` désigne le jour de la semaine. Vous pouvez utiliser les noms complets des jours de la semaine ou leurs abréviations (par exemple, pour lundi, vous pouvez spécifier `Mo`, `Mon` ou `Monday`). Pour les jours de la semaine, vous pouvez spécifier des intervalles ou des jours spécifiques. La semaine commence le dimanche. `< heure >` correspond aux heures [0:24]. Pour les heures, vous ne pouvez spécifier que des intervalles.

Affichage et modification des paramètres de contrôle Internet

Pour afficher les paramètres du Contrôle Internet, exécutez la commande suivante :

```
kesl-control --get-settings 26 [--file < chemin d'accès au fichier de configuration >] [--json]
```

où :

`--file < chemin d'accès au fichier de configuration >` est le chemin d'accès complet au fichier de configuration dans lequel les paramètres seront écrits.

`--json` : afficher les données au format JSON.

Pour modifier les paramètres du Contrôle Internet, exécutez la commande suivante :

```
kesl-control --set-settings 26 [--file < chemin d'accès au fichier de configuration >] [--json]
```

où :

`--file < chemin d'accès au fichier de configuration >` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés.

`--json` : importer les données d'un fichier au format JSON.

Pour supprimer les paramètres configurés et restaurer les paramètres du Contrôle Internet aux valeurs règle par défaut, exécutez la commande suivante :

```
kesl-control --set-settings 26 --set-to-default
```

Règles de formation des masques d'adresses de ressources Web

L'utilisation d'*un masque d'adresse de ressource Web* (ci-après également appelé « masque d'adresse ») peut être pratique dans les cas où, lors du processus de création d'une règle d'accès aux ressources Web, vous devez saisir de nombreuses adresses de ressources Web similaires. Un masque d'adresse bien formé peut remplacer de nombreuses adresses de ressources Web.

Lors de la génération d'un masque d'adresse, les règles suivantes doivent être utilisées :

1. Le caractère `*` remplace toute séquence de zéro ou plusieurs caractères.

   Par exemple, lorsque vous saisissez le masque d'adresse `*abc*`, la règle d'accès aux ressources Web est appliquée à toutes les adresses contenant la séquence `abc`. Exemple : `http://www.example.com/page_0-9abcdef.html`.

2. Séquence de caractères `*.` vous permet de sélectionner tous les domaines d'adresse : *masque de domaine*. Masque de domaine `*.` est traité comme n'importe quel nom de domaine, nom de sous-domaine ou chaîne vide.

   Exemple : les adresses suivantes sont soumises au masque `*.example.com` :

   - `http://pictures.example.com` – le masque de domaine `*.` correspond à `pictures.`
   - `http://user.pictures.example.com` – le masque de domaine `*.` correspond à `pictures.` et `user.`
   - `http://example.com` : masque de domaine `*.` est traité comme une chaîne vide.

3. La séquence de caractères `www.` au début du masque d'adresse est interprété comme la séquence `*.`

   Exemple : le masque d'adresse `www.example.com` est interprété comme `*.example.com`. Le masque couvre les adresses `www2.example.com` et `www.pictures.example.com`.

4. Si le masque d'adresse ne commence pas par le caractère `*`, alors le contenu du masque d'adresse est équivalent au même contenu préfixé par `*.`

5. Si un masque d'adresse se termine par un caractère autre que `/` ou `*`, alors le contenu du masque d'adresse est équivalent au même contenu avec un suffixe `/*`.

   Exemple : le masque d'adresse `http://www.example.com` comprend des adresses de la forme `http://www.example.com/abc`, où `a`, `b`, `c` sont des caractères quelconques.

6. Si un masque d'adresse se termine par un caractère `/`, alors 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 ressources Web à l'aide du masque d'adresse s'effectue en tenant compte du schéma (http ou https) :

   - S'il n'y a pas de protocole réseau dans le masque d'adresse, alors une adresse avec n'importe quel protocole réseau relève du masque d'adresse.

     Exemple : le masque d'adresse `example.com` comprend les adresses `http://example.com` et `https://example.com`.

   - Si un protocole réseau est présent dans le masque d'adresse, seules les adresses ayant le même protocole réseau que le masque d'adresse sont couvertes par le masque d'adresse.

     Exemple : le masque d'adresse `http://*.example.com` est soumis à l'adresse `http://www.example.com`, mais pas à l'adresse `https://www.example.com`.

9. Un masque d'adresse entre guillemets est traité sans tenir compte d'éventuelles substitutions supplémentaires, à l'exception du caractère `*`, s'il est initialement inclus dans le masque d'adresse. Pour les masques d'adresse entre guillemets doubles, les règles 5 et 7 ne sont pas suivies (voir les exemples 14 à 18 dans le tableau ci-dessous).

10. Lors de la comparaison avec un masque d'adresse de ressource Web, le nom d'utilisateur et le mot de passe, le port de connexion et la casse des caractères ne sont pas pris en compte.

Exemples d'application des règles de génération des masques d'adresses

Non.	Masque d'adresse	Adresse vérifiée de la ressource Web	L'adresse vérifiée satisfait-elle 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	Voir règles 3, 2, 1.
7	www.example.com	https://www.example.com	Oui	Voir règles 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Oui	Voir règles 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Oui	Voir règles 3, 5, 1.
10	example.com	http://www.example.com	Oui	Voir 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	Voir règles 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Oui	Voir règles 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Oui	Voir 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 de la ressource Web.

Contrôle de l'intégrité du système

L'application Kaspersky Endpoint Security vous permet de surveiller l'intégrité du système d'exploitation de l'appareil protégé en temps réel et à la demande.

- Le module *Contrôle de l'intégrité du système* vous permet de surveiller en temps réel les modifications apportées aux fichiers et répertoires que vous avez inclus dans la zone de surveillance dans les paramètres du module. Vous pouvez surveiller les modifications apportées aux fichiers pouvant indiquer une faille de sécurité sur l'appareil protégé.

- À l'aide des tâches *Vérification de l'intégrité du système*, vous pouvez vérifier les modifications apportées aux fichiers et répertoires que vous avez inclus dans la zone de surveillance en comparant l'état actuel de l'objet surveillé avec un état précédemment capturé.

Pour utiliser la fonctionnalité de surveillance de l'intégrité du système, une licence incluant cette fonctionnalité est requise.

Après avoir détecté les modifications apportées aux fichiers et répertoires dans la zone de surveillance, Kaspersky Endpoint Security génère des événements sur les modifications dans les listes de contrôle d'accès aux objets. Le module Contrôle de l'intégrité du système ne transmet pas de données sur les modifications exactes qui ont été apportées. La tâche *Vérification de l'intégrité du système* rapporte des informations sur les attributs modifiés et les fichiers et répertoires déplacés.

Surveillez l'intégrité du système en temps réel

Le module Contrôle de l'intégrité du système vous permet de déterminer chaque modification apportée à un objet inclus dans la zone de surveillance en interceptant les opérations sur les fichiers en temps réel.

Pendant l'exécution du module Contrôle de l'intégrité du système, l'application contrôle les modifications apportées aux paramètres de fichier suivants :

- Contenu (write (), truncate (), etc.).

- Métadonnées (possession rights (chmod / chown)).

- Horodateurs (utimensat).

- Attributs étendus (setxattr) et autres.

La somme de contrôle du fichier n'est pas calculée.

Les restrictions technologiques du système d'exploitation Linux empêchent une application de déterminer quel utilisateur ou processus a apporté une modification à un fichier.

Par défaut, le contrôle de l'intégrité du système est désactivé. Vous pouvez activer ou désactiver le contrôle de l'intégrité du système, ainsi que configurer les paramètres de fonctionnement du module :

- Définir les périmètres de surveillance pour le Contrôle de l'intégrité du système L'application surveille les opérations sur les fichiers dans les zones de surveillance spécifiées dans les paramètres du module Contrôle de l'intégrité du système. Pour que le module fonctionne, vous devez spécifier au moins une zone de surveillance. Par défaut, la zone de contrôle des *Objets internes de Kaspersky* (/opt/kaspersky/kesl/) est définie.

  Vous pouvez définir plusieurs zones de contrôle. Vous pouvez modifier en temps réel les zones de contrôle.

  > L'application ne contrôle pas les modifications des fichiers (attributs et contenu) avec des liens matériels qui ne se trouvent pas dans une zone de contrôle.

- Configurer l'exclusion des objets du contrôle de la surveillance par masque de nom.

- Configurer les zones d'exclusion pour contrôler l'intégrité du système. Les exclusions sont définies pour chaque zone de surveillance individuelle et ne fonctionnent que pour la zone spécifiée. Vous pouvez définir plusieurs zones d'exclusion du contrôle.

  Une exclusion a une priorité plus élevée que la zone de surveillance ; l'objet exclu n'est pas analysé, même s'il se trouve dans la zone de surveillance. Si une zone de surveillance est définie à un niveau inférieur au répertoire spécifié dans l'exclusion, l'application ne surveille pas cette zone de surveillance pendant la surveillance de l'intégrité du système.

> Lors de l'ajout d'un répertoire à une zone de surveillance ou à une zone d'exclusion, l'application ne vérifie pas si le répertoire existe.

Configuration du contrôle de l'intégrité du système dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de surveillance de l'intégrité du système dans les propriétés de la stratégie (**Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle de l'intégrité du système**).

Configuration du contrôle de l'intégrité du système dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres du Contrôle de l'intégrité du système dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Contrôle de l'intégrité du système**).

Paramètres du Contrôle de l'intégrité du système

Paramètre	Description
Activer le Contrôle de l'intégrité du système	La case active ou désactive le module Contrôle de l'intégrité du système. La case est décochée par défaut.
Zones de contrôle	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'analyse**.

Paramètre	Description
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'exclusion**.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre Exclusions d'après le masque.

Fenêtre Zones d'analyse

Le tableau contient les zones de contrôle pour le module Contrôle de l'intégrité du système. L'application contrôle les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone de contrôle **Objets internes de Kaspersky** (/opt/kaspersky/kesl/).

Paramètres Zones de contrôle

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone	Nom de la Zones de contrôle.
Chemin	Chemin au répertoire que l'application protège.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer des zones de contrôle pour le module du Contrôle de l'intégrité du système.

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone de contrôle. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application contrôle cette zone de contrôle pendant le fonctionnement de l'application. Si cette case est décochée, l'application ne contrôle pas cette zone de contrôle pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone de contrôle. Le champ ne peut être vide. Le chemin /opt/kaspersky/kesl est défini par défaut.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Zones d'exclusion

La fenêtre contient les zones d'exclusion du contrôle pour le module Contrôle de l'intégrité du système. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu du contrôle.
État	L'état indique si l'application exclut cette zone de l'analyse lorsque la tâche est exécutée.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer une liste des zones d'exclusion à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones d'exclusion vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones d'exclusion ou à ajouter des zones d'exclusion à une liste existante.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion du contrôle pour le module Contrôle de l'intégrité du système.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'exclusion**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone de surveillance pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone du contrôle pendant le fonctionnement du module. Si cette case est décochée, l'application ne contrôle pas cette zone pendant le fonctionnement du module. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion. Le champ ne peut être vide. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.

Paramètre	Description
Masques	La liste contient les masques des noms des objets exclus de la surveillance par l'application. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de la surveillance. Exemples : Le masque `*.txt` fait référence à tous les fichiers texte. Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets du contrôle, en fonction d'un masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de la surveillance.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Configuration du Contrôle de l'intégrité du système en ligne de commande

À partir de la ligne de commande, vous pouvez gérer le contrôle de l'intégrité du système en temps réel à l'aide de la tâche prédéfinie du contrôle de l'intégrité du système (*System_Integrity_Monitoring*). Type de tâche : *OAFIM*.

La tâche Contrôle de l'intégrité du système n'est pas exécutée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres du contrôle de l'intégrité du système sur l'appareil en modifiant les paramètres de la tâche prédéfinie Contrôle de l'intégrité du système.

Paramètre	Description	Valeurs
`UseExcludeMasks`	Active l'exclusion de la zone de contrôle des objets définis par le paramètre `ExcludeThreats.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion du contrôle des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez indiquer plusieurs masques. Chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.
La section **[ScanScope.item_#]** définit les zones de contrôle que la tâche Contrôle de l'intégrité du système doit surveiller. Il faut définir au moins une zone de contrôle pour la tâche. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Active l'analyse de la zone de contrôle.	`Yes` (valeur par défaut) : surveille la zone indiquée. `No` : ne surveille pas une zone indiquée.
`Path`	Chemin d'accès au répertoire à surveiller.	Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Valeur par défaut : /opt/kaspersky/kesl/
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (contrôler tous les objets).
[ExcludedFromScanScope.item_#] contient les objets à exclure de toutes les sections [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone de surveillance indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée de la surveillance. `No` : n'exclut pas la zone indiquée de la surveillance.

Paramètre	Description	Valeurs
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la surveillance.	Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. La valeur par défaut n'est pas définie.
`AreaMask.item_#`	Restriction de la zone d'exclusion du contrôle. Dans la zone d'exclusion du contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets du contrôle).

Vérification de l'intégrité du système

Au cours de la tâche *Vérification de l'intégrité du système*, une modification de chaque objet est déterminée en comparant l'état actuel de l'objet surveillé avec l'état initial. Des comparaisons peuvent être faites en utilisant les critères suivants :

- Somme de hachage du fichier
- heure de modification du fichier ;
- Taille du fichier

L'état initial des objets surveillés est enregistré sous forme d'*instantané de l'état du système*. La référence contient les chemins vers les objets surveillés et leurs métadonnées.

La référence peut contenir des données personnelles.

Un instantané du système est pris la première fois qu'une tâche de vérification de l'intégrité du système est exécutée sur un appareil. Si vous avez créé plusieurs tâches de vérification de l'intégrité du système, un instantané du système distinct est créé pour chaque tâche. La tâche s'exécute uniquement si l'instantané de l'état du système contient des informations sur les objets appartenant à la zone de surveillance configurée pour la tâche. Si la référence ne correspond pas à la zone de contrôle, l'application Kaspersky Endpoint Security génère un événement à propos de la violation de l'intégrité du système.

L'instantané de l'état du système est mis à jour chaque fois que les paramètres de la tâche sont modifiés (par exemple, lors de l'ajout d'une nouvelle zone de surveillance), ainsi que lorsque la tâche est démarrée avec `RebuildBaseline=Yes` paramètre (ou si la case **Actualiser l'instantané de l'état du système à chaque démarrage de la tâche** est sélectionnée dans les propriétés de la tâche dans Kaspersky Security Center).

L'application crée un stockage pour les instantanés de l'état du système sur l'appareil protégé. Par défaut, le stockage des références s'opère dans /var/opt/kaspersky/kesl/private/fim.db. L'accès à une base de données contenant des références requiert des privilèges root.

Vous pouvez supprimer un instantané du système en supprimant la tâche de vérification de l'intégrité du système associée.

Vous pouvez exécuter une vérification de l'intégrité du système à la demande et configurer les paramètres d'analyse :

- Activer ou désactiver la mise à jour de l'instantané de l'état du système à chaque fois que la tâche de vérification de l'intégrité du système est terminée.
- Sélectionnez les critères selon lesquels l'état actuel du fichier surveillé est comparé à l'état initial : utilisez le hachage et l'heure de modification du fichier ou simplement la taille du fichier.
- Configurer les zones de surveillance pour vérifier l'intégrité du système.
- Configurer les zones d'exclusion des vérifications d'intégrité du système. Vous pouvez spécifier des chemins d'accès aux fichiers et répertoires exclus et exclure des objets individuels par masque de nom.

Contrôle de l'intégrité du système dans Web Console

Dans Web Console, vous pouvez effectuer des vérifications de l'intégrité du système à l'aide de la tâche *Vérification de l'intégrité du système*.

Vous pouvez créer et lancer des tâches personnalisées de vérification de l'intégrité du système. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Paramètres de la tâche Vérification de l'intégrité du système

Paramètre	Description
Actualiser l'instantané de l'état du système à chaque démarrage de la tâche	Cette case active ou désactive la recréation d'une ligne de base de système chaque fois que la tâche *Vérification de l'intégrité du système* est démarrée. La case est décochée par défaut.
Utiliser le hachage SHA256 pour l'analyse	La case active ou désactive l'utilisation du hachage du fichier comme critère de comparaison de l'état actuel du fichier avec l'état d'origine. Si la case n'est pas cochée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique). La case est décochée par défaut.
Surveiller les répertoires des zones de contrôle	Cette case active ou désactive l'analyse des répertoires pendant l'exécution de la vérification de l'intégrité du système. La case est décochée par défaut.
Surveiller l'heure du dernier accès au fichier	Cette case active ou désactive le suivi du temps d'accès au fichier pendant l'exécution de la vérification de l'intégrité du système. La case est décochée par défaut.

Paramètre	Description
Zones de contrôle	Un tableau contenant les zones de contrôle vérifiées par la tâche. Par défaut, le tableau contient la zone de contrôle des **Objets internes de Kaspersky** (/opt/kaspersky/kesl/). Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les zones de montage dans le tableau. Vous pouvez également importer une liste des zones de surveillance à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des zones de surveillance vers un fichier au format JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des zones de surveillance ou à ajouter des zones de surveillance à une liste existante.

Fenêtre d'ajout d'une zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer une zone de contrôle pour la tâche Vérification de l'intégrité du système.

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone	Champ de saisie du nom de la zone de contrôle. Ce nom sera affiché dans le tableau de la section **Paramètres d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application contrôle cette zone de contrôle pendant le fonctionnement de l'application. Si cette case est décochée, l'application ne contrôle pas cette zone de contrôle pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone de contrôle. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide. Le chemin **/** est renseigné par défaut : l'application analyse tous les répertoires du système de fichiers local.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Zones d'exclusion

Vous pouvez également configurer les zones d'exclusion de l'analyse et les exclusions selon un masque pour la tâche Vérification de l'intégrité dans la section **Zones d'exclusion**.

Fenêtre Zones d'exclusion

Le tableau contient les zones d'exclusion du contrôle pour la tâche Vérification de l'intégrité du système. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau est vide.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu du contrôle.
État	L'état indique si l'application exclut cette zone du contrôle lorsque la tâche fonctionne.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Fenêtre d'ajout d'une zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion du contrôle pour la tâche Vérification de l'intégrité du système.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone de surveillance pendant le fonctionnement de l'application. Si cette case est cochée, l'application exclut cette zone du contrôle lorsque la tâche est exécutée. Si cette case est décochée, l'application ne contrôle pas cette zone lorsque la tâche est exécutée. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Masques	La liste contient les masques des noms des objets exclus de la surveillance par l'application. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets du contrôle, en fonction d'un masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Contrôle de l'intégrité du système dans la Console d'administration

Dans la Console d'administration, vous pouvez vérifier l'intégrité du système à l'aide de la tâche *Vérification de l'intégrité du système*.

Vous pouvez créer et lancer des tâches personnalisées de vérification de l'intégrité du système. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Dans la section **Paramètres** dans les propriétés de la tâche Vérification de l'intégrité du système, vous pouvez configurer les paramètres indiqués dans le tableau ci-dessous.

Paramètres de la tâche Vérification de l'intégrité du système

Paramètre	Description
Actualiser l'instantané de l'état du système à chaque démarrage de la tâche	Cette case active ou désactive la recréation d'une ligne de base de système chaque fois que la tâche Vérification de l'intégrité du système est démarrée. La case est décochée par défaut.
Utiliser le hachage SHA256 pour l'analyse	La case active ou désactive l'utilisation du hachage du fichier comme critère de comparaison de l'état actuel du fichier avec l'état d'origine. Si la case n'est pas cochée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique). La case est décochée par défaut.
Surveiller les répertoires des zones de contrôle	La case active ou désactive la vérification des répertoires dans les zones de surveillance spécifiées lors des vérifications de l'intégrité du système. La case est décochée par défaut.

Paramètre	Description
Surveiller l'heure du dernier accès au fichier	Cette case active ou désactive le suivi du temps d'accès au fichier pendant l'exécution de la vérification de l'intégrité du système. La case est décochée par défaut.
Zones de contrôle	Le groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'analyse**.

Dans la section **Zones d'exclusion** des propriétés de la tâche Vérification de l'intégrité du système, vous pouvez configurer des zones d'exclusion de la surveillance et d'exclusions d'après le masque.

Fenêtre Zones d'analyse

Le tableau contient les zones de contrôle pour la tâche Vérification de l'intégrité du système. L'application contrôle les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient une zone de contrôle **Objets internes de Kaspersky** (/opt/kaspersky/kesl/).

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone	Nom de la Zones de contrôle.
Chemin	Chemin au répertoire que l'application protège.
État	L'état indique si l'application analyse cette zone lors du fonctionnement.

Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments dans le tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

Fenêtre Nouvelle zone d'analyse

Cette fenêtre permet d'ajouter ou de configurer des zones de surveillance pour la tâche Vérification de l'intégrité du système.

Paramètres Zones de contrôle

Paramètre	Description
Nom de la zone d'analyse	Champ de saisie du nom de la zone de contrôle. Ce nom sera affiché dans le tableau de la fenêtre **Zones d'analyse**. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case active ou désactive l'analyse de cette zone pendant le fonctionnement de l'application. Si la case est cochée, l'application contrôle cette zone de contrôle pendant le fonctionnement de l'application. Si cette case est décochée, l'application ne contrôle pas cette zone de contrôle pendant son fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. La case est cochée par défaut.

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone de contrôle. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide. Le chemin /opt/kaspersky/kesl est défini par défaut.
Masques	La liste contient des masques de noms d'objets, que l'application vérifie au moment de l'exécution. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques.

Section Zones d'exclusion

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion du contrôle.
Exclusions d'après le masque	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions d'après le masque**. Cette fenêtre permet de configurer l'exclusion des objets du contrôle sur la base d'un masque de nom.

Fenêtre Zones d'exclusion

Le tableau contient les zones d'exclusion de l'analyse pour la tâche Vérification de l'intégrité du système. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau est vide.

Paramètres de la zone d'exclusion de l'analyse de la tâche Vérification de l'intégrité du système

Paramètre	Description
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès au répertoire exclu de l'analyse.
État	L'état indique si l'application exclut cette zone de l'analyse lorsque la tâche est exécutée.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Nouvelle zone d'exclusion

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion du contrôle pour la tâche Vérification de l'intégrité du système.

Paramètres de la zone d'exclusion du contrôle

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre Zones d'exclusion. Le champ de saisie ne peut être vide.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion d'une zone de surveillance pendant le fonctionnement de l'application. Si cette case est cochée, l'application exclut cette zone du contrôle lorsque la tâche est exécutée. Si cette case est décochée, l'application ne contrôle pas cette zone lorsque la tâche est exécutée. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. La case est cochée par défaut.
Système de fichiers, protocole d'accès et chemin	Champ de saisie du chemin du répertoire local à inclure dans la zone d'exclusion. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ ne peut être vide. Le chemin d'accès **/** est spécifié par défaut. L'application exclut de l'analyse tous les répertoires du système de fichiers local.
Masques	La liste contient les masques des noms des objets exclus de la surveillance par l'application. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse. Exemples : Le masque `*.txt` fait référence à tous les fichiers texte. Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets du contrôle, en fonction d'un masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Vous pouvez ajouter, modifier et supprimer des masques.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de définir, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security va exclure de l'analyse.

Exemples :
Le masque `*.txt` fait référence à tous les fichiers texte.
Le masque `*_my_file_??.html` fait référence aux fichiers html commençant par n'importe quoi et se terminant par `_my_file_` et suivi de deux caractères quelconques (par exemple, 2020_my_file_09).

Vous pouvez également importer la liste des exclusions depuis un fichier à l'aide du bouton **Importer** et exporter la liste des exclusions dans un fichier JSON à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cochez la case **Fusionner les valeurs lors de l'héritage**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Configuration de la vérification de l'intégrité du système en ligne de commande

Vous pouvez exécuter une vérification de l'intégrité du système sur un appareil en ligne de commande à l'aide de tâches utilisateur *Vérification de l'intégrité du système* (tâches *ODFIM*).

Vous pouvez démarrer, arrêter, suspendre et reprendre les tâches d'utilisateur manuellement et configurer la planification de lancement de la tâche. Vous pouvez configurer les paramètres de vérification de l'intégrité du système en modifiant les paramètres de ces tâches.

Paramètres de la tâche Vérification de l'intégrité du système

Paramètre	Description	Valeurs
`RebuildBaseline`	Activer la mise à jour de l'instantané de l'état du système une fois la tâche *Vérification de l'intégrité du système* terminée.	`Yes` : mettre à jour l'instantané de l'état du système à chaque fois que la tâche *Vérification de l'intégrité du système* est terminée. `No` (par défaut) : ne pas mettre à jour l'instantané de l'état du système à chaque fois que la tâche *Vérification de l'intégrité du système* est terminée.
`CheckFileHash`	Utilisez le hachage du fichier (SHA256) comme critère selon lequel l'état actuel du fichier contrôlé est comparé à l'état d'origine.	`Yes` : vérifier le hachage. `No` (valeur par défaut) : désactive une analyse de hash. Si la vérification est désactivée, l'application compare uniquement la taille du fichier (si la taille du fichier n'a pas changé, l'heure du changement n'est pas considérée comme un paramètre critique).
`TrackDirectoryChanges`	Active la surveillance des répertoires.	`Yes` : surveiller les répertoires tout en effectuant une vérification de l'intégrité du système. `No` (valeur par défaut) : ne surveille pas les répertoires.
`TrackLastAccessTime`	Active la vérification de l'heure du dernier accès au fichier. Dans les systèmes d'exploitation Linux, c'est le paramètre `noatime`.	`Yes` : vérifie la dernière fois où le fichier a été consulté. `No` (valeur par défaut) : ne vérifie pas la dernière fois où le fichier a été consulté.
`UseExcludeMasks`	Active l'exclusion de la zone de contrôle des objets définis par le paramètre `ExcludeMasks.item_#`. Ce paramètre fonctionne uniquement si le paramètre `ExcludeMasks.item_#` a été défini.	`Yes` : exclut de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de la zone de contrôle les objets définis par le paramètre `ExcludeMasks.item_#`.
`ExcludeMasks.item_#`	Exclusion du contrôle des objets en fonction du nom ou du masque. Ce paramètre permet d'exclure de la zone d'analyse indiquée un fichier distinct en fonction de son nom ou plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez indiquer plusieurs masques. Chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.	La valeur par défaut n'est pas définie.
La section **[ScanScope.item_#]** définit les zones de surveillance que la tâche *Vérification de l'intégrité du système* doit surveiller. Il faut définir au moins une zone de contrôle pour la tâche. Vous pouvez définir plusieurs sections [ScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone de contrôle contient des informations complémentaires sur la zone de contrôle.	La valeur par défaut n'est pas définie.

Paramètre	Description	Valeurs
`UseScanArea`	Active l'analyse de la zone de contrôle.	`Yes` (valeur par défaut) : surveille la zone indiquée. `No` : ne surveille pas une zone indiquée.
`Path`	Chemin d'accès au répertoire à surveiller.	Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Valeur par défaut : /opt/kaspersky/kesl/
`AreaMask.item_#`	Restriction de la zone de contrôle. Dans la zone de contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (contrôler tous les objets).
La section **[ExcludedFromScanScope.item_#]** contient les objets à exclure de toutes les sections [ScanScope.item_#]. Vous pouvez définir plusieurs sections [ExcludedFromScanScope.item_#] dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément. La section [ExcludedFromScanScope.item_#] contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'exclusion du contrôle contient des informations complémentaires sur la zone d'exclusion du contrôle.	La valeur par défaut n'est pas définie.
`UseScanArea`	Exclusion de la zone de surveillance indiquée.	`Yes` (valeur par défaut) : exclut la zone indiquée de la surveillance. `No` : n'exclut pas la zone indiquée de la surveillance.

Paramètre	Description	Valeurs
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la surveillance.	Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. La valeur par défaut n'est pas définie.
`AreaMask.item_#`	Restriction de la zone d'exclusion du contrôle. Dans la zone d'exclusion du contrôle, l'application analyse uniquement les objets renseignés à l'aide de masques au format shell. Vous pouvez définir plusieurs éléments `AreaMask.item_#` dans n'importe quel ordre. L'application traite les zones par ordre croissant d'index d'élément.	Valeur par défaut : `*` (exclure tous les objets du contrôle).

Détection comportementale

Le module Détection comportementale permet de contrôler l'activité malveillante des applications dans le système d'exploitation. En cas de détection d'une activité malveillante, l'application Kaspersky Endpoint Security peut arrêter le processus de l'application qui exécute l'activité malveillante.

Le module Détection comportementale est activé automatiquement avec les paramètres par défaut lorsque vous lancez l'application Kaspersky Endpoint Security.

Pour optimiser les performances du module Détection comportementale, nous vous recommandons d'activer le module Protection contre les menaces Internet.

Vous pouvez activer et désactiver l'analyse des comportements, ainsi que configurer les paramètres de fonctionnement du module :

- Sélectionnez l'action que Kaspersky Endpoint Security effectuera lorsqu'une activité malveillante est détectée dans le système d'exploitation : informer l'utilisateur ou bloquer l'application effectuant une activité malveillante.
- Exclure l'activité du processus de l'analyse par le module Détection comportementale et les modules MDR et EDR Expert (on-premise).

  L'application exclut automatiquement le processus du serveur Watchdog de l'analyse. Il est impossible du supprimer cette exclusion.

Par défaut, sur le système d'exploitation SynthesisM-Client, la configuration du service auditd est bloquée contre les modifications, c'est-à-dire qu'elle est dans le mode de fonctionnement `enabled 2`. Pour que le module Détection comportementale fonctionne correctement lors de l'intégration de Kaspersky Endpoint Security avec les solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform, vous devez modifier le mode de fonctionnement auditd dans les fichiers de configuration en mode sans bloquer la configuration `enabled 1` et redémarrer le système d'exploitation.

Si un utilisateur disposant des privilèges root n'a pas accès à un fichier situé dans un répertoire distant monté sur l'appareil via le protocole NFSv4, l'application bloque l'accès à ce fichier pour tous les utilisateurs.

Configuration de la détection comportementale dans Web Console

Dans Web Console, vous pouvez gérer les paramètres de la Détection comportementale dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Détection comportementale**).

Configuration de la détection comportementale dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Détection comportementale dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection avancée** → **Détection comportementale**).

Paramètres du module Détection comportementale

Paramètre	Description
Activer la Détection comportementale	La case active ou désactive le module Détection comportementale. La case est cochée par défaut.
Action en cas de détection d'une activité malveillante	Action que Kaspersky Endpoint Security entreprendra lorsqu'elle détectera une activité malveillante dans le système d'exploitation : • **Bloquer** une application qui exécute une activité malveillante (par défaut). Kaspersky Endpoint Security termine le processus à l'origine de l'activité malveillante et enregistre dans le journal des événements les informations sur l'activité malveillante détectée. • **Informer** l'utilisateur. Kaspersky Endpoint Security ne termine pas le processus qui exécute une activité malveillante, consigne uniquement l'événement de détection d'une activité malveillante dans le journal des événements.
Utiliser les exclusions par processus	La case active ou désactive l'utilisation des exclusions par processus dans le fonctionnement du module Détection comportementale. La case est décochée par défaut. Cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Exclusions par processus**. Dans cette fenêtre, vous pouvez configurer l'exclusion de l'activité de processus de l'analyse.

Fenêtre Exclusions par processus

La fenêtre contient les zones d'exclusion en fonction des processus. La zone d'exclusion en fonction des processus vous permet de configurer l'exclusion de l'activité du processus spécifié de l'analyse.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
Nom de la zone d'exclusion	Nom de la zone d'exclusion.
Chemin	Chemin d'accès complet au processus exclu.
État	L'état indique si cette exclusion est appliquée par l'application.

Par défaut, la table des zones d'exclusion est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Vous pouvez également importer la liste des exclusions d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter la liste des exclusions ajoutées vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**.

Fenêtre Processus de confiance

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**.
Chemin d'accès au processus exclu	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Le champ de saisie ne peut être vide.
Appliquer aux processus enfants	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre **Chemin d'accès au processus exclu**. La case est décochée par défaut.
Utiliser cette zone	Cette case permet d'activer ou de désactiver l'exclusion de cette zone pour l'analyse pendant le fonctionnement de l'application. Si la case est cochée, l'application exclut cette zone pendant son fonctionnement. Si cette case est décochée, l'application inclut cette zone pendant son fonctionnement. Par la suite, vous pouvez exclure cette zone après avoir coché la case. La case est cochée par défaut.
Exclure un processus de l'analyse par le module Détection comportementale	La case active ou désactive l'exclusion d'un processus de la vérification lorsque le module Détection comportementale est en cours d'exécution. La case est décochée par défaut.
Exclure un processus de la télémétrie MDR et EDR Expert (on-premises)	La case à cocher active ou désactive l'exclusion d'un processus de la télémétrie collectée par les modules MDR et EDR Expert (on-premises). La case est décochée par défaut.

Configuration de la Détection comportementale sur la ligne de commande

Depuis la ligne de commande, vous pouvez gérer l'analyse du comportement des applications dans le système d'exploitation à l'aide de la tâche prédéfinie d'analyse du comportement (*Behavior_Detection*).

La tâche Détection comportementale est exécutée par défaut. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres de la détection comportementale en modifiant les paramètres de la tâche prédéfinie Détection comportementale.

Paramètre	Description	Valeurs
`UseTrustedPrograms`	Exclusion de processus de l'analyse.	`Yes` : exclut l'activité des processus spécifiés de l'analyse. `No` (valeur par défaut) : analyse tous les processus.
`TaskMode`	Action exécutée par l'application suite à la détection d'une activité malveillante dans le système d'exploitation.	`Block` (valeur par défaut) : termine le processus de l'application qui exécute une activité malveillante. `Notify` : ne met pas fin au processus qui exécute une activité malveillante, consigne uniquement la détection d'une activité malveillante dans le journal des événements.
La section **[TrustedPrograms.item_#]** contient les processus exclus de l'analyse par le module Détection comportementale. Kaspersky Endpoint Security ne contrôle pas l'activité des processus renseignés.		
`ProgramPath`	Chemin d'accès au processus exclu.	`< chemin d'accès complet au processus >` – Exclut de l'analyse le processus dans le répertoire local spécifié. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.
`ApplyToDescendants`	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre `ProgramPath`.	`Yes` : exclut le processus spécifié et tous ses processus enfants de l'analyse. `No` (valeur par défaut) : exclut uniquement le processus spécifié de l'analyse, n'exclut pas les processus enfants de l'analyse.
`ProgramDesc`	Description du processus exclu.	
`UseTrustedProgram`	Utilisation de l'exclusion de l'activité du processus spécifié de l'analyse.	`Yes` (valeur par défaut) : utiliser une exclusion de l'analyse d'activité pour le processus spécifié. `No` : ne pas utiliser l'exclusion de l'activité du processus spécifié de l'analyse.
`UseTrustedProgramForDetects`	Exclusion de l'analyse de l'activité du processus lors de l'exécution du module Détection comportementale.	`Yes` : exclure de l'analyse l'activité du processus spécifié lors de l'exécution du module Détection comportementale. `No` (valeur par défaut) : ne pas exclure de l'analyse l'activité du processus spécifié lorsque le module Détection comportementale est en cours d'exécution.
`UseTrustedProgramForMDRAndEDR`	Exclusion de l'activité de processus de la télémétrie collectée par les modules MDR et EDR Expert (on-premises).	`Yes` : exclure l'activité du processus spécifié de la télémétrie collectée par les modules MDR et EDR Expert (on-premises). `No` (valeur par défaut) : ne pas exclure l'activité du processus spécifié de la télémétrie.

Paramètre	Description	Valeurs
`TelemetrySource`	Paramètres avancés de collecte de télémétrie envoyés aux solutions Detection and Response lors de l'intégration avec ces solutions. Le paramètre `UseTelemetryMonopolyMode` est appliqué uniquement si le paramètre `TelemetrySource` est défini sur `Default`.	`Default` (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie. `OnlyEBPF` : utiliser uniquement la technologie eBPF pour la collecte de télémétrie.
`UseTelemetryMonopolyMode`		`True` (valeur par défaut) : Kaspersky Endpoint Security utilise le service auditd en mode exclusif. `False` signifie que le service auditd est utilisé en mode multidiffusion.

Protection contre les Exploits

Le module Protection contre les Exploits surveille le code logiciel qui exploite les vulnérabilités de votre appareil pour obtenir des privilèges administrateur ou effectuer des actions malveillantes. Les exploits, par exemple, utilisent l'attaque par débordement de tampon. Dans ce cas, l'exploit envoie un gros volume de données à l'application vulnérable. Lors du traitement de ces données, l'application vulnérable exécute un code malveillant. Suite à cette attaque, un exploit pourrait lancer l'installation non autorisée d'une application malveillante. Si une tentative d'exécution d'un fichier exécutable à partir d'une application vulnérable n'a pas été effectuée par l'utilisateur, l'application Kaspersky Endpoint Security bloque le lancement de ce fichier ou informe l'utilisateur. Par défaut, la Protection contre les Exploits est désactivée.

Pour que le module Protection contre les Exploits fonctionne, vous devez activer le module Détection comportementale et l'utilisation du module de noyau mis à jour. Pour optimiser les performances du module Protection contre les Exploits, nous vous recommandons également d'activer le module Protection contre les menaces Internet.

Vous pouvez activer ou désactiver la Protection contre les Exploits, ainsi que configurer les paramètres de fonctionnement du module :

- Sélectionner l'action que l'application devra exécuter en cas de détection d'un Exploit.
- Configurez les exclusions d'objets de l'analyse. Une exclusion de l'analyse est un ensemble de conditions. Lorsque ces conditions sont remplies, l'application n'analyse pas les objets à la recherche de virus et autres logiciels malveillants. Vous pouvez exclure de l'analyse :
  - objets par les noms des menaces détectées dans les objets ;
  - fichiers et répertoires situés aux chemins indiqués ;
  - fichiers avec la somme de hachage spécifiée.

Configuration de la protection contre les Exploits dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de la Protection contre les Exploits dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection contre les menaces de l'hôte** → **Analyse comportementale** → **Protection contre les Exploits**).

Configuration de la protection contre les exploits dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de la Protection contre les Exploits dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection avancée** → **Détection comportementale**).

Paramètres du module Protection contre les Exploits

Paramètre	Description
Activer la Protection contre les Exploits	Le case active ou désactive le module Protection contre les Exploits. La case est décochée par défaut.
Groupe **Protection contre les Exploits**	Le bouton **Configurer** ouvre la fenêtre **Exclusions de la Protection contre les Exploits**, où vous pouvez configurer les exclusions d'analyse pour le module Protection contre les Exploits.
Action en cas de détection d'un Exploit	Action que l'application devra exécuter en cas de détection d'un Exploit : • **Bloquer** (valeur par défaut). L'application bloque les actions malveillantes de l'exploit et enregistre des informations à ce sujet dans le journal des événements. • **Informer**. L'application ne bloque pas les actions d'exploit, mais enregistre uniquement les informations sur la détection d'exploit dans le journal des événements.

Fenêtre Exclusions de la Protection contre les Exploits

Dans cette fenêtre, vous pouvez configurer les objets à exclure de l'analyse de la Protection contre les Exploits. L'application n'analysera pas les objets spécifiés. Par défaut, la liste des objets est vide.

Paramètres de l'exclusion de la Protection contre les Exploits

Paramètre	Description
Fusionner les valeurs lors de l'héritage	La case active ou désactive la fusion de la liste des lors de l'héritage dans les stratégies enfants. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.
État	L'état indique si cette exclusion est appliquée par l'application.
Nom de la menace	Nom de la menace exclue de l'analyse.
Chemin d'accès au fichier ou au répertoire	Chemin d'accès complet au fichier ou répertoire exclu de l'analyse.
Somme de hachage du fichier	Somme de hachage du fichier exclu de l'analyse.
Commentaire	Commentaire relatif à l'exclusion d'analyse.

Par défaut, la tableau des exclusions est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Fenêtre Exclusion de la Protection contre les Exploits

Dans cette fenêtre, vous pouvez ajouter ou configurer une exclusion d'analyse par le module Protection contre les Exploits.

Paramètres de l'exclusion de la Protection contre les Exploits

Paramètre	Description
Utiliser le nom de la menace	La case active ou désactive l'utilisation d'une exclusion d'analyse d'un objet en fonction du nom de la menace détectée dans l'objet. La case est cochée par défaut.
Nom de la menace	Champ permettant de saisir le nom de la menace détectée dans l'objet. Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet. Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/. Ce champ est disponible si la case **Utiliser le nom de la menace** est cochée.

Paramètre	Description
Utiliser la somme de hachage du fichier	Cette case active ou désactive l'utilisation des exclusions d'analyse de fichiers en fonction de leur valeur de hachage. La case est cochée par défaut.
Type de hachage de fichier	utilisez la liste déroulante pour sélectionner le type de hachage de fichier à utiliser pour exclure le fichier de l'analyse. • **MD5**. • **SHA256**. Cette liste déroulante est disponible si la case **Utiliser la somme de hachage du fichier** est cochée.
Somme de hachage du fichier	Ce champ vous permet de saisir la somme de hachage du fichier à utiliser pour exclure le fichier de l'analyse. Ce champ est disponible si la case **Utiliser la somme de hachage du fichier** est cochée.
Utiliser le chemin d'accès au fichier ou au répertoire	Cette case active ou désactive l'utilisation des exclusions d'analyse de fichiers en fonction du chemin d'accès au fichier dans lequel une menace a été détectée. La case est cochée par défaut.
Chemin d'accès au fichier ou au répertoire	Ce champ permet de saisir le chemin d'accès à un fichier ou un répertoire à exclure de l'analyse. Vous pouvez utiliser des symboles * et ? pour spécifier le chemin. Il est disponible si la case **Utiliser le chemin d'accès au fichier ou au répertoire** est cochée.
Commentaire	Champ de saisie pour un commentaire (facultatif).
Utiliser cette exclusion	La case à cocher active ou désactive l'utilisation de cette exclusion pendant l'exécution de l'application. La case est cochée par défaut.

Configuration de la protection contre les Exploits dans la ligne de commande

Dans la ligne de commande, vous pouvez contrôler la protection contre les Exploits à l'aide des paramètres de la tâche prédéfinie Détection comportementale (*Behavior_Detection*).

Vous pouvez configurer les paramètres de la protection contre les Exploits, en modifiant les paramètres de la tâche prédéfinie Détection comportementale (cf. tableau ci-dessous).

Paramètres de protection contre les exploits

Paramètre	Description	Valeurs
`UseAEP`	Activation du module Protection contre les Exploits.	`Yes` active la Protection contre les Exploits. `No` (valeur par défaut) : désactiver la Protection contre les Exploits.
`AEPMode`	L'action exécutée par l'application lorsqu'elle détecte un Exploit.	`Block` (valeur par défaut) : bloquer les actions malveillantes de l'Exploit et enregistre les informations à ce sujet dans le journal des événements. `Notify` : ne pas bloquer les actions d'exploit, mais enregistrer uniquement les informations sur la détection d'exploit dans le journal des événements.
La section **[AEPExclusions.item_#]** contient les exclusions d'analyse effectuées par le module Protection contre les Exploits.		
`Enabled`	Activation d'utilisation d'une exclusion d'analyse par le module Protection contre les Exploits.	`Yes` (valeur par défaut) – utiliser l'exclusion de la Protection contre les Exploits. `No` : ne pas utiliser l'exclusion d'analyse par Protection contre les Exploits.
`DetectName`	Exclusion d'un objet de l'analyse en fonction du nom de la menace détectée dans cet objet. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseDetectName` est activé.	Pour exclure un objet de l'analyse, indiquez le nom complet de la menace détectée dans cet objet, la chaîne de l'application contenant le verdict d'infection de l'objet. Vous pouvez trouver le nom complet de la menace détectée dans l'objet dans le journal de l'application ou sur le site https://threats.kaspersky.com/fr/.

Paramètre	Description	Valeurs
`Hash`	Exclusion d'analyse du fichier dans lequel une menace a été détectée, en fonction de son hachage. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UseHash` est activé.	
`HashType`	Type de somme de hachage du fichier à exclure de l'analyse à l'aide du paramètre `Hash`.	`Md5` : type de somme de hachage MD5. `Sha256` : type de somme de hachage SHA256.
`Path`	Exclusion d'analyse d'un fichier dans lequel une menace a été détectée, ainsi que le long du chemin d'accès à ce fichier. Avant d'indiquer les valeurs de ce paramètre, assurez-vous que le paramètre `UsePath` est activé.	`< chemin d'accès complet au fichier ou au répertoire local >` – exclure le fichier ou les objets du répertoire spécifié (y compris les sous-répertoires) des analyses. Vous pouvez utiliser des symboles `*` et `?` pour spécifier le chemin.
`UseDetectName`	Active l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `DetectName`.	`Yes` (valeur par défaut) : exclure de l'analyse les objets contenant les menaces désignées par le paramètre `DetectName`. `No` : ne pas exclure de l'analyse les objets contenant les menaces définies par le paramètre `DetectName`.
`UseHash`	Activation de l'exclusion d'analyse du fichier dans lequel une menace a été détectée, en fonction de sa somme de hachage. La somme de hachage du fichier est spécifié à l'aide du paramètre `Hash`.	`Yes` (valeur par défaut) : exclure de l'analyse le fichier contenant la menace détectée, en fonction de sa valeur de la somme de hachage. `No` : ne pas exclure de l'analyse le fichier contenant la menace détectée, en fonction de sa valeur de la somme de hachage.
`UsePath`	Activation de l'exclusion d'analyse du fichier contenant la menace détectée, en fonction de son chemin d'accès. Le chemin d'accès est spécifié à l'aide du paramètre `Path`.	`Yes` (valeur par défaut) : exclure de l'analyse le fichier dans lequel la menace a été détectée sur le chemin d'accès. `No` : ne pas exclure de l'analyse le fichier dans lequel la menace a été détectée sur le chemin d'accès.

Utilisation de Kaspersky Security Network

La fonctionnalité KSN peut ne pas être disponible dans le logiciel aux États-Unis.

Pour augmenter l'efficacité de la protection des appareils et des données utilisateur, l'application Kaspersky Endpoint Security peut utiliser la base de connaissances basée sur le cloud de Kaspersky sur la réputation des fichiers, des ressources Internet et des logiciels : Kaspersky Security Network (KSN). L'exploitation des données de Kaspersky Security Network garantit une réaction plus rapide face aux diverses menaces, des performances élevées des modules de protection et une réduction des risques de faux positifs.

L'utilisation de Kaspersky Security Network est volontaire. Vous pouvez commencer à participer au KSN ou vous retirer à tout moment.

Solutions d'infrastructure Kaspersky Security Network

Kaspersky Endpoint Security prend en charge les solutions d'infrastructure suivantes pour les bases de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est une solution qui vous permet de recevoir des informations de Kaspersky et d'envoyer des données à Kaspersky sur les objets détectés sur les appareils des utilisateurs en vue de permettre aux experts de Kaspersky une analyse complémentaire et d'enrichir les bases de réputation et de statistiques.

- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'appareils sur lesquels Kaspersky Endpoint Security est installée d'accéder aux bases de données de réputation de Kaspersky et à d'autres données statistiques sans envoyer de données à Kaspersky à partir de leurs appareils. KPSN a été mis au point pour les entreprises qui ne peuvent pas utiliser Kaspersky Security Network pour les raisons suivantes :

  - absence de connexion des postes de travail locaux à Internet ;

  - interdiction légale ou restriction de la sécurité de l'entreprise d'envoyer des données en dehors du pays ou du réseau local de l'entreprise.

Après avoir activé une application sous une nouvelle licence, vous devez fournir à votre fournisseur de services les nouvelles informations de clé de licence pour utiliser KPSN. Dans le cas contraire, il sera impossible d'échanger des informations avec KPSN en raison d'une erreur d'authentification.

Options d'utilisation de Kaspersky Security Network

Il existe deux options pour utiliser KSN :

- **Mode étendu de KSN** : vous pouvez recevoir des informations de la base de connaissances de Kaspersky, et Kaspersky Endpoint Security envoie automatiquement des informations statistiques de son fonctionnement à Kaspersky Security Network. L'application peut également envoyer à Kaspersky pour analyse complémentaire des fichiers (ou des parties de fichiers) que des individus malintentionnés pourraient utiliser pour nuire à l'appareil et aux données.

- **Mode KSN de base** : vous pouvez récupérer des informations de la base de connaissances de Kaspersky, et Kaspersky Endpoint Security n'envoie pas de statistiques anonymes ou de données sur les types et les sources de menaces.

Vous pouvez choisir d'utiliser Kaspersky Security Network à l'aide Web Console, de la Console d'administration ou de la ligne de commande.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour en savoir plus sur la soumission des statistiques obtenues pendant la participation à KSN, sur le stockage et la destruction de ces informations, consultez la Déclaration de Kaspersky Security Network et le site de Kaspersky. Le fichier qui reprend la Déclaration de Kaspersky Security Network figure dans le kit de distribution de l'application.

Mode de fonctionnement cloud de Kaspersky Endpoint Security

Le *mode Cloud* est le mode de fonctionnement de l'application Kaspersky Endpoint Security, qui utilise une version allégée des bases de données des logiciels malveillants. Cela permet de réduire la charge sur la mémoire de l'appareil.

Kaspersky Security Network facilite l'utilisation des bases de données anti-malware légères par l'application.

Si l'application Kaspersky Endpoint Security est utilisée en mode standard et que vous utilisez KSN dans l'application, vous pouvez activer le mode cloud de l'application.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation de bases de données légères de logiciels malveillants n'est pas prise en charge. L'application reçoit du Serveur de protection les bases de données spéciales nécessaires au fonctionnement du Light Agent.

Kaspersky Endpoint Security passe à l'utilisation d'une version allégée des bases de données des logiciels malveillants après avoir activé le mode cloud et effectué la prochaine mise à jour des bases de données et des modules de l'application. Si le mode cloud est désactivé, Kaspersky Endpoint Security télécharge la version complète des bases de données de l'application depuis les serveurs de Kaspersky lors de la prochaine mise à jour des bases de données et des modules de l'application.

Si vous n'utilisez pas KSN ou si le mode cloud est désactivé, Kaspersky Endpoint Security utilise la version complète des bases de données de l'application.

Le mode Cloud est automatiquement désactivé si l'utilisation de KSN est désactivée.

Utilisation du service proxy KSN

Les appareils des utilisateurs exécutés sous le contrôle du Serveur d'administration peuvent interagir avec KSN directement ou à l'aide du service du serveur proxy KSN sur le Serveur d'administration.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'interaction avec l'infrastructure KSN est assurée par le service du serveur proxy KSN. La communication directe avec KSN n'est pas prise en charge. Si le proxy KSN n'est pas disponible, KSN n'est pas utilisé dans le fonctionnement de l'application.

Le serveur proxy KSN offre les fonctionnalités suivantes :

- l'appareil peut interroger KSN et transmettre des informations à KSN, même en l'absence d'accès direct à Internet.
- Le serveur proxy KSN met en cache les données traitées, ce qui réduit la charge sur la connexion réseau externe et accélère la réception des informations sollicitées sur l'appareil de l'utilisateur.

Vous pouvez configurer les paramètres du serveur proxy KSN dans les propriétés du Serveur d'administration. Pour en savoir plus sur le serveur proxy KSN, consultez l'aide de Kaspersky Security Center.

Si l'application Kaspersky Endpoint Security est utilisée en mode standard, vous pouvez configurer les paramètres d'utilisation du serveur proxy KSN dans l'application à l'aide de Web Console ou de la Console d'administration de Kaspersky Security Center.

La configuration des paramètres du serveur proxy KSN à l'aide de la ligne de commande n'est pas disponible.

Dans Kaspersky Security Center, vous pouvez configurer les paramètres suivants pour l'utilisation du serveur proxy KSN par l'application Kaspersky Endpoint Security :

- activer et désactiver l'utilisation du Serveur d'administration comme serveur proxy KSN ;
- Autoriser ou refuser l'interaction avec les serveurs KSN directement si le service proxy KSN n'est pas disponible.

Configuration de l'utilisation de Kaspersky Security Network dans Web Console

Dans la Web Console, vous pouvez configurer l'utilisation de Kaspersky Security Network par l'application dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Kaspersky Security Network**).

Les informations sur la disponibilité du KSN sont affichées dans Kaspersky Security Center en utilisant l'état de l'appareil client (*OK, Critique, Avertissement*) dans la liste des appareils administrés sous l'onglet **Actifs (Appareils)**.

Configuration de l'utilisation de Kaspersky Security Network dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer l'utilisation de Kaspersky Security Network par Kaspersky Endpoint Security dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Protection avancée** → **Kaspersky Security Network**).

Le contenu de la Déclaration de Kaspersky Security Network est disponible dans la fenêtre **Déclaration de Kaspersky Security Network** qui s'ouvre via le lien **Déclaration de Kaspersky Security Network**.

Les informations sur la disponibilité du KSN sont affichées dans Kaspersky Security Center en utilisant l'état de l'appareil client (*OK, Critique, Avertissement*) dans la liste des appareils administrés sous l'onglet **Appareils**.

Paramètres de Kaspersky Security Network

Paramètre	Description
Déclaration de Kaspersky Security Network	Cliquez sur ce lien pour ouvrir la fenêtre **Déclaration de Kaspersky Security Network**. Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Security Network.
Kaspersky Security Network (KSN)	Le groupe affiche des informations sur le mode d'utilisation de KSN ou sur le fait que KSN n'est pas utilisé dans le fonctionnement de Kaspersky Endpoint Security. En cliquant sur le bouton **Modifier**, une fenêtre s'ouvre dans laquelle vous pouvez configurer l'utilisation de Kaspersky Security Network.
Activer le mode cloud	La case active ou désactive le mode de fonctionnement dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données des logiciels malveillants. La case est disponible si KSN est activé. La case est cochée si, lors de la création de la stratégie, vous avez accepté les termes de la Déclaration de Kaspersky Security Network et utilisé le mode avancé de KSN. Le mode est activé ou désactivé après la prochaine mise à jour de la base de données de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Utiliser le Serveur d'administration comme serveur proxy KSN	Si la case est sélectionnée, l'application Kaspersky Endpoint Security interagit avec les serveurs KSN à l'aide du service du serveur proxy KSN sur le Serveur d'administration. La case est cochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. En mode Light Agent pour la protection des environnements virtuels, l'application ne peut interagir avec l'infrastructure KSN à l'aide du serveur proxy KSN uniquement.
Utiliser les serveurs KSN si le proxy KSN n'est pas disponible	Si la case est sélectionnée, l'application Kaspersky Endpoint Security communique directement avec les serveurs KSN lorsque le service proxy KSN n'est pas disponible. La case est cochée par défaut. La case est disponible si la case **Utiliser le Serveur d'administration comme serveur proxy KSN** est sélectionnée. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.

Paramètres de Kaspersky Security Network

Cette fenêtre permet de configurer les paramètres de participation à Kaspersky Security Network.

Paramètres de Kaspersky Security Network

Paramètre	Description
En savoir plus	Cliquez sur ce lien pour accéder au site Internet de Kaspersky.
Ne pas utiliser Kaspersky Security Network	En sélectionnant cette option, vous refusez d'utiliser Kaspersky Security Network.
Mode KSN de base	En sélectionnant cette option, vous acceptez les conditions d'utilisation de Kaspersky Security Network. Vous pourrez recevoir des informations de la base de connaissances en ligne de Kaspersky sur la réputation des fichiers, des ressources Web et des logiciels.
Mode étendu de KSN	En sélectionnant cette option, vous acceptez les conditions d'utilisation de Kaspersky Security Network. Vous pourrez recevoir des informations de la base de connaissances en ligne de Kaspersky sur la réputation des fichiers, des ressources Web et des logiciels. En outre, des statistiques et informations anonymes sur les types et sources de différentes menaces seront envoyées pour améliorer Kaspersky Security Network dans Kaspersky.
Déclaration de Kaspersky Security Network	Le lien ouvre la fenêtre **Déclaration de Kaspersky Security Network** dans laquelle vous pouvez lire le texte de la Déclaration de Kaspersky Security Network.

Déclaration de Kaspersky Security Network

Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Security Network et d'en accepter les dispositions.

Paramètres de Kaspersky Security Network

Paramètre	Description
Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network	En sélectionnant cette option, vous confirmez que vous souhaitez utiliser Kaspersky Security Network et que vous avez entièrement lu, compris et accepté les dispositions de la déclaration de Kaspersky Security Network affichée. L'option est disponible si vous avez sélectionné l'option **Mode KSN de base** ou **Mode étendu de KSN** dans la fenêtre **Paramètres de Kaspersky Security Network**.
Je n'accepte pas les conditions de la Déclaration de Kaspersky Security Network	En choisissant cette option, vous confirmez que vous ne souhaitez pas utiliser Kaspersky Security Network L'option est disponible si vous avez sélectionné l'option **Mode KSN de base** ou **Mode étendu de KSN** dans la fenêtre **Paramètres de Kaspersky Security Network**.

Déclaration de Kaspersky Private Security Network

Cette fenêtre permet de lire le texte de la Déclaration de Kaspersky Private Security Network et d'en accepter les dispositions.

Paramètre	Description
Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network	En sélectionnant cette option, vous confirmez que vous souhaitez participer au Kaspersky Security Network et que vous avez entièrement lu, compris et accepté les dispositions de la déclaration de Kaspersky Private Security Network affichée.
Je n'accepte pas les conditions de la Déclaration de Kaspersky Security Network	En choisissant cette option, vous confirmez que vous ne souhaitez pas utiliser Kaspersky Security Network

Configuration de l'utilisation de Kaspersky Security Network sur la ligne de commande

Depuis la ligne de commande, vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide de l'option `UseKSN` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre `UseKSN` à l'aide des clés de la ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Pour activer l'utilisation de Kaspersky Security Network à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

où :

- `<Extended/Basic>` : mode Kaspersky Security Network.
- `--accept-ksn` : option signifiant que vous acceptez les conditions de la Déclaration de Kaspersky Security Network. Vous confirmez avoir entièrement lu, compris et accepté les termes de la Déclaration de Kaspersky Security Network.

Le fichier ksn_license.<ID de la langue> contenant le texte de la Déclaration de Kaspersky Security Network se trouve dans le répertoire /opt/kaspersky/kesl/doc/.

Pour désactiver l'utilisation de Kaspersky Security Network à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseKSN=No
```

Pour activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide du fichier de configuration, exécutez la commande suivante :

```
kesl-control --set-app-settings --file <chemin d'accès au fichier de configuration> [--
json] [--accept-ksn]
```

où :

- `--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration contenant les paramètres généraux de l'application, dans lequel est configurée la valeur requise du paramètre `UseKSN`.
- `--json` : spécifiez cette clé si vous importez des paramètres à partir d'un fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.
- `--accept-ksn` : option signifiant que vous acceptez les conditions de la Déclaration de Kaspersky Security Network. La clé est requise si vous activez l'utilisation de Kaspersky Security Network.

Si Kaspersky Endpoint Security, installé sur un appareil client, fonctionne sous une stratégie de Kaspersky Security Center, la valeur du paramètre `UseKSN` peut être modifiée uniquement à l'aide de Kaspersky Security Center. Quand l'application Kaspersky Endpoint Security, installée sur un appareil client, n'est plus soumis à la stratégie, la valeur du paramètre devient `UseKSN=No`.

Vérification de la connexion à Kaspersky Security Network à l'aide de la ligne de commande

Pour vérifier la connexion à Kaspersky Security Network, exécutez la commande suivante :

```
kesl-control --app-info
```

La ligne **Utilisation de Kaspersky Security Network** affiche l'état de la connexion à Kaspersky Security Network :

- Si l'état `Mode étendu de KSN` est affiché, l'application Kaspersky Endpoint Security utilise Kaspersky Security Network, des informations peuvent être obtenues dans la base de connaissances, les statistiques anonymes et les informations sur les types et les sources des nouvelles menaces sont envoyées.
- Si l'état `Mode KSN de base` est affiché, l'application Kaspersky Endpoint Security utilise Kaspersky Security Network, des informations peuvent être obtenues dans la base de connaissances, mais les statistiques anonymes et les informations sur les types et les sources des nouvelles menaces ne sont pas envoyées.
- Si l'état `Désactivé` est affiché, l'application Kaspersky Endpoint Security n'utilise pas Kaspersky Security Network.

La ligne **Infrastructure de Kaspersky Security Network** affiche des informations sur la solution d'infrastructure utilisée pour travailler avec les bases de réputation de Kaspersky : `Kaspersky Security Network` ou `Kaspersky Private Security Network`.

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- l'appareil de l'utilisateur n'est pas connecté à Internet.
- L'utilisation du Kaspersky Security Network est désactivée.
- L'application n'est pas activée ou la licence a expiré.
- Des problèmes liés à la clé de licence ont été détectés. Par exemple, la clé figure dans la liste des clés interdites.

Activer ou désactiver le mode cloud à l'aide de la ligne de commande

Le *mode Cloud* est le mode de fonctionnement de l'application Kaspersky Endpoint Security, qui utilise une version allégée des bases de données des logiciels malveillants.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation de bases de données légères de logiciels malveillants n'est pas prise en charge. L'application reçoit du Serveur de protection les bases de données spéciales nécessaires au fonctionnement du Light Agent.

À partir de la ligne de commande, vous pouvez activer et désactiver le mode cloud à l'aide du paramètre `CloudMode=Yes/No` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre `CloudMode` à l'aide du fichier de configuration, qui contient tous les paramètres généraux de l'application, ou à l'aide des clés de la ligne de commande.

Le mode cloud de l'application est disponible si l'utilisation de Kaspersky Security Network est activée.

Paramètres supplémentaires de fonctionnement de l'application

Vous pouvez configurer les paramètres supplémentaires suivants de l'application :

- Serveur proxy pour l'application.
- Exclusions globales : exclusion des points de montage de l'interception des opérations sur les fichiers pour les modules Protection contre les fichiers malicieux, Protection contre le chiffrement, Surveillance du conteneur et des tâches Analyse des logiciels malveillants, Analyse des zones critiques, Analyse du conteneur et Analyse des disques amovibles.
- Exclusion de la mémoire d'un processus de l'analyse
- Mode d'interception des opérations sur les fichiers.
- Détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.
- Surveillance de la stabilité de l'application.
- Paramètres de démarrage de l'application.
- Limite d'utilisation de la mémoire et du processeur pour les tâches d'analyse.
- Limite d'utilisation de la mémoire résidente par une application.
- Limite du nombre des tâches d'analyse personnalisées qu'un utilisateur non privilégié peut exécuter simultanément.
- Paramètres d'envoi d'informations vers le stockage de Kaspersky Security Center.
- Autorisations pour gérer les tâches.
- Annulation de l'exécution des tâches planifiées sur un appareil fonctionnant sur batterie.
- Paramètres d'interception des événements système.
- Paramètres avancés de la télémétrie.

Configuration du serveur proxy

Vous pouvez configurer les paramètres du serveur proxy si les utilisateurs des appareils clients accèdent à Internet via un serveur proxy. L'application Kaspersky Endpoint Security peut utiliser un serveur proxy pour se connecter aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites à l'aide du module Protection contre les menaces Internet.

Par défaut, l'utilisation d'un serveur proxy est désactivée.

Si vous activez des appareils situés dans un segment isolé du réseau sans accès à Internet à l'aide d'un code d'activation, vous pouvez utiliser le Serveur d'administration de Kaspersky Security Center comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky. Vous pouvez activer l'utilisation du Serveur d'administration comme serveur proxy pour accéder aux serveurs d'activation dans Web Console ou dans la Console d'administration.

Vous pouvez configurer les exceptions suivantes lors de l'utilisation d'un serveur proxy dans Web Console, dans la Console d'administration ou dans la ligne de commande :

- Ceci s'applique aux modules EDR Expert (on-premise), NDR (KATA) et Sandbox, qui assurent l'intégration avec les solutions Detection and Response. Vous pouvez spécifier les modules qui n'utiliseront pas de serveur proxy.
- Pour les adresses Internet. Vous pouvez créer une liste d'adresses auxquelles un serveur proxy ne sera pas utilisé pour la connexion.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'utilisation d'un serveur proxy pour la connexion à Kaspersky Security Network, à la SVM et au Serveur d'intégration n'est pas prise en charge. L'utilisation du Serveur d'administration de Kaspersky Security Center comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky n'est pas non plus prise en charge.

Configuration des paramètres du serveur proxy dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'utilisation d'un serveur proxy dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres du réseau**).

Configuration des paramètres du serveur proxy dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres du proxy dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres du serveur proxy**).

Paramètres du serveur proxy

Paramètre	Description
Ne pas utiliser de serveur proxy	Si cette option est sélectionnée, le serveur proxy n'est pas utilisé dans le fonctionnement de l'application.
Utiliser les paramètres indiqués du serveur proxy	Si cette option est sélectionnée, l'application utilise les paramètres de serveur proxy spécifiés pour se connecter aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites avec le module Protection contre les menaces Internet.
Adresse et port	Champs de saisie de l'adresse IP ou du nom de domaine et du port du serveur proxy. Port par défaut : 3128. Les champs sont accessibles si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée.

Paramètre	Description
Utiliser l'authentification sur le serveur proxy	Cette case active ou désactive l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe pour l'accès au serveur proxy. La case est accessible si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée. La case est décochée par défaut. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.
Nom d'utilisateur	Champ de saisie du nom d'utilisateur pour son authentification sur le serveur proxy. Le champ de saisie est disponible si la case **Utiliser l'authentification sur le serveur proxy** est cochée.
Mot de passe	Champ de saisie du mot de passe de l'utilisateur pour l'authentification sur le serveur proxy. Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois. Cliquez sur le bouton **Afficher** pour afficher le mot de passe de l'utilisateur en clair dans le champ **Mot de passe**. Par défaut, le mot de passe de l'utilisateur est masqué et s'affiche sous forme de points. Le champ de saisie et le bouton sont accessibles si la case **Utiliser l'authentification sur le serveur proxy** est cochée.
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation	Active ou désactive l'utilisation du Serveur d'administration de Kaspersky Security Center comme serveur proxy pour accéder aux serveurs d'activation de Kaspersky. Cela est nécessaire lors de l'activation de l'application dans un segment isolé du réseau sans accès à Internet à l'aide d'un code d'activation. Si la case est sélectionnée, l'application accède aux serveurs d'activation via le Serveur d'administration avec accès à Internet. La case est décochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard. Si l'application est utilisée en mode Light Agent pour protéger les environnements virtuels, le serveur de protection fournit des informations de licence.
Exclusions pour le serveur proxy	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Exclusions pour le serveur proxy**.

Fenêtre Exclusions pour le serveur proxy

Dans cette fenêtre, vous pouvez configurer l'utilisation d'un serveur proxy lors de l'intégration avec les modules de la solution Kaspersky Anti Targeted Attack Platform, ainsi qu'une liste d'adresses pour se connecter auxquelles aucun serveur proxy ne sera utilisé.

Exclusions pour le serveur proxy

Paramètre	Description
Ne pas utiliser le serveur proxy lors de l'exécution des modules	Cochez les cases en regard des modules d'application pour lesquels vous ne souhaitez pas utiliser le serveur proxy : • **Endpoint Detection and Response Expert (on-premises)** : ne pas utiliser de serveur proxy lors de la connexion à des serveurs qui fournissent une intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA). • **Sandbox** : ne pas utiliser de serveur proxy pour vous connecter aux serveurs qui offrent une intégration avec Sandbox. • **Network Detection and Response (KATA)** : ne pas utiliser de serveur proxy lors de la connexion à des serveurs qui offrent une intégration avec Kaspersky Network Detection and Response (KATA).

Paramètre	Description
Ne pas utiliser de serveur proxy pour les adresses	Le tableau contient une liste d'adresses pour lesquelles le serveur proxy ne sera pas utilisé pour se connecter : • **Adresse IP/nom DNS** : adresse IP ou nom DNS pour se connecter auquel aucun serveur proxy ne sera utilisé. Pour spécifier l'adresse, vous pouvez utiliser des masques (symboles `*` et `?`). • **Commentaire** : champ de saisie pour un commentaire (facultatif). Vous pouvez **ajouter**, **modifier** et **supprimer** des adresses dans le tableau. Cliquez le bouton **Supprimer** pour exclure la zone sélectionnée de l'analyse. Le bouton est accessible si au moins une zone d'analyse est sélectionnée dans le tableau. La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre qui permet de définir les paramètres d'un nouvel élément.

Configuration des paramètres du serveur proxy via la ligne de commande

Dans la ligne de commande, vous pouvez configurer la manière dont les modules de l'application utilisent un serveur proxy à l'aide des paramètres `UseProxy`, `ProxyServer`, `ProxyBypass`, `ProxyBypassEdr`, `ProxyBypassNdr` et `ProxyBypassSandbox` des paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseProxy` peut prendre les valeurs suivantes :

- `Yes` : active l'utilisation d'un serveur proxy.
- `No` : désactive l'utilisation d'un serveur proxy.

Le paramètre `ProxyServer` permet de spécifier les paramètres du serveur proxy au format suivant : `< protocole de connexion >://[< utilisateur >[:< mot de passe >]@]< adresse du serveur proxy<code class="programcharacter">a>:<</code>numéro de port >`, où :

- `< utilisateur >` est le nom d'utilisateur utilisé pour l'authentification sur le serveur proxy.
- `< mot de passe >` est le mot de passe utilisateur utilisé pour l'authentification sur le serveur proxy.
- `< adresse du serveur proxy >` est l'adresse IP ou le nom de domaine du serveur proxy.
- `< numéro de port >` est le numéro de port du serveur proxy.

La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.

Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.

Le paramètre `ProxyBypass` vous permet de spécifier une liste d'adresses auxquelles un serveur proxy ne sera pas utilisé pour se connecter. L'adresse est indiquée au format `< adresse >[:< numéro de port >]`. Pour spécifier des adresses, vous pouvez utiliser des masques (symboles `*`) et des commentaires (après le symbole \).

Les paramètres suivants vous permettent de configurer l'utilisation d'un serveur proxy dans le fonctionnement des modules EDR Expert (on-premises), NDR (KATA) et Sandbox, qui assurent l'intégration avec les solutions Detection and Response :

- le paramètre `ProxyBypassEdr` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion à des serveurs qui assurent l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec Kaspersky Endpoint Detection and Response (KATA) ;
- le paramètre `ProxyBypassNdr` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion à des serveurs qui assurent l'intégration avec Kaspersky Network Detection and Response (KATA) ;
- le paramètre `ProxyBypassSandbox` vous permet d'activer ou de désactiver l'utilisation d'un serveur proxy lors de la connexion aux serveurs qui fournissent une interaction avec Sandbox.

Les paramètres peuvent prendre les valeurs suivantes :

- `Yes` : active l'utilisation d'un serveur proxy.
- `No` : désactive l'utilisation d'un serveur proxy.

Configuration des exclusions globales

Vous pouvez configurer l'exclusion des points de montage de l'interception des opérations sur les fichiers pour les modules Protection contre les fichiers malicieux et Protection contre le chiffrement, ainsi que de l'analyse à l'aide des tâches Analyse des logiciels malveillants, Analyse des zones critiques et Analyse du conteneur. L'exclusion des points de montage vous permet d'exclure les répertoires locaux ou distants montés sur l'appareil de l'interception des opérations sur les fichiers. De plus, les exclusions globales affectent le fonctionnement du module Surveillance des conteneurs (Analyse du conteneur, Surveillance des conteneurs) et de la tâche Analyse des disques amovibles.

Configuration des exclusions globales dans Web Console

Dans Web Console, vous pouvez configurer des exclusions globales dans les propriétés de la stratégie (**Paramètres de l'application** → **Zone de confiance** → **Points de montage fiables**).

Configuration des exclusions globales dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les exclusions globales dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Exclusions globales**).

Le groupe de paramètres **Points de montage exclus** contient un bouton **Configurer**. Ce bouton permet d'ouvrir la fenêtre **Points de montage exclus**.

La liste dans la fenêtre contient les chemins vers les points de montage exclus. Par défaut, la liste est vide. Vous pouvez ajouter, modifier et supprimer des éléments dans la liste.

Fenêtre Chemin du point de montage

Paramètres de point de montage

Paramètre	Description
Système de fichiers, protocole d'accès et chemin	Le groupe de paramètres vous permet de spécifier l'emplacement du point de montage. La liste déroulante des systèmes de fichiers permet de sélectionner le type du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'analyse : • **Local** : points de montage locaux. • **Monté** : répertoires distants montés sur l'appareil via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur l'appareil via les protocoles Samba et NFS.
	Si le type **Monté** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez sélectionner le protocole d'accès à distance dans la liste déroulante de droite : • **NFS** : répertoires distants montés sur l'appareil via le protocole NFS. • **Samba** : répertoires distants montés sur l'appareil via le protocole Samba. • **Personnalisé** : tous les ressources de système de fichiers de l'appareil indiqué dans le champ ci-après.
	Si le type **Local** est sélectionné dans la liste déroulante des systèmes de fichiers, vous pouvez spécifier dans le champ de saisie le chemin d'accès au point de montage que vous souhaitez ajouter aux exclusions de l'interception des opérations de fichier. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.
Nom du système de fichiers	Champ de saisie du nom du système de fichiers dans lequel se trouve les répertoires que vous souhaitez ajouter aux exclusions de l'interception des opérations de fichier. Le champ est disponible si vous avez choisi l'option **Monté** dans la liste déroulante des systèmes de fichiers et l'option **Personnalisé** dans la liste déroulante de droite.

Configuration des exclusions globales sur la ligne de commande

À partir de la ligne de commande, vous pouvez configurer les exclusions de points de montage à l'aide du paramètre `ExcludedMountPoint.item_#` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `ExcludedMountPoint.item_#` peut prendre les valeurs suivantes :

- `AllRemoteMounted` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'appareil via les protocoles SMB et NFS.
- `Mounted:NFS` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole NFS.
- `Mounted:SMB` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole SMB.
- `Mounted:<type de système de fichiers>` — Exclut de l'interception des opérations sur les fichiers tous les répertoires montés avec le type de système de fichiers indiqué.
- `/mnt` — exclut les objets du point de montage /mnt (y compris les sous-répertoires) de l'interception des opérations sur les fichiers. Ce répertoire est utilisé comme point de montage temporaire pour les disques amovibles.
- `<chemin qui contient le masque /mnt/user* ou /mnt/**/user_share>` — Exclut de l'interception des opérations sur les fichiers les objets des points de montage dont le nom contient le **masque** indiqué.

  Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

  Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

  Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

  Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

  Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques).

  Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même.

  Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.

Vous pouvez spécifier plusieurs points de montage que vous souhaitez exclure de l'analyse.

Exclure la mémoire de processus de l'analyse

Vous pouvez configurer des exclusions d'analyse pour la mémoire des processus. L'application n'analysera pas la mémoire des processus spécifiés.

Configuration des exclusions dans Web Console

Dans Web Console, vous pouvez configurer l'exclusion de la mémoire des processus des analyses dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Performances**).

Configuration des exclusions dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les exclusions de la mémoire des processus dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux → Exclure la mémoire des processus**).

Cliquer sur le bouton **Configurer** dans le groupe **Exclure la mémoire de processus de l'analyse** ouvre une fenêtre dans laquelle vous pouvez créer une liste d'exclusions.

La liste de la fenêtre **Exclure la mémoire de processus de l'analyse** contient les chemins d'accès aux processus que l'application exclut de l'analyse de la mémoire de processus. Vous pouvez utiliser des **masques** pour spécifier le chemin. Par défaut, la liste est vide.

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques).

Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Vous pouvez activer la fusion de la liste des exclusions pendant l'héritage dans les stratégies enfants. Pour fusionner des éléments de liste, vous devez cocher la case **Fusionner les valeurs lors de l'héritage** dans la fenêtre **Exclure la mémoire du processus de l'analyse**. Si la case est cochée, les éléments de la liste des stratégies parents sont affichés dans les stratégies enfants et des éléments peuvent être ajoutés à la liste des stratégies enfants. Si la case est décochée, les éléments de la liste ne sont pas fusionnés lorsque les paramètres de stratégie sont hérités. La case est décochée par défaut.

Configuration des exclusions dans la ligne de commande

Dans la ligne de commande, vous pouvez configurer l'exclusion de la mémoire de processus de l'analyse à l'aide du paramètre `MemScanExcludedProgramPath.item_#` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `MemScanExcludedProgramPath.item_#` contient le chemin complet du processus dans le répertoire local. Vous pouvez utiliser des **masques** pour spécifier le chemin.

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`.

Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect.

Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Vous pouvez spécifier plusieurs processus dont vous souhaitez exclure la mémoire de l'analyse.

Sélection du mode d'interception pour les opérations sur les fichiers

Le mode d'interception des opérations sur les fichiers affecte le fonctionnement des modules Protection contre les fichiers malicieux et Contrôle des appareils.

- Une application peut bloquer l'accès aux fichiers analysés par le module Protection contre les fichiers malicieux pendant l'analyse. Par défaut, l'accès est bloqué : tout accès au fichier en cours d'analyse attend les résultats de l'analyse. Si l'analyse ne détecte aucune menace dans le fichier, l'application autorise l'accès au fichier. Lorsque des objets infectés sont détectés, l'application exécute les actions spécifiées dans le paramètre **Action lors de la détection d'une menace** (`ActionOnThreat`) du module Protection contre les fichiers malicieux.

  Vous pouvez désactiver le blocage de l'accès aux fichiers analysés par le module Protection contre les fichiers malicieux. Dans ce cas, l'analyse est effectuée de manière asynchrone.

- Une application peut bloquer l'accès aux fichiers sur un appareil tandis que le Contrôle des appareils détermine si l'accès à l'appareil peut être accordé. Par défaut, l'accès est bloqué : tout accès aux fichiers sur l'appareil contrôlé attend les résultats de l'analyse. L'application autorise l'accès aux fichiers si suite à une analyse, le Contrôle des appareils autorise l'accès à l'appareil contenant les fichiers.

  Vous pouvez désactiver le blocage de l'accès aux fichiers sur un appareil contrôlé par le module Contrôle des appareils. Dans ce cas, le Contrôle des appareils détermine s'il est possible de fournir un accès à l'appareil en mode asynchrone.

Si le mode de blocage pour l'interception des opérations sur les fichiers n'est pas activé, les modules Protection contre les fichiers malicieux et Contrôle des appareils, ainsi que Prévention de l'exécution des objets fonctionnent en mode de notification, quel que soit le mode de fonctionnement configuré.

Configuration dans Web Console

Dans Web Console, vous pouvez configurer le mode d'interception des opérations sur les fichiers dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de détection**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de traçage de l'application dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application** → section **Mode d'interception des opérations sur les fichiers**).

La case **Bloquer l'accès aux fichiers pendant l'analyse** active ou désactive le blocage de l'accès aux fichiers pendant l'analyse par les modules Protection contre les fichiers malicieux et Contrôle des appareils.

La case est cochée par défaut.

Si la case est décochée, l'accès à n'importe quel fichier est autorisé pendant la durée de l'analyse, et l'analyse s'exécute en mode asynchrone.

Configuration sur la ligne de commande

Sur la ligne de commande, vous pouvez configurer la manière dont les opérations sur les fichiers sont interceptées à l'aide du paramètre `FileBlockDuringScan` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `FileBlockDuringScan` peut prendre les valeurs suivantes :

- `Yes` (valeur par défaut) : bloquer l'accès aux fichiers pendant l'analyse par les modules Protection contre les fichiers malicieux et Contrôle des appareils.
- `No` : ne pas bloquer l'accès aux fichiers lors de l'analyse. L'accès à n'importe quel fichier est autorisé, la vérification est effectuée en mode asynchrone.

  Ce mode d'interception des opérations sur les fichiers a moins d'impact sur les performances du système pendant le fonctionnement, mais il existe un risque qu'une menace dans un fichier ne soit pas désinfectée ou supprimée si, lors de l'analyse, ce fichier peut, par exemple, changer de nom avant que l'application ne prenne une décision sur l'état de ce dossier.

Configuration de la détection des applications que les intrus peuvent utiliser pour causer des dommages

Vous pouvez activer ou désactiver la détection des applications légitimes qui pourraient être utilisées par des intrus pour endommager des appareils ou des données. Ces applications ne possèdent pas de fonctionnalités malveillantes en elles-mêmes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données des utilisateurs, consultez le site internet de l'Encyclopédie des virus de Kaspersky.

Configuration dans Web Console

Dans Web Console, vous pouvez gérer les paramètres de détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de détection**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, section **Paramètres d'analyse**).

La case **Détecter les applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données** active ou désactive la détection des applications légitimes par lesquelles les intrus peuvent endommager l'appareil ou les données de l'utilisateur.

La case est décochée par défaut.

Configuration sur la ligne de commande

Via la ligne de commande, vous pouvez activer ou désactiver la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données à l'aide du paramètre `DetectOtherObjects` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `DetectOtherObjects` peut prendre les valeurs suivantes :

- `Yes` : activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.
- `No` : ne pas activer pas la détection des applications légitimes qui pourraient être utilisées par des intrus pour endommager les appareils ou les données.

Activer la surveillance de la stabilité des applications

Vous pouvez activer ou désactiver la surveillance de la stabilité de l'application Kaspersky Endpoint Security, qui vous permet de suivre le nombre d'arrêts anormaux de l'application et d'informer l'administrateur du fonctionnement instable de l'application, ainsi que de configurer les paramètres de surveillance.

Configuration dans Web Console

Dans la Web Console, vous pouvez activer ou désactiver la surveillance de la stabilité de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → Paramètres généraux → **Performances**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver la surveillance de la stabilité de l'application dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, **Paramètres avancés de l'application**).

La case **Activer la surveillance de la stabilité de l'application** active ou désactive la surveillance de l'état de fonctionnement de l'application Kaspersky Endpoint Security.

La case est décochée par défaut.

Pour appliquer ce paramètre, vous devez redémarrer l'application et l'Agent d'administration

Si l'application est instable, le message suivant s'affiche dans les propriétés de l'appareil avec l'application installée : *<Number> arrêts anormaux de l'application depuis<date and time>*.

Configuration sur la ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de surveillance de la stabilité de l'application Kaspersky Endpoint Security à l'aide des paramètres `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` et `WarnRemovingThreshold` dans le fichier de configuration kesl.ini.

Le paramètre `TrackProductCrashes` vous permet d'activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center lorsque l'application est instable. Le paramètre peut prendre les valeurs suivantes :

- `Yes/true` : activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.
- `No/false` : désactiver l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.

Le paramètre `ProductHealthLogFile` vous permet de spécifier le chemin d'accès au fichier utilisé pour surveiller la stabilité de l'application. Valeur par défaut : /var/opt/kaspersky/kesl/private/kesl_health.log.

Le paramètre `WarnThreshold` permet de préciser l'intervalle de temps (en secondes) pendant lequel l'application doit compter le nombre d'arrêts anormaux avant d'afficher un avertissement d'instabilité. Valeur par défaut : 3600 secondes.

Le paramètre `WarnRemovingThreshold` permet de définir l'intervalle de temps (en secondes) après lequel l'état instable de l'application sera supprimé. Valeur par défaut : 86400 secondes.

Le paramètre `WarnAfter_#_crash` permet de définir le nombre d'arrêts anormaux de l'application, une fois atteint, une notification concernant le fonctionnement instable de l'application s'affiche. Le paramètre peut prendre des valeurs de 0 à 10. Valeur par défaut : 10. Si la valeur est 0, la notification d'instabilité de l'application ne s'affiche pas.

Configuration des paramètres de lancement de l'application

Vous pouvez personnaliser les options de lancement de l'application.

Configuration d'une limite dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de lancement de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Interaction avec l'utilisateur**).

Configuration d'une limite dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de lancement de l'application dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, **Paramètres de lancement de l'application**).

Dans le groupe **Paramètres de démarrage de l'application**, cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Paramètres de démarrage de l'application**, dans laquelle vous pouvez configurer les paramètres de lancement de l'application (cf. le tableau ci-dessous).

Paramètres de démarrage de l'application

Paramètre	Description
Nombre maximum de tentatives consécutives infructueuses pour démarrer une application	Champ de saisie du nombre maximum de tentatives consécutives infructueuses de lancement de l'application. Valeur par défaut : 5.
Durée maximale d'attente pour le démarrage de l'application (min)	Champ de saisie du temps maximum d'attente pour le démarrage de l'application (en minutes), après quoi le processus kesl sera redémarré. Valeur par défaut : 3.

Configuration d'une limite dans la ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de démarrage de l'application à l'aide des paramètres `MaxRestartCount` et `StartupTimeout` dans le fichier de configuration kesl.ini.

Le paramètre `MaxRestartCount` permet de définir le nombre maximum de tentatives consécutives infructueuses de démarrage d'une application. Le paramètre peut prendre des valeurs de 1 à 10. Valeur par défaut : 5.

Le paramètre `StartupTimeout` permet de définir le temps maximum d'attente avant le démarrage de l'application (en minutes), après quoi le processus kesl sera redémarré. Le paramètre peut prendre des valeurs de 1 à 60. Valeur par défaut : 3.

Limite d'utilisation de la mémoire résidente par une application

Vous pouvez configurer la limite d'utilisation de la mémoire résidente pour l'application. Le réglage par défaut est automatique.

Configuration d'une limite dans Web Console

Dans la Web Console, vous pouvez gérer la limite d'utilisation de la mémoire résidente dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Performances**).

Configuration d'une limite dans la Console d'administration

Dans la Console d'administration, vous pouvez définir une limite d'utilisation de la mémoire résidente dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux → Paramètres de l'application**).

Dans le groupe **Paramètres d'application avancés**, cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Paramètres avancés**, dans laquelle vous pouvez configurer la limite d'utilisation de la mémoire résidente (cf. le tableau ci-dessous).

Pour appliquer les modifications, redémarrez l'application Kaspersky Endpoint Security sur l'appareil administré après l'application de la stratégie.

Paramètres

Paramètre	Description
Utilisation de la mémoire par l'application	Dans la liste déroulante, vous pouvez sélectionner comment limiter l'utilisation de la mémoire résidente : • **Pas limitée**. Si cette option est sélectionnée, l'utilisation de la mémoire résidente n'est pas limitée. • **Limitée automatiquement (recommandé)**. Lorsque vous sélectionnez cet élément de la liste, l'utilisation de la mémoire résidente est automatiquement limitée (par défaut). • **Limitée à un pourcentage du volume total**. Lorsque vous sélectionnez cet élément de la liste, le champ **Limite d'utilisation de la mémoire (%)** devient disponible, dans lequel vous pouvez spécifier la valeur de pourcentage souhaitée. • **Limitée à une valeur en mégaoctets**. Lorsque vous sélectionnez cet élément de la liste, le champ **Limite d'utilisation de la mémoire (Mo)** devient disponible, dans lequel vous pouvez spécifier la valeur souhaitée en mégaoctets. • **Limité à la plus petite des valeurs spécifiées (%, Mo)**. Lorsque vous sélectionnez cet élément de la liste, les champs **Limite d'utilisation de la mémoire (%)** et **Limite d'utilisation de la mémoire (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs souhaitées. • **Limité à la plus grande des valeurs spécifiées (%, Mo)**. Lorsque vous sélectionnez cet élément de la liste, les champs **Limite d'utilisation de la mémoire (%)** et **Limite d'utilisation de la mémoire (Mo)** deviennent disponibles, dans lesquels vous pouvez spécifier les valeurs souhaitées.
Limite d'utilisation de la mémoire (%)	Champ de saisie pour limiter l'utilisation de la mémoire (en pourcentage). Valeur par défaut : 50.
Limite d'utilisation de la mémoire (Mo)	Champ de saisie des limites d'utilisation de la mémoire (en mégaoctets). Valeur par défaut : 2000.

Configuration d'une limite dans la ligne de commande

Sur la ligne de commande, vous pouvez configurer la limite d'utilisation de la mémoire résidente à l'aide du paramètre `MaxMemory` dans le fichier de configuration kesl.ini.

Le paramètre `MaxMemory` peut prendre les valeurs suivantes :

- `off` : l'utilisation de la mémoire résidente n'est pas limitée.
- < `valeur` >% – valeur comprise entre 1 et 100 % de la mémoire RAM.
- < `valeur` >`MB` – valeur en mégaoctets.
- `lowest`/< `valeur` >%/< `valeur` >`MB` – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets.

- `highest/< valeur >%/< valeur >MB` – la plus grande des deux : la valeur en pourcentage et la valeur absolue en mégaoctets.
- `auto` : jusqu'à 50 % de la mémoire disponible, mais pas moins de 2 Go et pas plus de 16 Go.

Valeur par défaut : `auto`.

Limite d'utilisation de la mémoire et du processeur

Vous pouvez configurer la limite d'utilisation de la mémoire pour les tâches d'analyse. La limite par défaut est de 8 192 mégaoctets.

> Il est recommandé de spécifier une limite d'utilisation de la mémoire pour les tâches d'analyse inférieure à la limite d'utilisation de la mémoire résidente afin d'éviter d'utiliser toute la mémoire disponible pour les tâches d'analyse et de redémarrer l'application.

Vous pouvez configurer des limites d'utilisation des ressources du processeur pour les tâches d'analyse. Par défaut, il n'y a pas de limite. Lors de la configuration de la limite, il est recommandé de noter que la ressource totale de tous les cœurs de processeur est considérée comme étant de 100 %. L'utilitaire `top` affiche la charge du processeur, en supposant que la ressource d'un cœur est de 100 %. Ainsi, une valeur de 400 % pour un processeur à 10 cœurs (soit un total de 1 000 % mesuré par l'utilitaire `top`) signifie que l'ensemble du processeur (tous les cœurs au total) est utilisé à 40 %. Si vous souhaitez que la valeur indiquée par l'utilitaire `top` reste inférieure à 150 % sur ce même processeur à 10 cœurs, vous devez spécifier `15` comme limite d'utilisation du processeur. La limite doit être un entier compris entre 10 et 100. De plus, la limite d'utilisation du processeur n'est pas appliquée à toutes les tâches de l'application, mais uniquement aux tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse des conteneurs*. Par conséquent, l'utilisation du processeur lorsqu'elle est limitée peut être supérieure à celle souhaitée.

Configuration d'une limite dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de limitation de l'utilisation du processeur et de la mémoire pour les tâches d'analyse dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Performances**).

Configuration d'une limite dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver la limite d'utilisation du processeur et configurer une limite de RAM pour les tâches d'analyse dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, section **Performances**).

En cliquant sur le bouton **Configurer** dans le groupe **Performances**, la fenêtre **Paramètres des performances des tâches d'analyse** s'ouvre, dans laquelle se trouve la section **Consommation du processeur et de la mémoire** où vous pouvez configurer des limites (voir tableau ci-dessous).

Paramètre	Description
Limiter la consommation de ressources du processeur pour les tâches d'analyse (%)	La case active ou désactive la limite d'utilisation des ressources CPU pour les tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse du conteneur*. Si la case est cochée, la charge maximale de tous les cœurs du processeur pour ces tâches est maintenue en dessous du pourcentage indiqué dans le champ situé à droite (la charge totale maximale de tous les cœurs du processeur est considérée comme égale à 100 %). La valeur dans le champ doit être un entier et être comprise entre 10 et 100. La case est décochée par défaut.
Limite d'utilisation de la mémoire pour les tâches d'analyse (Mo)	Champ de saisie permettant de limiter l'utilisation de la mémoire pour les tâches d'analyse (en mégaoctets). Valeur par défaut : 8192.

Configuration d'une limite dans la ligne de commande

Sur la ligne de commande, vous pouvez configurer des limites d'utilisation du processeur pour les tâches *ODS*, *ContainerScan* et *InventoryScan* à l'aide des paramètres `UseOnDemandCPULimit` et `OnDemandCPULimit` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseOnDemandCPULimit` peut prendre les valeurs suivantes :

- `Yes` :activer la limitation de la consommation des ressources du processeur pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan*.
- `No` : désactiver la limite de la consommation des ressources du processeur pour les tâches.

Le paramètre `OnDemandCPULimit` permet de spécifier la valeur maximale de la charge sur tous les noyaux de processeur (en pourcentage) lors de l'exécution des tâches de type *ODS*, *ContainerScan* et *InventoryScan*. La valeur du paramètre doit être un entier et être comprise entre 10 et 100. Valeur par défaut : 100.

Sur la ligne de commande, vous pouvez configurer des limites d'utilisation de la mémoire pour les tâches *ODS*, *ContainerScan* et *InventoryScan* à l'aide du paramètre `ScanMemoryLimit` dans le fichier de configuration kesl.ini. Valeur par défaut : 8192.

Limite du nombre de tâches d'analyse personnalisée

Vous pouvez configurer la limite sur le nombre de tâches d'analyse personnalisée qu'un utilisateur non privilégié peut exécuter simultanément sur un appareil. Il n'y a pas de limite au nombre de tâches qu'un utilisateur root peut exécuter.

Configuration d'une limite dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer, dans les propriétés de la stratégie, la limite du nombre de tâches d'analyse personnalisée simultanées qu'un utilisateur non privilégié peut exécuter sur l'appareil (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, section **Performances**).

En cliquant sur le bouton **Configurer** dans le groupe **Performances** , la fenêtre **Paramètres des performances des tâches d'analyse** s'ouvre. Dans cette fenêtre dans le groupe **Nombre de tâches d'analyse** du champ de saisie **Nombre maximum de tâches d'analyse personnalisée**, vous pouvez spécifier une valeur comprise entre 0 et 100 000. Valeur par défaut : 0. Si la valeur 0 est attribuée, l'utilisateur non privilégié ne peut pas exécuter de tâches d'analyse personnalisée.

Configuration d'une limite dans la ligne de commande

À partir de la ligne de commande, vous pouvez configurer la limite du nombre de tâches d'analyse personnalisée exécutées simultanément à l'aide du paramètre `LimitNumberOfScanFileTasks` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `LimitNumberOfScanFileTasks` peut prendre des valeurs comprises entre 0 et 100000. Si la valeur 0 est attribuée, l'utilisateur non privilégié ne peut pas exécuter de tâches d'analyse personnalisée. Valeur par défaut : 5.

Configuration de l'envoi des informations vers le stockage de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez activer ou désactiver l'envoi d'informations sur les fichiers de la sauvegarde, les fichiers en quarantaine, les fichiers non traités et les appareils connectés au stockage de Kaspersky Security Center.

Une liste générale des fichiers mis en quarantaine par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans Web Console (**Opérations → Stockages → Quarantaine**) et dans la Console d'administration (**Avancés → Stockages → Quarantaine**).

Une liste générale des fichiers placés dans la sauvegarde par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans Web Console (**Opérations → Stockages → Sauvegarde**) et dans la Console d'administration (**Avancés → Stockages → Sauvegarde**).

Les informations sur les fichiers non traités sont affichées dans la liste des menaces actives dans Web Console (**Opérations → Stockages → Menaces actives**) et dans la Console d'administration (**Avancés → Stockages → Menaces actives**).

Les informations sur les appareils installés ou connectés à l'appareil client sont affichées dans la liste des équipements dans Web Console (**Opérations → Stockages → Équipement**) et dans la Console d'administration (**Avancés → Stockages → Équipement**). Les informations sont transmises si le module Contrôle des appareils est activé.

Les informations sur les applications détectées sur l'appareil client s'affichent dans la liste des applications dans Web Console (**Opérations → Applications tierces → Registre des applications**) et dans la Console d'administration (**Avancés → Gestion des applications → Registre des applications**). Les informations sont transmises si le module Contrôle des applications est activé.

Activation ou désactivation de l'envoi d'informations à Web Console

Dans la Web Console, vous pouvez gérer les paramètres d'intégration avec le Serveur d'administration dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Intégration KSC**, section **Transfert des données au Serveur d'administration**, lien **Paramètres avancés**) et dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Paramètres de stockage**, section **Paramètres de transfert de données vers le Serveur d'administration**).

Les paramètres de transfert des données vers le Serveur d'administration dans les propriétés de la stratégie de Web Console sont décrits dans l'Annexe 5.

Les paramètres de transfert des données vers le Serveur d'administration dans les propriétés de l'appareil administré sont décrits dans le tableau ci-dessous.

Paramètres de transfert des données vers le Serveur d'administration dans les propriétés de l'appareil

Paramètre	Description
Notifier sur les fichiers de la sauvegarde	La case à cocher active ou désactive le transfert des informations sur les fichiers de la sauvegarde vers le Serveur d'administration. La case est décochée par défaut.
Notifier sur les fichiers de quarantaine	La case à cocher active ou désactive le transfert des informations sur les fichiers mis en quarantaine vers le Serveur d'administration. La case est décochée par défaut.
Notifier sur les fichiers non traités	La case active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration. La case est décochée par défaut.
Notifier sur les appareils installés	La case active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci. La case est décochée par défaut.
Notifier sur les applications détectées sur l'appareil	La case active ou désactive la transmission au Serveur d'administration de la liste des applications détectées sur l'appareil client à la suite de la tâche d'inventaire. La case est décochée par défaut.

Activation et désactivation du transfert de données dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver le transfert de données vers le Serveur d'administration dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de stockage**, **Transfert de données vers le Serveur d'administration**) ou dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres de stockage**, section **Transfert de données vers le Serveur d'administration**).

En cliquant sur le bouton **Configurer** dans le groupe **Transfert de données vers le Serveur d'administration** , la fenêtre **Paramètres de transfert des données** s'ouvre, dans laquelle vous pouvez activer ou désactiver l'envoi d'informations au Serveur d'administration.

Paramètre	Description
À propos des fichiers de quarantaine.	La case à cocher active ou désactive le transfert des informations sur les fichiers mis en quarantaine vers le Serveur d'administration. La case est cochée par défaut.
À propos des fichiers de la sauvegarde.	La case à cocher active ou désactive le transfert des informations sur les fichiers de la sauvegarde vers le Serveur d'administration. La case est cochée par défaut.
À propos des fichiers non traités	La case active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration. La case est cochée par défaut.
À propos des appareils installés	La case active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci. La case est cochée par défaut.
À propos des applications détectées sur l'appareil	La case active ou désactive la transmission au Serveur d'administration de la liste des applications détectées sur l'appareil client à la suite de la tâche d'inventaire. La case est cochée par défaut.

Configuration des autorisations de gestion des tâches

Dans Kaspersky Security Center, vous pouvez configurer les autorisations suivantes pour les utilisateurs :

- autorisation d'utiliser les tâches locales créées dans l'application Kaspersky Endpoint Security. Si la stratégie de Kaspersky Security Center interdit aux utilisateurs d'afficher et de modifier les tâches locales, les informations sur les tâches Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (en mode standard) et Rollback (en mode standard) ne sont pas disponibles.

- autorisation d'afficher et de gérer les tâches créées dans Kaspersky Security Center sur les appareils clients.

Configuration dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres des autorisations d'affichage et de gestion des tâches dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Interaction avec l'utilisateur**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les autorisations d'affichage et de gestion des tâches dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Tâches locales** → **Gestion de la tâche**).

Paramètre	Description
Autoriser l'utilisation des tâches locales	La case permet d'autoriser ou non l'utilisateur à consulter les tâches locales créées dans l'application Kaspersky Endpoint Security et à les gérer sur les appareils clients administrés. Si cette case est cochée, les utilisateurs peuvent configurer et exécuter des tâches dans l'interface graphique de l'application et dans la ligne de commande. Si la case est décochée, l'utilisation des tâches locales est arrêtée. Les tâches locales ne s'exécutent pas selon le calendrier prévu. Les tâches ne sont pas disponibles pour le lancement et la configuration dans l'interface graphique de l'application ou dans la ligne de commande. La case est décochée par défaut.
Autoriser à consulter et à administrer les tâches créées via KSC	La case permet ou non aux utilisateurs de visualiser les tâches créées via Kaspersky Security Center et d'administrer ces tâches sur les appareils clients. Si la case est cochée, les tâches créées via Kaspersky Security Center s'affichent dans l'interface graphique de l'application. Les utilisateurs peuvent démarrer et arrêter ces tâches à partir de l'interface graphique de l'application et dans la ligne de commande. Si la case est décochée, l'affichage et la gestion des tâches créées via Kaspersky Security Center ne sont pas disponibles dans l'interface graphique de l'application ni dans la ligne de commande. La case est décochée par défaut.

Arrêter le lancement des tâches lors de l'utilisation de la batterie

Vous pouvez activer ou désactiver la possibilité d'annuler les tâches planifiées en les faisant fonctionner sur batterie. La suppression des tâches planifiées peut réduire la consommation de ressources et prolonger la durée de vie de la batterie.

Si l'annulation des tâches planifiées est activée et que l'appareil fonctionne sur batterie, l'application Kaspersky Endpoint Security annule le lancement planifié des tâches suivantes :

- toutes les tâches d'analyse (analyse personnalisée, analyse des conteneurs, analyse personnalisée des conteneurs, analyse des zones critiques, analyse des logiciels malveillants) ;
- Inventaire
- mise à jour des bases et des modules de l'application ;
- analyse IOC ;
- Vérification de l'intégrité du système

Vous pouvez exécuter les tâches requises manuellement.

Configuration dans Web Console

Dans la Web Console, vous pouvez configurer l'annulation des tâches planifiées dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Performance**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer l'annulation des tâches planifiées dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**, **Performances**).

La case **Ignorer les tâches planifiées lors de l'utilisation de la batterie** active ou désactive la possibilité d'ignorer l'exécution des tâches planifiées.

La case est cochée par défaut.

Si la case est décochée, toutes les tâches planifiées sont exécutées sur l'appareil, quelle que soit la source d'alimentation à laquelle l'appareil est connecté (réseau ou batterie).

Configuration sur la ligne de commande

Dans la ligne de commande, vous pouvez configurer l'annulation des tâches planifiées dans les à l'aide du paramètre `PowerSaveMode` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `PowerSaveMode` peut prendre les valeurs suivantes :

- `Yes` (valeur par défaut) : ignorer l'exécution des tâches planifiées lorsque l'appareil fonctionne sur batterie.
- `No` : exécuter les tâches selon un calendrier, quelle que soit la source d'alimentation à laquelle l'appareil est connecté (réseau ou batterie).

Configuration des paramètres d'interception des événements système

Pour fonctionner correctement, l'application doit utiliser l'interception des événements système – opérations sur les fichiers et lancements de processus. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Si le système d'exploitation de votre appareil prend en charge la technologie fanotify, vous pouvez choisir le mécanisme que l'application doit utiliser pour intercepter les événements système :

- Mécanisme d'interception du système basé sur la technologie fanotify. Ce mécanisme est utilisé par défaut.
- Mécanisme d'interception basé sur un *module de noyau mis à jour*. L'utilisation d'un module de noyau mis à jour vous permet d'optimiser l'interception des opération de fichiers et des lancements de processus par l'application Kaspersky Endpoint Security. Le module de noyau mis à jour intercepte les opérations sur les fichiers lors de l'ouverture, du renommage et de la modification des fichiers. Les performances de l'application sont améliorées grâce à l'utilisation d'un cache de fichiers et de processus ne nécessitant pas de vérification.

Lors de l'utilisation d'un module de noyau mis à jour, vous pouvez configurer plus précisément les exclusions globales. Si le mécanisme d'interception basé sur fanotify est utilisé, les points de montage spécifiés sont entièrement exclus de l'interception des opérations sur les fichiers. Le module de noyau mis à jour vous permet d'exclure des répertoires locaux ou distants spécifiques montés sur l'appareil.

Le module de noyau mis à jour est inclus avec l'application.

Pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, le choix du mécanisme d'interception n'est pas disponible. L'application utilise un module de noyau spécial pour intercepter les événements système afin de se protéger contre les fichiers malicieux. Ce module est automatiquement compilé au lancement de la Protection contre les fichiers malicieux, à condition que les paquets de compilation et les utilitaires nécessaires soient disponibles.

Une application peut utiliser le mécanisme d'interception basé sur le module de noyau mis à jour si le système d'exploitation répond aux exigences d'installation du module de noyau mis à jour.

Exigences d'installation du module de noyau mis à jour

Pour installer et utiliser le module de noyau mis à jour, l'appareil doit disposer de l'un des systèmes d'exploitation 64 bits suivants :

- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)

  Si Kaspersky Endpoint Security est utilisé en mode standard, le module de noyau mis à jour peut être utilisé sur les appareils exécutant des systèmes d'exploitation Astra Linux en mode environnement logiciel fermé.

- CentOS 7.x.
- CentOS Stream 8
- Debian GNU/Linux 12.0
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 8.10
- SberLinux 8.10
- SberLinux 9.1
- SberLinux 9.6
- SberLinux 9.7
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS

- ALT SP Workstation version 10
- ALT SP Server version 10
- ALT Education 10
- ALT Workstation version 11.
- ALT Server version 11
- ALT Education 11
- RED OS 7.3
- RED OS 8
- ROSA « Cobalt » 7.9 Workstation
- ROSA « Cobalt » 7.9 Server
- ROSA « Chrome » 12 Workstation.
- ROSA « Chrome » 12 Server

Les systèmes d'exploitation 32 bits et les systèmes d'exploitation à architecture Arm ne sont pas pris en charge.

Il peut y avoir des conflits dans le fonctionnement du module de noyau mis à jour sur les appareils dotés de certaines versions de noyaux du système d'exploitation Linux, ainsi que lors de l'utilisation de certaines applications tierces.

Vous pouvez vérifier si votre appareil répond aux exigences d'installation du module de noyau mis à jour à l'aide de l'utilitaire Kaspersky ULKM tool.

Si votre système d'exploitation répond aux exigences, vous pouvez sélectionner le mécanisme d'interception basé sur le module de noyau mis à jour lors de l'installation de l'application. Le module de noyau mis à jour sera alors installé. Vous pouvez également installer le module de noyau mis à jour ultérieurement si la prise en charge de votre système d'exploitation devient disponible. Pour ce faire, procédez comme suit :

1. Exécutez la mise à jour des bases et des modules de l'application. Le module de noyau mis à jour est installé dans le cadre d'une mise à jour.
2. Sélectionnez le mécanisme d'interception basé sur un module de noyau mis à jour. Vous pouvez sélectionner le mécanisme d'interception des événements système dans **Web Console**, dans la Console d'administration ou dans la **ligne de commande**.

   Sur la ligne de commande, vous pouvez configurer les paramètres d'interception des événements système à l'aide `InterceptorMode`, `InterceptorFallbackStrategy` et `InterceptorApplyStrategy` dans les paramètres généraux de l'application.

   Les paramètres sont affichés et peuvent être modifiés uniquement sur les appareils dont le système d'exploitation prend en charge la technologie fanotify.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `InterceptorMode` vous permet de sélectionner le mécanisme d'interception des événements système que l'application utilise dans son travail. Le paramètre peut prendre les valeurs suivantes :

- `UseFanotify` pour utiliser la technologie fanotify afin d'intercepter les événements système.
- `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.

Le paramètre `InterceptorFallbackStrategy` est appliqué si un module de noyau mis à jour est sélectionné. Ce paramètre permet de spécifier l'action que l'application effectue en cas d'erreur au démarrage du module de noyau mis à jour. Le paramètre peut prendre les valeurs suivantes :

- `FallbackToFanotify` : passer à l'utilisation de la technologie fanotify pour intercepter les événements système en cas d'erreur lors du démarrage du module de noyau mis à jour.
- `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système en cas d'erreur lors du démarrage du module de noyau mis à jour. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Le paramètre `InterceptorApplyStrategy` est appliqué si un module de noyau mis à jour est sélectionné. Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis :

- `RestartServiceAutomatically` : redémarrer automatiquement l'application pour exécuter le module du noyau à actualiser.
- `RestartServiceManually` : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur.

Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.

Dans la Web Console, vous pouvez configurer l'interception des événements système dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Paramètres d'interaction du système d'exploitation**).

Ces paramètres ne s'appliquent qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Une application peut passer à l'utilisation d'un module de noyau mis à jour dans les situations suivantes :

- Si vous avez modifié le mécanisme d'interception des événements système dans les paramètres de l'application vers un module de noyau mis à jour.
- Si sur un appareil où le module de noyau mis à jour n'était pas en cours d'exécution, des mises à jour ont été reçues pendant la mise à jour des bases de l'application et des modules qui fournissent la prise en charge du module de noyau mis à jour.

Pour que l'application fonctionne correctement, le passage à l'utilisation du module de noyau mis à jour doit être effectué après le redémarrage automatique de l'application.

Si vous sélectionnez le mécanisme d'interception basé sur le module de noyau mis à jour, vous pouvez configurer le comportement de l'application si une erreur se produit lors du démarrage du module du noyau mis à jour et que le module ne démarre pas. Dans ce cas, l'application peut passer à l'utilisation de la technologie fanotify pour intercepter les événements système ou désactiver l'interception des événements système.

Vous pouvez afficher des informations sur l'état et la disponibilité du module de noyau mis à jour sur votre appareil :

- Dans Web Console ou dans la Console d'administration, en utilisant l'état du module fonctionnel **Module de noyau mis à jour**.
- Dans la ligne de commande à l'aide de la commande `kesl-control --app-info`.

Les informations sur l'état du module du noyau mis à jour sont affichées sous forme d'états :

- **Démarré** : le module est installé et en cours d'exécution.
- **Arrêté** : le module est installé mais ne fonctionne pas.
- **Indisponible** : le module n'est pas pris en charge sur l'appareil.
- **Erreur de fonctionnement** : une erreur s'est produite lors du démarrage du module, le module ne fonctionne pas.

Vérification de la possibilité d'installer un module du noyau à actualiser

Vous pouvez vérifier si votre appareil répond aux exigences d'installation du module de noyau mis à jour à l'aide de l'utilitaire Kaspersky ULKM tool.

Pour exécuter l'utilitaire à l'aide de Kaspersky Security Center Web Console ou à l'aide de la Console d'administration :

1. Téléchargez l'archive ulkmtool.zip depuis la page de téléchargement de l'application dans la section **Kaspersky Endpoint Security for Linux**.
2. Créez un paquet d'installation pour l'utilitaire.

   Comment créer un paquet d'installation dans Web Console

   1. Placez l'archive téléchargée ulkmtool.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center.
   2. Dans la fenêtre principale de Web Console, sélectionnez l'une des sections suivantes :
      - **Découverte et déploiement des appareils → Déploiement et attribution → Paquets d'installation**.
      - **Opérations → Stockages → Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

3. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création du paquet d'installation démarre.

4. Sélectionnez le mode de création du paquet d'installation : **Créer un paquet d'installation à partir d'un fichier**.

5. Saisissez le nom du nouveau paquet d'installation, cliquez sur le bouton **Parcourir** et spécifiez le chemin d'accès à l'archive ulkmtool.zip que vous avez téléchargée.

6. Quittez l'Assistant.

Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

Comment créer un paquet d'installation dans la Console d'administration

1. Décompressez l'archive ulkmtool.zip dans un dossier accessible au Serveur d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Avancés** → **Installation à distance** → **Paquets d'installation**.

   La liste des paquets d'installation disponibles sur le Serveur d'administration s'ouvrira.

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

   L'Assistant de création du paquet d'installation démarre.

4. Cliquez sur le bouton **Créer un paquet d'installation pour l'application Kaspersky**.

5. Saisissez le nom du nouveau paquet d'installation, puis passez à l'étape suivante de l'Assistant.

6. Cliquez sur le bouton **Parcourir** et spécifiez le chemin d'accès au fichier ulkmtool.kud. Le fichier se trouve dans le dossier où vous avez décompressé l'archive ulkmtool.zip.

   Passez à l'étape suivante de l'Assistant.

7. Attendez que le fichier soit téléchargé et quittez l'Assistant.

Le paquet d'installation est alors créé et ajouté à la liste des paquets d'installation.

3. Installez l'Agent d'administration de Kaspersky Security Center sur les appareils dont vous souhaitez vérifier la conformité avec les exigences d'installation du module de noyau mis à jour.

   Comment installer l'Agent d'administration

   1. Préparez vos appareils Linux pour l'installation de l'Agent d'administration. L'ensemble des actions nécessaires dépend du système d'exploitation.

   2. Installez et effectuez la configuration initiale de l'Agent d'administration. Consultez l'aide de Kaspersky Security Center pour obtenir des instructions.

4. Dans Kaspersky Security Center Web Console ou la Console d'administration de Kaspersky Security Center, créez et exécutez une tâche d'Installation à distance des applications sur les appareils dont vous souhaitez vérifier la conformité. Dans les paramètres de la tâche, sélectionnez le paquet d'installation que vous avez créé.

   Pour obtenir une description de la procédure d'installation à distance, consultez l'aide de Kaspersky Security Center.

   Les résultats de l'exécution de la tâche pour chaque appareil sur lequel la tâche a été exécutée indiquent si l'appareil prend en charge l'installation et le fonctionnement du module de noyau mis à jour.

En fonction des résultats de la tâche, une étiquette est automatiquement attribuée à chaque appareil :

- *UpdatableKernelModule=No* : l'appareil ne prend pas en charge l'installation d'un module de noyau mis à jour.
- *UpdatableKernelModule=Oui* : l'appareil répond aux exigences d'installation et d'exécution d'un module de noyau mis à jour.
- *UpdatableKernelModule=Use* : l'appareil dispose d'un module de noyau mis à jour installé et en cours d'exécution.
- *UpdatableKernelModule=Error* : un module de noyau pouvant être mis à jour est installé sur l'appareil, mais une erreur s'est produite lors du démarrage du module, le module ne fonctionne pas.

Vous pouvez utiliser ces tags pour créer des sélections d'appareils. Par exemple, vous pouvez sélectionner des appareils qui répondent aux exigences du module de noyau mis à jour et installer l'application Kaspersky Endpoint Security avec le module de noyau mis à jour sur ces appareils.

Mode « Sécurisé » lors de l'utilisation d'un module de noyau mis à jour

Si l'application est instable lors de l'utilisation du module de noyau mis à jour, après avoir atteint le nombre maximal spécifié d'arrêts anormaux, l'application bascule automatiquement en mode de fonctionnement « sécurisé » (`SafeMode=yes` est défini dans le fichier de configuration kesl.ini). Par défaut, l'application passe en mode « sécurisé » après trois arrêts anormaux. Le nombre maximal d'arrêts anormaux de l'application est configuré dans le paramètre `PanicThreshold` du fichier de configuration kesl.ini.

Si l'application s'exécute en mode « sécurisé », le module de noyau mis à jour n'est pas lancé et l'application passe à l'utilisation de la technologie fanotify pour intercepter les événements système. L'application envoie le tag `UpdatableKernelModule=Error` à Kaspersky Security Center.

Pour continuer à utiliser le module de noyau mis à jour après avoir résolu les problèmes de l'application, vous devez désactiver le mode de fonctionnement « sécurisé ».

Pour désactiver le mode « sécurisé » de l'application :

1. Ouvrez le fichier /var/opt/kaspersky/kesl/common/kesl.ini pour le modifier.
2. Dans la section `[General]`, définissez la valeur du paramètre `SafeMode=no`.
3. Redémarrez Kaspersky Endpoint Security :

   ```
   systemctl restart kesl
   ```

Configuration des paramètres d'interception dans Web Console

Dans la Web Console, vous pouvez configurer l'interception des événements système dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres d'interaction du système d'exploitation**).

Ces paramètres ne s'appliquent qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Configuration des paramètres d'interception dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres d'interception des événements système dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** →**Paramètres d'interaction avec le système d'exploitation**, **Paramètres d'interception des événements système**).

Ces paramètres ne s'appliquent qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.

Paramètres d'interception des événements système

Paramètre	Description
Mécanisme d'interception	Le mécanisme d'interception des événements système utilisé par l'application dans son travail : • **Technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, l'application utilise le module de noyau mis à jour pour l'interception des événements système.
Si le module de noyau mis à jour ne parvient pas à démarrer	Action effectuée par l'application si le module de noyau mis à jour ne parvient pas à démarrer : • **Utiliser la technologie fanotify** (valeur par défaut). Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système** Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau à actualiser** est sélectionné.

Configuration des paramètres d'interception dans la ligne de commande

Sur la ligne de commande, vous pouvez configurer les paramètres d'interception des événements système à l'aide `InterceptorMode`, `InterceptorFallbackStrategy` et `InterceptorApplyStrategy` dans les paramètres généraux de l'application.

Les paramètres sont affichés et peuvent être modifiés uniquement sur les appareils dont le système d'exploitation prend en charge la technologie fanotify.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `InterceptorMode` vous permet de sélectionner le mécanisme d'interception des événements système que l'application utilise dans son travail. Le paramètre peut prendre les valeurs suivantes :

- `UseFanotify` pour utiliser la technologie fanotify afin d'intercepter les événements système.
- `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.

Le paramètre `InterceptorFallbackStrategy` est appliqué si un module de noyau mis à jour est sélectionné. Ce paramètre permet de spécifier l'action que l'application effectue en cas d'erreur au démarrage du module de noyau mis à jour. Le paramètre peut prendre les valeurs suivantes :

- `FallbackToFanotify` : passer à l'utilisation de la technologie fanotify pour intercepter les événements système en cas d'erreur lors du démarrage du module de noyau mis à jour.
- `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système en cas d'erreur lors du démarrage du module de noyau mis à jour. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Le paramètre `InterceptorApplyStrategy` est appliqué si un module de noyau mis à jour est sélectionné. Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis :

- `RestartServiceAutomatically` : redémarrer automatiquement l'application pour exécuter le module du noyau à actualiser.
- `RestartServiceManually` : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur.

Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.

Configuration des paramètres avancés de la télémétrie

Vous pouvez configurer les paramètres avancés suivants pour la collecte de télémétrie envoyée aux solutions Detection and Response lors de leur intégration :

- Source de la télémétrie. La collecte de télémétrie peut être réalisée à l'aide d'eBPF et du service auditd, ou d'eBPF seul.
- Mode d'utilisation du service auditd. Kaspersky Endpoint Security peut utiliser le service auditd en mode exclusif ou en mode multidiffusion.

Configuration dans Web Console

Dans Web Console, vous pouvez gérer les paramètres avancés de télémétrie dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres d'interaction du système d'exploitation**).

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres complémentaires de télémétrie dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** →**Paramètres d'interaction avec le système d'exploitation**, **Paramètres complémentaires de télémétrie**).

Paramètres avancés de collecte de télémétrie

Paramètre	Description
Source de la télémétrie	Source de collecte de télémétrie utilisée par Kaspersky Endpoint Security : • **Utiliser eBPF uniquement** : utiliser la technologie eBPF seule pour la collecte de télémétrie. • **Utiliser eBPF et auditd** (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie.
Utilisation d'auditd	Mode d'utilisation du service auditd : • **Mode exclusif** (valeur par défaut) : l'application Kaspersky Endpoint Security utilise le service auditd en mode exclusif. • **Mode multidiffusion** : le service auditd est utilisé en mode multidiffusion. Ce paramètre s'applique uniquement si l'option **Utiliser eBPF et auditd** est sélectionnée pour le paramètre **Source de télémétrie**.

Configuration sur la ligne de commande

À partir de la ligne de commande, vous pouvez gérer les paramètres de télémétrie supplémentaires à l'aide des paramètres `TelemetrySource` et `UseTelemetryMonopolyMode` de la tâche prédéfinie Behavior_Detection.

Vous pouvez modifier les paramètres à l'aide de la commande `kesl-control --set-settings 20`, en modifiant le fichier de configuration qui contient tous les paramètres de la tâche ou en utilisant les options de ligne de commande au format < `nom du paramètre` >=< `valeur du paramètre` >.

Le paramètre `TelemetrySource` spécifie la source de télémétrie. Le paramètre peut prendre les valeurs suivantes :

- `Default` (valeur par défaut) : utiliser la technologie eBPF et le service auditd pour la collecte de télémétrie.
- `OnlyEBPF` : utiliser uniquement la technologie eBPF pour la collecte de télémétrie.

Le paramètre `UseTelemetryMonopolyMode` permet de spécifier le mode dans lequel le service auditd est utilisé lorsqu'il est utilisé pour collecter la télémétrie. Le paramètre peut prendre les valeurs suivantes :

- `True` (valeur par défaut) : Kaspersky Endpoint Security utilise le service auditd en mode exclusif.
- `False` signifie que le service auditd est utilisé en mode multidiffusion.

Le paramètre `UseTelemetryMonopolyMode` est appliqué uniquement si le paramètre `TelemetrySource` est défini sur `Default`.

Sauvegarde

Si, lors de l'analyse d'un appareil protégé, Kaspersky Endpoint Security détecte un code malveillant dans un fichier, l'application peut bloquer le fichier, lui attribuer l'état *Infecté*, et placer une copie dans la sauvegarde et tenter de désinfecter le fichier.

La *sauvegarde* est un stockage des copies de sauvegarde des fichiers qui ont été supprimés ou modifiés pendant la désinfection. La *copie de sauvegarde* est une copie d'un fichier créée avant que le fichier ne soit désinfecté ou supprimé. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Par défaut, le répertoire /var/opt/kaspersky/kesl/common/objects-backup/ est utilisé pour stocker les copies de sauvegarde des fichiers. Ce répertoire stocke également les fichiers mis en quarantaine. Vous pouvez modifier le répertoire dans lequel les objets de sauvegarde et de quarantaine sont stockés à l'aide de la ligne de commande.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations importantes devenues totalement ou partiellement inaccessibles suite au traitement, vous pouvez tenter de restaurer le fichier à partir d'une copie de sauvegarde de celui-ci.

La restauration d'objets infectés peut infecter l'appareil.

Les fichiers sauvegardés dans la sauvegarde peuvent contenir des données personnelles. Pour accéder aux objets de la sauvegarde, les privilèges root sont requis.

Vous pouvez configurer les paramètres de la sauvegarde sur un appareil à l'aide d'une stratégie dans Web Console, dans la Console d'administration ou à l'aide de la ligne de commande. Vous pouvez configurer les paramètres suivants de la sauvegarde :

- Durée de stockage des objets dans la sauvegarde. Par défaut, les objets sont stockés pendant 30 jours.
- Taille maximale de la sauvegarde. Par défaut, la taille de la sauvegarde est illimitée.

Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine (ce paramètre est configurable uniquement à l'aide de la ligne de commande).

Une fois qu'un délai spécifié s'est écoulé ou que la taille maximale de la sauvegarde a été atteinte, l'application supprime automatiquement les copies de sauvegarde les plus anciennes des fichiers avec n'importe quel état de la sauvegarde.

Vous pouvez également supprimer vous-même la copie de sauvegarde du fichier restauré et non restauré.

Une liste générale des fichiers placés dans la sauvegarde par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans la Console d'administration (**Avancés** → **Stockages** → **Sauvegarde**) et dans Web Console (**Opérations** → **Stockages** → **Sauvegarde**). Vous pouvez afficher les propriétés des fichiers situés dans la sauvegarde sur les appareils protégés et en supprimer des fichiers. Kaspersky Security Center ne copie pas les fichiers de la sauvegarde vers le Serveur d'administration ; tous les fichiers sont placés dans la sauvegarde sur les appareils protégés. La récupération de fichiers est effectuée sur un appareil protégé.

Le fichier mis dans la sauvegarde est restauré à son emplacement d'origine selon les paramètres spécifiés. L'étiquette de mandat (uniquement sur les appareils exécutant Astra Linux) et les attributs du fichier source (sauf les attributs immutable et append-only) sont conservés lors de la restauration.

Sur les appareils exécutant Astra Linux, la restauration d'un fichier à partir d'une sauvegarde se termine par une erreur si :

- L'étiquette de mandat du fichier est supérieure à l'étiquette de capacité du répertoire de destination.
- L'étiquette de mandat du fichier est inférieure à celle du répertoire de destination et l'indicateur ccnr n'est pas défini pour ce répertoire.

Pour effectuer des actions avec les fichiers de la sauvegarde dans Kaspersky Security Center, vous devez activer le transfert de données sur les fichiers de la sauvegarde vers le Serveur d'administration.

Configuration des paramètres de la sauvegarde dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de la sauvegarde dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Rapports et stockage**) et dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Paramètres de stockage**).

Les paramètres de la sauvegarde dans les propriétés de la stratégie de Web Console sont décrits dans l'Annexe 5.

Les paramètres de la sauvegarde dans les propriétés de l'appareil administré sont décrits dans le tableau ci-dessous.

Paramètres de la sauvegarde dans les propriétés de l'appareil

Paramètre	Description
Ne pas conserver les objets plus de (jours)	Le champ de saisie pour spécifier la période de conservation des objets dans la sauvegarde. Valeurs admises : 1 à 10000. Si la case n'est pas cochée, la durée de conservation des objets dans la sauvegarde est illimitée. Valeur par défaut : 30.
Limiter la taille de la sauvegarde à (Mo)	Champ de saisie pour spécifier la taille maximale de la sauvegarde (en mégaoctets). Si la case est décochée, la taille de la sauvegarde n'est pas limitée. Valeur par défaut : 1024.

Configuration des paramètres de la sauvegarde dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de la quarantaine dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres des stockages**) et dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres des stockages**).

Paramètres de sauvegarde

Paramètre	Description
Ne pas conserver les objets plus de (jours)	La case active ou désactive la limitation de la période de stockage des objets dans la sauvegarde selon un intervalle de temps spécifié. Valeurs admises : 0 à 10000. Si la valeur définie est 0, les objets sont conservés dans la sauvegarde pour une période indéterminée. Valeur par défaut : 30.
Limiter la taille de la sauvegarde à (Mo)	La case active ou désactive la limitation de la taille maximale de la sauvegarde par la valeur spécifiée (en mégaoctets). Valeurs admises : 1 à 999999. Si la case est décochée, la taille de la sauvegarde n'est pas limitée. La case est décochée par défaut.

Configuration des paramètres de la Sauvegarde via la ligne de commande

À partir de la ligne de commande, vous pouvez configurer les paramètres de la sauvegarde à l'aide des paramètres `BackupDaysToLive`, `BackupSizeLimit` et `QuarantineBackupFolder` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Paramètres de sauvegarde

Paramètre	Description	Valeur
`BackupDaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Après une durée spécifiée, l'application supprime les fichiers de sauvegarde les plus anciens. Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.	0 – 10000 0 : la durée de conservation des objets dans la sauvegarde n'est pas limitée. Valeur par défaut : 30.
`BackupSizeLimit`	Volume maximal de la sauvegarde (Mo). Quand la taille de la sauvegarde atteint la valeur maximale définie, l'application supprime les objets les plus anciens. Pour supprimer la limite sur la taille de la sauvegarde, spécifiez la valeur 0.	0 – 999999 0 : la taille de la sauvegarde est illimitée. Valeur par défaut : 0.
`QuarantineBackupFolder`	Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine. Vous pouvez définir un répertoire autre que celui défini par défaut. Les répertoires de n'importe quel appareil peuvent être utilisés comme répertoire pour stocker des objets de sauvegarde et de quarantaine. Il est déconseillé de désigner des répertoires qui se trouvent sur des appareils à distance, par exemple des répertoires montés via les protocoles Samba et NFS. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : /var/opt/kaspersky/kesl/common/objects-backup/ L'accès au répertoire par défaut requiert les privilèges root.

Utilisation des objets de Sauvegarde sur la ligne de commande

Dans la ligne de commande, à l'aide des commandes de gestion de la sauvegarde, vous pouvez effectuer les actions suivantes avec les objets de la sauvegarde :

- Afficher des informations sur les objets de la sauvegarde.
- Supprimer tous les objets spécifiés ou uniquement ceux spécifiés de la sauvegarde.
- Restaurer les objets à partir de la sauvegarde.

La restauration d'objets infectés peut infecter l'appareil.

Affichage des informations sur les objets de la sauvegarde

Pour afficher des informations sur les objets de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --query ["<conditions de filtrage>"] [-n <nombre>] [--json]
```

où :

- `<conditions de filtrage>` spécifient une ou plusieurs expressions logiques au format `<champ> <opération de comparaison> '<valeur>'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtre, l'application affichera des informations sur tous les objets de la sauvegarde.
- `<nombre>` indique le nombre d'objets les plus récents dans le stockage à afficher. Si vous ne spécifiez pas la clé `-n`, l'application affichera les informations des 30 objets les plus récents. Pour afficher les informations de tous les objets, indiquez la valeur `0`.
- `--json` : afficher les données au format JSON.

La ligne `ObjectId` affichera l'identifiant numérique que l'application a attribué à l'objet lors de son placement dans la sauvegarde. Cet identifiant est utilisé pour effectuer des actions sur un objet, telles que la restauration ou la suppression d'un objet de la Sauvegarde.

Restauration des objets depuis la sauvegarde

Pour restaurer un objet sous son nom d'origine dans son emplacement d'origine, exécutez la commande suivante :

```
kesl-control -B --restore <identifiant de l'objet>
```

où < identifiant de l'objet > est l'identifiant numérique que l'application a attribué à l'objet lors de son placement dans la Sauvegarde.

Pour restaurer un objet sous un nouveau nom dans le répertoire indiqué, exécutez la commande suivante :

```
kesl-control -B --restore < identifiant de l'objet > --file < chemin d'accès au fichier >
```

où --file < chemin d'accès au fichier > est le nouveau nom du fichier et le chemin d'accès au répertoire dans lequel vous souhaitez l'enregistrer. Si le répertoire indiqué n'existe pas, l'application le crée.

Sur les appareils exécutant le système d'exploitation Astra Linux, en mode environnement logiciel fermé, vous ne pouvez restaurer un fichier que sous le compte sous lequel il a été placé dans la sauvegarde.

Suppression des objets de la sauvegarde

Pour supprimer les objets sélectionnés de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --mass-remove --query "< conditions de filtrage >"
```

où < conditions de filtrage > correspond à une ou plusieurs expressions logiques au format < champ > < opérateur de comparaison > '< valeur >', combinées à l'aide de l'opérateur logique and pour limiter les résultats.

Exemples :
Pour supprimer l'objet ayant ID=15 :

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

Pour supprimer les objets qui contiennent "test" dans leur nom ou chemin :

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

Pour supprimer tous les objets de la sauvegarde, exécutez la commande suivante :

```
kesl-control -B --mass-remove
```

Intégration avec les 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 de Detection and Response vous fournissent des informations sur les menaces détectées et vous permettent de gérer votre réponse aux détections.

Kaspersky Endpoint Security peut interagir avec les solutions de détection et de réponse suivantes de Kaspersky :

- Kaspersky Endpoint Detection and Response Expert (on-premise) sur Open Single Management Platform (OSMP). L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response Expert (on-premise) (ci-après également *EDR Expert (on-premise)*).
- Les modules Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sont intégrés à Kaspersky Anti Targeted Attack Platform. L'intégration est assurée par les modules suivants de Kaspersky Endpoint Security :
  - Endpoint Detection and Response Expert (on-premise) (ci-après également *EDR Expert (on-premise)*).
  - Network Detection and Response (KATA) (ci-après également *NDR (KATA)*).
- Sandbox sur Open Single Management Platform (OSMP) ou sur Kaspersky Anti Targeted Attack Platform. L'intégration est assurée par le module *Sandbox* de l'application Kaspersky Endpoint Security.
- Kaspersky Unified Monitoring and Analysis Platform.
- Kaspersky Endpoint Detection and Response Optimum. L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (ci-après également appelé *EDR Optimum*).
- Kaspersky Managed Detection and Response. L'intégration est assurée par le module de l'application Kaspersky Endpoint Security – Managed Detection and Response (ci-après également appelé *MDR*).

Si vous utilisez Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent, l'intégration est prise en charge uniquement avec Kaspersky Endpoint Detection and Response Expert (on-premise) sur Open Single Management Platform (OSMP) et avec les modules Kaspersky Endpoint Detection and Response et Kaspersky Network Detection and Response sur Kaspersky Anti Targeted Attack Platform.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec les solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform, un grand nombre d'événements peuvent être enregistrés dans le journal système. Si vous souhaitez désactiver la journalisation des audits dans systemd, vous devez désactiver le socket systemd-journald-audit et redémarrer le système d'exploitation.

Pour désactiver le socket systemd-journald-audit, exécutez les commandes suivantes :

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket
```

```
systemctl mask systemd-journald-audit.socket
```

Par défaut, sur le système d'exploitation SynthesisM-Client, la configuration du service auditd est bloquée contre les modifications, c'est-à-dire qu'elle est dans le mode de fonctionnement `enabled 2`. Pour que le module Détection comportementale fonctionne correctement lors de l'intégration de Kaspersky Endpoint Security avec les solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform, vous devez modifier le mode de fonctionnement auditd dans les fichiers de configuration en mode sans bloquer la configuration `enabled 1` et redémarrer le système d'exploitation.

Les solutions Detection and Response peuvent ne pas fonctionner correctement sur les machines virtuelles créées à partir d'une image sur laquelle Kaspersky Endpoint Security for Linux est installé. Lors de l'intégration aux solutions Detection and Response, un identifiant unique (Sensor ID) de l'ordinateur est utilisé. L'application génère cet identifiant lors de l'installation initiale, et il est conservé même après la désinstallation de l'application. Lors du clonage d'une image, la machine virtuelle hérite du Sensor ID, ce qui peut conduire les solutions Detection and Response à identifier plusieurs machines virtuelles comme étant le même appareil.

Recommandations relatives à la création d'une image de référence pour une intégration correcte avec MDR

Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premise)

À propos des actions pour répondre aux commandes des solutions Detection and Response

Lors de l'intégration avec les solutions Detection and Response, l'application Kaspersky Endpoint Security peut effectuer des actions de réponse visant à garantir les fonctions de sécurité. Les actions de réponse peuvent être générées côté solution Detection and Response et exécutées automatiquement sur les appareils équipés de Kaspersky Endpoint Security si cette fonction est activée dans les paramètres de la solution Detection and Response. Vous pouvez également configurer et exécuter manuellement les actions de réponse.

Les options de réponse varient en fonction de la solution Detection and Response avec laquelle l'application Kaspersky Endpoint Security est intégrée.

L'application Kaspersky Endpoint Security peut effectuer les actions de réponse suivantes :

- Isolation réseau d'un appareil.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, l'isolement du réseau est activé et désactivé du côté de la solution Detection and Response correspondante. Vous pouvez désactiver manuellement l'isolement réseau d'un appareil.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, l'appareil peut être isolé du réseau automatiquement ou manuellement. Vous pouvez configurer les paramètres d'isolement du réseau et désactiver manuellement l'isolement du réseau pour votre appareil.

- Mettre un fichier en quarantaine.

  L'action est effectuée à l'aide de la tâche de mise des fichiers en quarantaine (Quarantine file).

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, un fichier peut être mis en quarantaine automatiquement suite à la détection d'indicateurs de compromission.

Lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response, vous pouvez également mettre les fichiers en quarantaine manuellement.

- Restauration d'un fichier depuis la quarantaine.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, l'action de réponse est générée du côté de la solution Detection and Response correspondante. Vous pouvez également effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

- Suppression d'un fichier de la quarantaine.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), la réaction est mise en œuvre du côté de la solution Detection and Response correspondante. Vous pouvez également effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center ou à l'aide de la ligne de commande.

- Récupération d'un fichier depuis la quarantaine.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), la réaction est mise en œuvre du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez effectuer l'action manuellement à l'aide de Kaspersky Security Center.

- Réception d'un fichier depuis l'appareil.

  L'action est effectuée à l'aide de la tâche d'obtention du fichier depuis l'appareil (*Get file*). Par exemple, vous pouvez configurer pour recevoir un fichier journal des événements généré par un logiciel tiers.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer des tâches pour recevoir des fichiers à partir des appareils dans Web Console.

- Suppression d'un fichier de l'appareil.

  L'action est effectuée à l'aide de la tâche de suppression du fichier de l'appareil (*Delete file*).

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer des tâches de suppression des fichiers à partir des appareils dans Web Console.

- Lancer à distance un processus sur un appareil.

  L'action est effectuée à l'aide de la tâche d'exécution du processus (*Run application*). Par exemple, vous pouvez exécuter à distance un utilitaire qui crée un fichier de configuration de l'appareil, puis récupérer le fichier créé à l'aide de la tâche de réception d'un fichier depuis un appareil.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer et exécuter des tâches de lancement des processus dans Web Console.

- Terminer à distance un processus sur un appareil.

  L'action est effectuée à l'aide de la tâche de fin du processus (*Kill process*). Par exemple, vous pouvez arrêter à distance l'utilitaire de test de vitesse Internet lancé à l'aide de la tâche de démarrage du processus.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, la tâche est créée et lancée du côté de la solution Detection and Response correspondante.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez créer et exécuter des tâches de terminaison des processus dans Web Console.

- Détecter les *indicateurs de compromission (IOC)* sur les appareils. *Indicateur de compromission (Indicator of Compromise, IOC)* est un ensemble de données sur un objet ou une activité qui indique un accès non autorisé à un appareil (compromission de données). Par exemple, un indicateur de compromission pourrait être un nombre élevé de tentatives de connexion échouées.

  Lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Expert (on-premise) ou à Kaspersky Endpoint Detection and Response (KATA), une tâche d'analyse IOC est créée et lancée sur un appareil où Kaspersky Endpoint Security est installé, côté solution Detection and Response correspondante.

  Lorsqu'elle est intégrée avec Kaspersky Endpoint Detection and Response Optimum, l'analyse IOC est effectuée à l'aide de la tâche d'analyse IOC (*IOC Scan*). Vous pouvez créer des tâches d'analyse IOC manuellement :

- Lancement de l'*analyse YARA*. Une *analyse YARA* est un processus au cours duquel Kaspersky Endpoint Security utilise des fichiers YARA pour rechercher des signatures d'activités malveillantes sur l'appareil. Les *fichiers YARA* sont des fichiers avec l'extension YARA ou YAR qui contiennent des règles YARA. Les *règles YARA* décrivent les signatures des attaques ciblées et des intrusions dans l'infrastructure informatique d'une organisation. Kaspersky Endpoint Security analyse les objets à l'aide de ces règles. Si une règle est détectée, l'analyseur signale une infection et consigne les détails correspondants dans le journal. L'analyse est effectuée de manière récursive sur les disques locaux. L'analyse des ressources réseau, connectées et cloud n'est pas prise en charge.

  La commande d'analyse YARA sur un appareil où Kaspersky Endpoint Security est installé est créée et exécutée par Kaspersky Endpoint Detection and Response Expert (on-premise).

- Prévention de l'exécution

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez activer l'application de règles de prévention du lancement des objets. L'application Kaspersky Endpoint Security prévient le lancement des objets ou l'ouverture de documents répondant aux critères des règles de prévention.

  Lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Expert (on-premise) ou à Kaspersky Endpoint Detection and Response (KATA), l'application reçoit les règles de la prévention du lancement de ces mêmes logiciels.

  Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez configurer des règles de prévention du lancement des objets dans Web Console.

- Collecte de données forensiques.

  L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) permet de collecter des données numériques pouvant servir de preuves lors d'enquêtes sur des cybercrimes et des fuites de données.

Ceci est réalisé à l'aide des tâches suivantes :

- une tâche de collecte de données forensiques *Get forensics*, qui collecte les types d'informations suivants :
  - une liste de fichiers
  - une liste de processus
  - une liste de points de démarrage
- des tâches de génération de vidage mémoire (*Get memory dump*)
- des tâches de génération d'un vidage de mémoire du processus (*Get process memory dump*)
- des tâches d'image disque (*Get disk image*)

Les tâches sont créées et exécutées du côté de la solution Kaspersky Endpoint Detection and Response Expert (on-premise).

Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)

Kaspersky Endpoint Detection and Response Expert (on-premise) est une solution de cybersécurité pour entreprises qui permet de se protéger contre la plupart des risques de cybersécurité et couvre les principaux scénarios de propagation des menaces. Les modules de Kaspersky Endpoint Detection and Response Expert (on-premises) sont déployés sur la plateforme de gestion unique Open Single Management Platform (OSMP). Pour plus d'informations sur la solution et la plateforme, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premise).

Lors de l'intégration à Kaspersky Endpoint Detection and Response Expert (on-premise), Kaspersky Endpoint Security peut effectuer les actions suivantes :

- Les données d'événements des appareils (télémétrie) sont envoyées au serveur de collecte de télémétrie sur la plateforme OSMP (ci-après dénommé *serveur de collecte de télémétrie OSMP*). Kaspersky Endpoint Security envoie au serveur de collecte de télémétrie des données de surveillance sur les processus, les connexions réseau ouvertes et les fichiers modifiés, ainsi que des données sur les menaces détectées par l'application et des données sur les résultats du traitement de ces menaces.

- Des actions de réponse visant à garantir les fonctions de sécurité sont mises en œuvre en fonction des commandes reçues du serveur d'actions de réponse sur la plateforme OSMP (ci-après dénommé *d'actions de réponse OSMP*).

L'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) est assurée par le module de l'application Kaspersky Endpoint Security, Endpoint Detection and Response Expert (on-premise) (ci-après également dénommé *EDR Expert (on-premise)*).

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), les appareils exécutant Kaspersky Endpoint Security établissent des connexions HTTPS chiffrées avec le serveur d'actions de réponse aux menaces OSMP et le serveur de télémétrie OSMP. Les certificats suivants émis par les serveurs OSMP sont utilisés pour sécuriser la connexion :

- Certificat du serveur. La connexion est chiffrée à l'aide du certificat TLS du serveur. Vous pouvez augmenter le niveau de sécurité de la connexion en activant la vérification du certificat du serveur du côté de Kaspersky Endpoint Security. Pour ce faire, vous devez ajouter le certificat du serveur avant d'activer l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise).

- Certificat client. Ce certificat est utilisé pour sécuriser davantage la connexion avec une vérification en deux étapes (c'est-à-dire, l'analyse des appareils avec l'application Kaspersky Endpoint Security par les serveurs OSMP). Le même certificat client peut être utilisé par plusieurs appareils. Par défaut, le serveur ne vérifie pas les certificats clients, mais la vérification en deux étapes peut être activée côté Kaspersky Endpoint Detection and Response Expert (on-premises). Dans ce cas, vous devez activer l'authentification bidirectionnelle dans les paramètres du module EDR Expert (on-premises) et ajouter un certificat client (cryptocontainer avec certificat et clé privée).

Les certificats permettant de sécuriser les connexions aux serveurs OSMP sont fournis par l'administrateur de la plateforme OSMP.

Si l'utilisation d'un serveur proxy est configuré dans les paramètres généraux de l'application Kaspersky Endpoint Security, il est utilisé pour se connecter aux serveurs OSMP.

Pour utiliser la fonctionnalité Endpoint Detection and Response Expert (on-premise), vous devez activer le module EDR Expert (on-premise). Si la licence principale sous laquelle vous utilisez l'application Kaspersky Endpoint Security n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez acheter une licence distincte pour cette fonctionnalité et ajouter la clé de licence EDR Expert (on-premise) à l'application.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant des clés de licence à la SVM.

L'intégration avec Endpoint Detection and Response Expert (on-premise) comprend les étapes suivantes :

1. **Activation des modules requis de Kaspersky Endpoint Security**

   Le module EDR Expert (on-premise) peut utiliser les données des modules suivants :

   - Protection contre les fichiers malicieux.
   - Protection contre les menaces réseau.
   - Protection contre les menaces Internet.
   - Protection contre le chiffrement.
   - Contrôle des applications.
   - Contrôle des appareils.
   - Contrôle de l'intégrité du système.

Pour une intégration complète de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez activer le module Détection comportementale. Si la Détection comportementale est désactivée, aucune donnée de télémétrie requise n'est transmise (à l'exception des demandes de synchronisation et des données de détection des menaces provenant d'autres modules de protection).

Lorsque vous utilisez le mécanisme eBPF pour obtenir la télémétrie du système dans le module Détection comportementale (disponible sur les systèmes d'exploitation 64 bits avec la version de noyau 4.18 et supérieure avec prise en charge eBPF), les données de télémétrie seront plus complètes.

2. **Activation du module EDR Expert (on-premise)**

   Assurez-vous que l'une des conditions suivantes est remplie :

   - Vous utilisez l'application Kaspersky Endpoint Security sous une licence qui inclut la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise).
   - Vous avez acheté une licence distincte pour utiliser la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise) et ajouté à l'application une clé de licence EDR Expert (on-premise).

     Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, une clé de licence pour activer des fonctionnalités supplémentaires est ajoutée à la SVM.

3. **Activation du module EDR Expert (on-premise)**

   L'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) est désactivée par défaut. Pour activer l'intégration, vous devez activer le module EDR Expert (on-premise) et configurer ses paramètres.

   - à l'aide de Kaspersky Security Center Web Console ;
   - À l'aide de la ligne de commande.

   La configuration de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans la Console d'administration de Kaspersky Security Center n'est pas prise en charge.

   Pour intégrer Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez sélectionner le mode d'intégration *EDR Expert (OSMP)* dans les paramètres du module EDR Expert (on-premise). Si vous utilisez Web Console, sélectionnez **Endpoint Detection and Response Expert (version 8.0 et supérieures)** dans les paramètres de la stratégie. Si vous utilisez la ligne de commande, définissez le paramètre `Mode=EDRExpertOnPrem` dans les paramètres de tâche. Pour configurer l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) sur un appareil, dans Web Console, vous devez gérer les « cadenas » pour l'une ou l'autre version (version 8.0 et ultérieure, et version 7.1 et antérieure).

Pour utiliser la fonctionnalité de la prévention du lancement des objets, vous pouvez activer l'application des règles de la prévention du lancement des objets du module EDR Expert (on-premise).
Vous pouvez vérifier l'état de fonctionnement du module EDR Expert (on-premise) :

- Utilisation du *Rapport sur l'état des modules de l'application* dans Web Console.

  Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

- Dans les propriétés de l'appareil dans Web Console (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → **Général** → **Modules**).

- À l'aide de la ligne de commande, en exécutant la commande `kesl-control --app-info`.

Comment préparer une image de référence pour une intégration correcte avec EDR Expert (on-premise)

Avant de préparer l'image, assurez-vous que le fichier `/var/opt/kaspersky/.ids_generated` n'existe pas sur l'appareil de référence.

Pour préparer une image de référence en vue d'une intégration correcte avec Kaspersky Endpoint Detection and Response Expert (on-premise) :

Ne redémarrez pas l'appareil de référence ni l'application Kaspersky Endpoint Security pendant que vous suivez ces instructions.

1. Exécutez les commandes suivantes en tant que root :

   ```
   systemctl stop kesl
   systemctl edit kesl
   ```

2. Dans l'éditeur, ajoutez l'une des configurations suivantes entre les lignes `### Anything between here and the comment below will become the contents of the drop-in file` et `### Edits below this comment will be discarded` :

   - Mettez à jour le SensorID à chaque démarrage de l'application sur les machines virtuelles temporaires

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - Mettez à jour le SensorID une seule fois sur les machines virtuelles persistantes

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. Enregistrez vos modifications et fermez l'éditeur.

   Le fichier `/etc/systemd/system/kesl.d/override.conf` est créé. Vérifiez son contenu pour vous assurer qu'il correspond à la configuration ajoutée.

4. Rechargez le service systemd en exécutant la commande suivante :

   ```
   systemctl daemon-reload
   ```

5. Créez le fichier `/usr/bin/uuid-regen.sh` avec le contenu suivant :

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ---------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode ----------------------------------------------
MODE="a"
# ----- parse command-line arguments ------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file -----------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini ---------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. Modifiez les autorisations du fichier `/usr/bin/uuid-regen.sh` à l'aide de la commande suivante :

```
chmod 700 /usr/bin/uuid-regen.sh
```

L'appareil de référence est maintenant prêt pour la création de l'image du système d'exploitation.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans Web Console

Dans Web Console, vous pouvez activer ou désactiver le module EDR Expert (on-premise) et gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans les propriétés de la stratégie (**Paramètres de l'application → Configuration des agents intégrés → Endpoint Detection and Response Expert (on-premise)**).

Pour intégrer Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez activer le module EDR Expert (on-premise) et sélectionner l'option **Endpoint Detection and Response Expert (version 8.0 et supérieures)**, c'est-à-dire le mode d'intégration *EDR Expert (OSMP)*.

Pour les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), les stratégies de niveau hiérarchique imbriqué vous permettent désormais de définir vos propres valeurs, même si tous les autres paramètres de la stratégie sont hérités. Si l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) est activée dans la stratégie parent et que l'héritage des paramètres dans la stratégie enfant est activé, alors par défaut, les paramètres d'intégration dans la stratégie enfant sont également hérités et ne peuvent pas être modifiés. Si vous souhaitez configurer vos propres paramètres d'intégration, sélectionnez l'option **Utiliser les paramètres de connexion personnalisés** dans la liste déroulante. Les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) pourront être modifiés.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) dans la ligne de commande

Dans la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) sur la plate-forme OSMP à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)*.

Cette tâche permet également de configurer les paramètres d'intégration avec le module Kaspersky Endpoint Detection and Response (KATA). Pour l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez sélectionner le mode d'intégration *EDR Expert (OSMP)* et gérer les paramètres d'intégration selon les besoins.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) en modifiant les paramètres d'une tâche prédéfinie.

Par défaut, la tâche *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez gérer les certificats utilisés pour se connecter aux serveurs OSMP à l'aide des commandes d'administration des modules EDR Expert (on-premises).

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)

Le tableau ci-dessous décrit les paramètres de la tâche préinstallée *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)* que vous pouvez configurer lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise).

Cette tâche permet également de configurer les paramètres d'intégration avec le module Kaspersky Endpoint Detection and Response (KATA). Pour intégrer Kaspersky Endpoint Detection and Response Expert (on-premise), sélectionnez le mode d'intégration *EDR Expert (OSMP)* dans les paramètres de la tâche (paramètre `Mode=EDRExpertOnPrem`).

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Security communique avec les serveurs de la plate-forme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` : mode d'intégration EDR Expert (OSMP). Permet d'activer l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur d'actions de réponse OSMP. Si la vérification en deux étapes est activée du côté du serveur d'actions de réponse OSMP, vous devez activer la vérification en deux étapes dans les paramètres de la tâche *Intégration à Kaspersky Endpoint Detection and Response Expert (on-premise)* et ajouter un certificat client avant d'exécuter la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur d'actions de réponse aux menaces OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence d'envoi des requêtes de synchronisation au serveur de réponse OSMP (en minutes).	Valeur par défaut : `5`.
`ConnectionTimeout`	Délai d'expiration maximal de la connexion au serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`RequestTimeout`	Délai d'attente maximal d'une réponse du serveur de réponse OSMP (en secondes).	Valeur par défaut : `10`.
`EnableTelemetry`	Activation et désactivation de l'envoi de données sur les événements sur les appareils (télémétrie) au serveur de collecte de télémétrie OSMP.	`Yes` (valeur par défaut) : envoyer la télémétrie au serveur de collecte de télémétrie OSMP. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur d'actions de réponse OSMP. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur d'actions de réponse OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur d'actions de réponse OSMP.	Valeur par défaut : `443`.

Paramètre	Description	Valeur
La section **[TelemetrySettings]** contient les paramètres généraux de connexion aux serveurs de collecte de télémétrie OSMP.		
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage votre connexion au serveur de collecte de télémétrie OSMP. Si la vérification en deux étapes est activée du côté du serveur de collecte de télémétrie OSMP, vous devez activer la vérification en deux étapes dans les paramètres de la tâche *Intégration à Kaspersky Endpoint Detection and Response Expert (on-premise)* et ajouter un certificat client avant d'exécuter la tâche.	`Yes` active l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur de télémétrie OSMP. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur de collecte de télémétrie OSMP en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente d'une réponse du serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `10`.
`OnlyTaggedEvents`	Activer ou désactiver l'envoi des seules données de télémétrie comportant un indicateur d'attaque (Indicator of Attack, IOA). L'*indicateur d'attaque* décrit un comportement suspect d'objets au sein de l'infrastructure informatique d'une organisation, pouvant indiquer une attaque ciblée.	`Yes` : envoyer uniquement les données de télémétrie comportant un indicateur d'attaque (Indicator of Attack, IOA). `No` (valeur par défaut) : envoyer toutes la télémétrie.
La section **[TelemetrySettings.Endpoints.item_#]** contient l'adresse et le port du serveur de collecte de télémétrie OSMP. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur de collecte de télémétrie OSMP. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur de collecte de télémétrie OSMP.	Valeur par défaut : `443`.
La section **[TelemetrySettings.EventTransferSettings]** contient les paramètres de transfert des données vers le serveur de collecte de télémétrie OSMP.		
`MaximumDataTransferTime`	Délai maximal d'envoi des événements au serveur de collecte de télémétrie OSMP (en secondes).	Valeur par défaut : `30`.
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur de collecte de télémétrie OSMP.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Gestion des certificats pour la connexion aux serveurs OSMP

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion aux serveurs OSMP. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer des certificats des serveurs OSMP : serveur d'actions de réponse et serveur de collecte de télémétrie
- afficher des informations sur les certificats de serveurs
- supprimer les certificat des serveurs
- ajouter ou remplacer des certificats client utilisés pour sécuriser les connexions aux serveurs OSMP : serveur de réponse et serveur de collecte de télémétrie
- afficher des informations sur le certificats client
- supprimer les certificats client

Administration des certificats de connexion au serveur d'actions de réponse OSMP

Pour ajouter ou remplacer le certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <fichier> --server-type response
```

où < `fichier` > est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse :

1. Exécutez la commande :

   ```
   kesl-control [-R] --add-kataedr-client-certificate <fichier> --server-type response
   ```

   où < `fichier` > est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur OSMP si la vérification du certificat client est activée dans les paramètres du serveur OSMP et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premise)*, le paramètre `UseClientPinnedCertificate` de la section `[KATAEDR]` est défini sur `yes`.

Pour afficher les informations relatives au certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

Pour afficher les informations relatives au certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer le certificat du serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

Pour supprimer le certificat client utilisé pour sécuriser la connexion au serveur d'actions de réponse, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

Administration des certificats de connexion au serveur de collecte de télémétrie OSMP

Pour ajouter ou modifier un certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <fichier> --server-type telemetry
```

où `<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie :

1. Exécutez la commande :

   ```
   kesl-control [-R] --add-kataedr-client-certificate <fichier> --server-type telemetry
   ```

   où `<fichier>` est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur OSMP si la vérification du certificat client est activée dans les paramètres du serveur OSMP et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premise)*, le paramètre `UseClientPinnedCertificate` de la section `[TelemetrySettings]` est défini sur `yes`.

Pour afficher les informations relatives au certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

Pour afficher des informations sur le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

Pour supprimer le certificat client utilisé pour sécuriser la connexion au serveur de collecte de télémétrie, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Intégration avec Kaspersky Anti Targeted Attack Platform

L'application Kaspersky Endpoint Security est compatible avec la solution Kaspersky Anti Targeted Attack Platform conçu pour protéger l'infrastructure informatique d'une entreprise et assurer la détection rapide des menaces telles que les attaques ZeroDay, les attaques ciblées et les attaques ciblées complexes des menaces persistantes avancées (ci-après également appelées "APT"). Pour en savoir plus sur la solution, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

L'application Kaspersky Endpoint Security peut s'intégrer aux modules suivants de Kaspersky Anti Targeted Attack Platform :

- Kaspersky Endpoint Detection and Response (KATA). Le module assure la protéction des appareils dans le réseau local de l'organisation. Lors de l'integration avec Kaspersky Endpoint Detection and Response (KATA), l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

  - Envoyer les données sur les événements sur les appareils (télémétrie) au serveur avec le module Central Node, qui assure l'interaction avec Kaspersky Endpoint Detection and Response (KATA) (ci-après également appelé *serveur KATA*). L'application Kaspersky Endpoint Security transmet au serveur doté du module Central Node de Kaspersky Anti Targeted Attack Platform des données de surveillance sur les processus, les connexions réseau ouvertes et les fichiers modifiés, ainsi que des données sur les menaces détectées par l'application et des données sur les résultats du traitement de ces menaces.

  - Effectuez les actions de réponse visant à garantir les fonctions de sécurité sur la base des commandes reçues de Kaspersky Anti Targeted Attack Platform.

  L'intégration avec Kaspersky Endpoint Detection and Response (KATA) versions 7.1 et antérieures est prise en charge.

- Kaspersky Network Detection and Response (KATA). Le module assure la protection du réseau interne de l'organisation. Lorsqu'elle est intégrée à Kaspersky Network Detection and Response (KATA), l'application Kaspersky Endpoint Security peut envoyer des données sur les événements sur les appareils (télémétrie) à un serveur avec le module Central Node qui assure l'interaction avec Kaspersky Network Detection and Response (KATA) (ci-après également appelé *serveur NDR*).

- Sandbox. La technologie Sandbox permet l'analyse et l'exploration des objets sur des serveurs dédiés, dotés d'images virtuelles de systèmes d'exploitation, afin de détecter les activités malveillantes et les signes d'attaques ciblées sur l'infrastructure informatique de l'organisation. Lors de l'intégration de Kaspersky Endpoint Security avec Sandbox sur la Kaspersky Anti Targeted Attack Platform, l'application envoie les fichiers à analyser à un serveur équipé du module Central Node, qui facilite l'interaction avec Sandbox.

L'intégration avec les modules sur Kaspersky Anti Targeted Attack Platform est assurée par les modules suivants de l'application Kaspersky Endpoint Security :

- Module Endpoint Detection and Response Expert (on-premise) (ci-après également appelé *EDR Expert (on-premise)*).

  À partir de Kaspersky Endpoint Security for Linux 12.4, le module Endpoint Detection and Response (KATA) a été renommé Endpoint Detection and Response Expert (on-premise). Ce module assure désormais l'intégration non seulement avec Kaspersky Endpoint Detection and Response (KATA), un module de Kaspersky Anti Targeted Attack Platform, mais aussi avec Kaspersky Endpoint Detection and Response Expert (on-premise).

- module Network Detection and Response (KATA) (ci-après également *NDR (KATA)*) ;

- Module *Sandbox*.

Vous pouvez configurer l'intégration de l'application Kaspersky Endpoint Security avec tous les modules de la solution Kaspersky Anti Targeted Attack Platform ou avec chaque module séparément.

Lors de l'intégration avec la solution Kaspersky Anti Targeted Attack Platform, les appareils exécutant Kaspersky Endpoint Security établissent des connexions chiffrées HTTPS avec les serveurs hébergeant le module Central Node qui facilite l'intégration. Les certificats suivants émis par les serveurs Central Node sont utilisés pour sécuriser la connexion :

- Certificat du serveur. La connexion est chiffrée à l'aide du certificat TLS du serveur. Vous pouvez augmenter le niveau de sécurité de la connexion en activant la vérification du certificat du serveur du côté de Kaspersky Endpoint Security. Pour ce faire, vous devez ajouter le certificat du serveur avant d'activer l'intégration avec la solution Kaspersky Anti Targeted Attack Platform.

- Certificat client. Ce certificat est utilisé pour sécuriser davantage la connexion avec une vérification en deux étapes (c'est-à-dire, l'analyse des appareils avec l'application Kaspersky Endpoint Security par les serveurs Central Node). Le même certificat client peut être utilisé par plusieurs appareils. Par défaut, le serveur n'effectue pas la validation du certificat client, mais l'authentification bidirectionnelle peut être activée du côté de Kaspersky Anti Targeted Attack Platform. Dans ce cas, vous devez activer l'authentification bidirectionnelle dans les paramètres du module EDR Expert (on-premises), NDR (KATA) ou Sandbox et ajouter un certificat client (cryptocontainer avec certificat et clé privée).

Les certificats permettant de sécuriser les connexions aux serveurs compatibles avec les modules de Kaspersky Anti Targeted Attack Platform sont fournis par l'administrateur de cette plateforme.

Si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application de Kaspersky Endpoint Security, il sera utilisé pour se connecter à ces serveurs.

Pour utiliser la fonctionnalité de Kaspersky Endpoint Detection and Response (KATA), vous devez activer le module EDR Expert (on-premise). Si la licence principale sous laquelle vous utilisez l'application Kaspersky Endpoint Security n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise), vous devez acheter une licence distincte pour cette fonctionnalité et ajouter la clé de licence EDR Expert (on-premise) à l'application.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant des clés de licence à la SVM.

L'intégration avec les modules Kaspersky Endpoint Detection and Response (KATA) et Kaspersky Network Detection and Response (NDR) se déroule comme suit :

1. **Activation des modules requis de Kaspersky Endpoint Security**

   Les modules EEDR Expert (on-premise) et NDR (KATA) peuvent utiliser les données obtenues à partir des modules suivants :

   - Protection contre les fichiers malicieux.
   - Protection contre les menaces réseau.
   - Protection contre les menaces Internet.
   - Protection contre le chiffrement.
   - Contrôle des applications.
   - Contrôle des appareils.
   - Contrôle de l'intégrité du système.

Pour intégrer complètement l'application Kaspersky Endpoint Security à Kaspersky Anti Targeted Attack Platform, vous devez activer le module Détection comportementale. Si la Détection comportementale est désactivée, aucune donnée de télémétrie requise n'est transmise (à l'exception des demandes de synchronisation et des données de détection des menaces provenant d'autres modules de protection).

Lorsque vous utilisez le mécanisme eBPF pour obtenir la télémétrie du système dans le module Détection comportementale (disponible sur les systèmes d'exploitation 64 bits avec la version de noyau 4.18 et supérieure avec prise en charge eBPF), les données de télémétrie seront plus complètes.

2. **Activation du module EDR Expert (on-premise)**

Pour intégrer Kaspersky Endpoint Detection and Response (KATA), vous devez activer le module EDR Expert (on-premise). Assurez-vous que l'une des conditions suivantes est remplie :

- Vous utilisez l'application Kaspersky Endpoint Security sous une licence qui inclut la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise).
- Vous avez acheté une licence distincte pour utiliser la fonctionnalité Kaspersky Endpoint Detection and Response Expert (on-premise) et ajouté à l'application une clé de licence EDR Expert (on-premise).

  Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, une clé de licence pour activer des fonctionnalités supplémentaires est ajoutée à la SVM.

L'activation du module NDR (KATA) n'est pas requise ; les licences de base de Kaspersky Endpoint Security incluent l'intégration avec Kaspersky Network Detection and Response (KATA).

3. **Activation du module EDR Expert (on-premise)**

Par défaut, l'intégration avec Kaspersky Endpoint Detection and Response (KATA) est désactivée. Pour activer l'intégration, vous devez activer le module EDR Expert (on-premise) et configurer ses paramètres.

- à l'aide de Kaspersky Security Center Web Console ;
- À l'aide de la Console d'administration de Kaspersky Security Center.
- À l'aide de la ligne de commande.

Si vous utilisez Web Console ou la ligne de commande pour intégrer Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration *EDR (KATA)* dans les paramètres du module Kaspersky Endpoint Detection and Response Expert (on-premise). Si vous utilisez Web Console, sélectionnez **Endpoint Detection and Response Expert (version 7.1 et antérieures)** dans les paramètres de la stratégie. Si vous utilisez la ligne de commande, définissez le paramètre `Mode=EDRKATA` dans les paramètres de tâche. Pour configurer l'intégration avec Kaspersky Endpoint Detection and Response (KATA) sur un appareil, dans Web Console, vous devez gérer les « cadenas » pour l'une ou l'autre version (version 8.0 et ultérieure et version 7.1 et antérieure).

Pour utiliser la fonctionnalité de la prévention du lancement des objets, vous pouvez activer l'application des règles de la prévention du lancement des objets du module EDR Expert (on-premise).

4. **Activation du module NDR (KATA)**

Par défaut, l'intégration avec Kaspersky Network Detection and Response (KATA) est désactivée. Pour activer l'intégration, vous devez activer le module NDR (KATA) et configurer ses paramètres.

- à l'aide de Kaspersky Security Center Web Console ;
- À l'aide de la Console d'administration de Kaspersky Security Center.
- À l'aide de la ligne de commande.

Vous pouvez vérifier l'état de fonctionnement des modules EDR Expert (on-premise) et NDR (KATA) :

- Utilisation du *Rapport sur l'état des modules de l'application* dans Web Console.

  Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.

- Dans les propriétés de l'appareil dans Web Console (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → **Général** → **Modules**).

- À l'aide de la ligne de commande, en exécutant la commande `kesl-control --app-info`.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans Web Console

Dans Web Console, vous pouvez gérer les paramètres d'intégration de Kaspersky Endpoint Detection and Response (KATA) dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premise)**).

Pour intégrer Kaspersky Endpoint Detection and Response (KATA), vous devez activer le module EDR Expert (on-premise) et sélectionner l'option **Endpoint Detection and Response Expert (version 7.1 et antérieures)**, c'est-à-dire le mode d'intégration *EDR (KATA)*.

Pour appliquer la valeur du paramètre **Délai maximal lors de l'envoi des événements (s)** spécifiée sous **Paramètres de transfert de données** pour le module Endpoint Detection and Response Expert (KATA) dans la stratégie de Web Console, vous devez fermer les « cadenas » des groupes de paramètres **Paramètres de transfert de données** et **Limitation des requêtes** dans les propriétés de la stratégie. Pour autoriser la modification locale du paramètre `MaximumDataTransferTime` sur l'appareil, dans la section `[EventTransferSettings]` de la tâche KATAEDR en mode EDR (KATA), vous devez déverrouiller les « cadenas » des groupes de paramètres **Paramètres de transfert de données** et **Limitation des requêtes** dans les propriétés de la stratégie.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver le module EDR Expert (on-premises) et gérer les paramètres de l'intégration de Kaspersky Endpoint Security avec le module Kaspersky Endpoint Detection and Response (KATA) dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Detection and Response → EDR Expert (on-premises)**).

Si l'option **Endpoint Detection and Response Expert (version 8.0 ou supérieure)** est sélectionnée pour le module Endpoint Detection and Response Expert (on-premise) dans Web Console, c'est-à-dire le mode d'intégration EDR Expert (OSMP), un avertissement s'affiche dans la Console d'administration : les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) sont indisponibles. Vous pouvez modifier le mode d'intégration dans Web Console.

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description
Activer Endpoint Detection and Response Expert (on-premise)	La case active ou désactive le module EDR Expert (on-premise), qui assure l'intégration avec Kaspersky Endpoint Detection and Response (KATA). Le module est désactivé par défaut.
Activer la prévention du lancement des objets	La case active ou désactive l'application de règles de prévention du lancement des objets du module EDR Expert (on-premise).
Serveurs KATA	Cliquer sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer la connexion aux serveurs KATA, ainsi qu'afficher la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion au serveur	Cliquez sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs KATA, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs KATA.
Paramètres de transfert des données	Le bouton **Configurer** ouvre une fenêtre dans laquelle vous pouvez configurer les paramètres de transfert des données aux serveurs KATA.

Configuration de connexion aux serveurs KATA

Le tableau affiche une liste des paramètres de connexion aux serveurs KATA. Pour chaque serveur auquel une connexion est configurée, le tableau indique l'adresse IP du serveur (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) et le port.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur KATA.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Paramètres de connexion au serveur

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur KATA, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur. Valeur par défaut : `127.0.0.1`.
Port	Port de connexion au serveur KATA. Valeur par défaut : `443`.

+-/Configuration des paramètres généraux de connexion aux serveurs KATA

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs KATA.

Paramètres de connexion au serveur KATA

Paramètre	Description
Envoyer une demande de synchronisation au serveur KATA toutes les (minutes)	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur KATA, en minutes. Valeur par défaut : `5`.
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur KATA en secondes. Valeur par défaut : `10`.
Durée d'attente maximale de la réponse du serveur (en secondes)	Durée maximale d'attente de la réponse du serveur KATA en secondes. Valeur par défaut : `10`.
Autoriser l'envoi de télémétrie	Active ou désactive l'envoi de données d'événement sur les appareils (télémétrie) au serveur KATA. La télémétrie est activée par défaut.

Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur :
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
	Dans la fenêtre d'ajout un certificat, vous pouvez ajouter un certificat du serveur KATA de l'une des manières suivantes :
	  • Dans le champ **Ajouter à partir d'un fichier**, spécifiez le chemin d'accès au fichier de certificat contenant le certificat au format DER ou PEM. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier.
	  • Copier le contenu du fichier de certificat dans le champ **Saisir les données du certificat**.
	Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.
	• **Supprimer** : supprime un certificat du serveur ajouté précédemment. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.

Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes : • **Utiliser la vérification en deux étapes** : active ou désactive l'utilisation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur KATA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client. L'authentification bidirectionnelle doit être activée du côté du serveur KATA. • **Ajouter** : ouvre la fenêtre d'ajout de certificat client pour sécuriser davantage la connexion au serveur KATA. Le bouton apparaît si la case **Utiliser la vérification en deux étapes** est cochée et que le certificat client n'a pas encore été ajouté. Pour ajouter un certificat client, dans la fenêtre d'ajout d'un certificat, indiquez le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Si l'archive est protégée par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe de conteneur de chiffrement**. • **Supprimer** : supprime le certificat client précédemment ajouté. Le bouton s'affiche uniquement si le certificat client a été ajouté.

Configuration des paramètres du transfert des données aux serveurs KATA

Cette fenêtre permet de configurer les paramètres de connexion au serveur KATA.

Paramètres de transfert des données aux serveurs KATA

Paramètre	Description
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur KATA. Valeur par défaut : `30`.
Activer la régulation du nombre d'événements	Active ou désactive la limitation du nombre d'événements envoyés au serveur KATA.
Nombre maximum d'événements par heure.	Nombre maximum d'événements par heure. Valeur par défaut : `3000`.
Pourcentage d'événements dépassant la limite	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type (par exemple, les événements de changement de registre) et le nombre total d'événements dépasse la limite définie en pourcentage. Valeur par défaut : `15`.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans la ligne de commande

Dans la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Endpoint Detection and Response (KATA) à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)*.

Cette tâche vous permet également de configurer les paramètres d'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises). Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration *EDR (KATA)* dans les paramètres de la tâche et gérer les paramètres d'intégration si nécessaire.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) en modifiant les paramètres d'une tâche prédéfinie.

Par défaut, la tâche *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises)* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez gérer les certificats utilisés pour se connecter aux serveurs KATA à l'aide des commandes d'administration des modules EDR Expert (on-premises).

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Le tableau ci-dessous décrit les paramètres de la tâche préinstallée *Intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) (KATAEDR)* que vous pouvez configurer lors de l'intégration avec Kaspersky Endpoint Detection and Response (KATA).

Cette tâche vous permet également de configurer les paramètres d'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises). Pour intégrer le module Kaspersky Endpoint Detection and Response (KATA), vous devez sélectionner le mode d'intégration *EDR (KATA)* (paramètre `Mode=EDRKATA`) dans les paramètres de la tâche.

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description	Valeur
`Mode`	Mode d'intégration. Pour l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Security communique avec les serveurs de la plate-forme OSMP. Pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security communique avec les serveurs de Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (valeur par défaut) : mode d'intégration EDR (KATA). Permet d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA), avec le module Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` : mode d'intégration EDR Expert (OSMP). Permet d'activer l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premises).
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. Si la vérification en deux étapes est activée du côté du serveur KATA, vous devez activer la vérification en deux étapes dans les paramètres de la tâche *Intégration à Kaspersky Endpoint Detection and Response Expert (on-premises)* et ajouter un certificat client avant d'exécuter la tâche.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KATA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur KATA, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KATA en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur KATA en secondes.	Valeur par défaut : `10`.
`EnableTelemetry`	Activation et désactivation de l'envoi de données sur les événements sur les appareils (télémétrie) à KATA.	`Yes` (valeur par défaut) : envoie la télémétrie au serveur KATA. `No` désactive l'envoi de la télémétrie.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur KATA. Vous pouvez ajouter plusieurs serveurs.		
`Address`	Adresse du serveur KATA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolement réseau de l'appareil est activé, il est recommandé de spécifier l'adresse IP du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur KATA.	Valeur par défaut : `443`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des données vers le serveur KATA.		

Paramètre	Description	Valeur
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur KATA.	Valeur par défaut : `30`.
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur KATA.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`EventLimitExceededPercentage`	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.

Gestion des certificats pour la connexion au serveur KATA

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur KATA. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur KATA ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur KATA ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --add-kataedr-server-certificate <fichier>
```

où `<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande :

```
kesl-control [-R] --add-kataedr-client-certificate <fichier>
```

où < `fichier` > est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur KATA si la vérification du certificat client est activée dans les paramètres du serveur KATA et si, dans les paramètres de la tâche *Intégration de Kaspersky Endpoint Detection and Response Expert (on-premises)*, le paramètre `UseClientPinnedCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat de serveur, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-server-certificate
```

Pour afficher les informations relatives au certificat client, exécutez la commande suivante :

```
kesl-control [-R] --query-kataedr-client-certificate
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres d'intégration avec Kaspersky Network Detection and Response (KATA) dans les propriétés de la stratégie (**Paramètres de l'application → Configuration des agents intégrés → Network Detection and Response (KATA)**).

Pour appliquer la valeur du paramètre **Délai maximal lors de l'envoi des événements (s)** indiquée sous **Paramètres de transfert de données** pour le module Network Detection and Response (KATA) dans la stratégie de la Web Console, vous devez fermer les « cadenas » pour les groupes de paramètres **Paramètres de transfert de données** et **Limitation des requêtes** dans les propriétés de la stratégie. Pour autoriser la modification locale du paramètre `MaximumDataTransferTime` sur l'appareil, dans la section `[EventTransferSettings]` de la tâche KATANDR, vous devez déverrouiller les « cadenas » pour les groupes de paramètres **Paramètres de transfert de données** et **Limitation des requêtes** dans les propriétés de la stratégie.

Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver le module NDR (KATA) et gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Network Detection and Response (KATA) dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Detection and Response → Network Detection and Response (KATA)**).

Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)

Paramètre	Description
Activer Network Detection and Response (KATA)	La case active ou désactive le module NDR (KATA). Le module est désactivé par défaut.
Serveurs NDR	Cliquer sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer la connexion aux serveurs NDR, ainsi qu'afficher la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion au serveur	Cliquez sur le bouton **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs NDR, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs NDR.
Paramètres de transfert des données	Le bouton **Configurer** ouvre une fenêtre dans laquelle vous pouvez configurer les paramètres de transfert des données aux serveurs NDR.

Configuration de connexion aux serveurs NDR

Le tableau affiche une liste des paramètres de connexion aux serveurs NDR. Pour chaque serveur auquel une connexion est configurée, le tableau indique l'adresse IP du serveur (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) et le port.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur NDR.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Paramètres de connexion au serveur

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur NDR, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Valeur par défaut : `127.0.0.1`.
Port	Port de connexion au serveur NDR. Valeur par défaut : `443`.

+-/Configuration des paramètres généraux de connexion aux serveurs NDR

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs NDR.

Paramètres de connexion au serveur NDR

Paramètre	Description
Envoyer une demande de synchronisation au serveur NDR toutes les (minutes)	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en minutes. Valeur par défaut : `5`.
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur NDR en secondes. Valeur par défaut : `10`.
Durée d'attente maximale de la réponse du serveur (en secondes)	Durée maximale d'attente de la réponse du serveur NDR en secondes. Valeur par défaut : `10`.

Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur :
	• **Ajouter** : ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
	Dans la fenêtre d'ajout d'un certificat, vous pouvez ajouter un certificat du serveur NDR de l'une des manières suivantes :
	  • Dans le champ **Ajouter à partir d'un fichier**, spécifiez le chemin d'accès au fichier de certificat contenant le certificat au format DER ou PEM. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier.
	  • Copier le contenu du fichier de certificat dans le champ **Saisir les données du certificat**.
	Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.
	• **Supprimer** : supprime un certificat du serveur ajouté précédemment. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.

Paramètre	Description
Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes : • **Utiliser la vérification en deux étapes** : active ou désactive l'utilisation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur NDR. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client. L'authentification bidirectionnelle doit être activée du côté du serveur NDR. • **Ajouter** : ouvre la fenêtre d'ajout de certificat client pour sécuriser davantage la connexion au serveur NDR. Le bouton apparaît si la case **Utiliser la vérification en deux étapes** est cochée et que le certificat client n'a pas encore été ajouté. Pour ajouter un certificat client, dans la fenêtre d'ajout d'un certificat, indiquez le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Si l'archive est protégée par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe de conteneur de chiffrement**. • **Supprimer** : supprime le certificat client précédemment ajouté. Le bouton s'affiche uniquement si le certificat client a été ajouté.

Configuration des paramètres du transfert des données aux serveurs NDR

Cette fenêtre permet de configurer les paramètres de connexion au serveur NDR.

Paramètres de transfert des données aux serveurs NDR

Paramètre	Description
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur NDR. Valeur par défaut : `30`.
Nombre maximum d'événements dans un paquet	Nombre maximum d'événements dans un paquet. Valeur par défaut : `1024`.
Fréquence d'interrogation des serveurs	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en secondes. Valeur par défaut : `450`.
Activer la régulation du nombre d'événements	Active ou désactive la limitation du nombre d'événements envoyés au serveur NDR.
Nombre maximum d'événements par heure.	Nombre maximum d'événements par heure. Valeur par défaut : `3000`.
Pourcentage d'événements dépassant la limite	Pourcentage d'événements dépassant la limite. La transmission d'événements est limitée si le rapport entre les événements du même type (par exemple, les événements de changement de registre) et le nombre total d'événements dépasse la limite définie en pourcentage. Valeur par défaut : `15`.

Configuration de l'intégration avec Kaspersky Network Detection and Response (KATA) dans la ligne de commande

Dans la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec le module Kaspersky Network Detection and Response (KATA) à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Network Detection and Response (KATA) (KATANDR)* :

Par défaut, la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter la tâche manuellement.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Network Detection and Response (KATA) en modifiant les paramètres d'une tâche prédéfinie.

Vous pouvez gérer les certificats utilisés pour se connecter aux serveurs NDR à l'aide des commandes d'administration des modules NDR (KATA).

Paramètres d'intégration avec Kaspersky Network Detection and Response (KATA)

Le tableau ci-dessous décrit tous les paramètres disponibles et les valeurs par défaut de tous les paramètres que vous pouvez spécifier pour la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)*.

Paramètres de la tâche Intégration à Kaspersky Network Detection and Response (KATA)

Paramètre	Description	Valeur
`UseClientPinnedCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. Si l'analyse du certificat client est activée du côté serveur NDR, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)*.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur NDR. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`SynchronizationPeriod`	Fréquence à laquelle les demandes de synchronisation sont envoyées au serveur NDR, en minutes.	Valeur par défaut : `5`.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur NDR en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur NDR en secondes.	Valeur par défaut : `10`.
La section **[Endpoints.item_#]** contient l'adresse et le port du serveur NDR.		
`Address`	Adresse du serveur NDR. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur NDR.	Valeur par défaut : `8081`.
La section **[EventTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur NDR.		
`MaximumDataTransferTime`	Délai maximum en secondes pour l'envoi des événements au serveur NDR.	Valeur par défaut : `30`.
`MaximumNumberOfEventsInPackage`	Nombre maximum d'événements dans un paquet.	Valeur par défaut : `1024`.
`UseRequestCountLimits`	Activation et désactivation de la régulation du nombre d'événements envoyés au serveur NDR.	`Yes` (valeur par défaut) : permet de régler le nombre d'événements à envoyer. `No` - ne pas régler le nombre d'événements.
`MaximumNumberOfEventsInHour`	Nombre maximum d'événements par heure.	Valeur par défaut : `3000`.
`EventLimitExceededPercentage`	Pourcentage de dépassement de la limite d'événements. La transmission d'événements est limitée si le rapport entre les événements du même type et le nombre total d'événements dépasse la limite définie en pourcentage.	Valeur par défaut : `15`.
`PingPeriod`	Fréquence d'interrogation des serveurs NDR en secondes.	Valeur par défaut : `450`.

Gestion des certificats pour la connexion au serveur NDR

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur NDR. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur NDR ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer le certificat client utilisé pour sécuriser la connexion au serveur NDR ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --add-katandr-server-certificate <fichier>
```

où < `fichier` > est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande :

   ```
   kesl-control [-R] --add-katandr-client-certificate <fichier>
   ```

   où < `fichier` > est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur NDR si la vérification du certificat client est activée dans les paramètres du serveur NDR et que, dans les paramètres de la tâche *Intégration avec Kaspersky Network Detection and Response (KATA)*, le paramètre `UseClientPinnedCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat de serveur, exécutez la commande suivante :

```
kesl-control [-R] --query-katandr-server-certificate
```

Pour afficher les informations relatives au certificat client, exécutez la commande suivante :

```
kesl-control [-R] --query-katandr-client-certificate
```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-R] --remove-katandr-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-R] --remove-katandr-client-certificate
```

Intégration avec Sandbox

La technologie Sandbox permet l'analyse et l'exploration des objets sur des serveurs dédiés, dotés d'images virtuelles de systèmes d'exploitation, afin de détecter les activités malveillantes et les signes d'attaques ciblées sur l'infrastructure informatique de l'organisation.

Kaspersky Endpoint Security peut interagir avec Sandbox sur Open Single Management Platform (OSMP) ou sur Kaspersky Anti Targeted Attack Platform. Selon la plateforme, Kaspersky Endpoint Security communique avec Sandbox via le *serveur Sandbox* : soit le serveur OSMP, soit un serveur doté du module Central Node.

L'intégration avec Sandbox est assurée par le module *Sandbox* de l'application Kaspersky Endpoint Security.

Lors de l'intégration avec Sandbox, les appareils exécutant Kaspersky Endpoint Security établissent des connexions chiffrées via HTTPS avec les Serveurs d'intégration. Pour garantir la sécurité de la connexion, les certificats suivants, émis par le serveur OSMP ou le serveur Central Node, sont utilisés :

- Certificat du serveur. La connexion est chiffrée à l'aide du certificat TLS du serveur. Vous pouvez augmenter le niveau de sécurité de la connexion en activant la vérification du certificat du serveur du côté de Kaspersky Endpoint Security. Pour ce faire, vous devez ajouter le certificat du serveur avant d'activer l'intégration Sandbox.
- Certificat client. Ce certificat est utilisé pour sécuriser davantage la connexion avec une vérification en deux étapes (c'est-à-dire, l'analyse des appareils avec l'application Kaspersky Endpoint Security par le serveur OSMP ou le serveur Central Node). Le même certificat client peut être utilisé par plusieurs appareils. Par défaut, le serveur n'effectue pas la validation du certificat client, mais l'authentification bidirectionnelle peut être activée du côté de la plate-forme OSMP ou Kaspersky Anti Targeted Attack Platform. Dans ce cas, vous devez activer l'authentification bidirectionnelle dans les paramètres du module Sandbox et ajouter un certificat client (cryptocontainer avec certificat et clé privée).

Les certificats permettant de sécuriser les connexions aux serveurs autorisant l'interaction avec Sandbox sont fournis par l'administrateur de OSMP ou Kaspersky Anti Targeted Attack Platform.

Si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application Kaspersky Endpoint Security, le serveur proxy est utilisé pour se connecter aux serveurs qui assurent l'interaction avec Sandbox.

La soumission des fichiers et des répertoires pour analyse à Sandbox peut se faire selon l'un des modes suivants :

- *Manuellement*. Dans ce mode, vous pouvez soumettre des objets à Sandbox pour analyse manuellement à l'aide d'une commande ou depuis l'interface graphique.
- *Automatique uniquement*. L'application soumet automatiquement les objets pour analyse, mais il n'est pas possible de soumettre manuellement les objets pour analyse à Sandbox.
- *Automatique et manuel*. L'application soumet automatiquement les objets pour analyse, mais vous pouvez également les soumettre manuellement à Sandbox à l'aide d'une commande ou via l'interface graphique.

Par défaut, l'intégration avec Sandbox est désactivée. Vous pouvez activer ou désactiver le module Sandbox et configurer les paramètres d'intégration suivants à l'aide de Web Console et de la ligne de commande :

- Sélectionner le mode de soumission des objets pour analyse (manuel, automatique uniquement, automatique et manuel).
- Sélectionnez les actions que l'application effectuera en cas de détection d'une menace (en mode d'envoi asynchrone d'objets à Sandbox) :
  - Supprimer le fichier contenant l'objet détecté et mettre en quarantaine une copie de ce fichier.
  - Lancer la tâche d'analyse des zones critiques. Par défaut, l'application analyse la mémoire du processus, la mémoire du noyau, les secteurs de démarrage, les objets de démarrage et le chemin d'accès à l'objet détecté.
  - Créer une tâche d'analyse IOC. L'application crée automatiquement une tâche d'analyse IOC. Vous pouvez configurer le mode de lancement de la tâche, la zone de recherche et l'action effectuée en cas de détection d'un IOC (suppression de l'objet détecté, exécution d'une tâche d'analyse des zones critiques).
- Configurer les paramètres généraux de connexion aux serveurs Sandbox.
- Ajouter et supprimer des certificats de serveur Sandbox.
- Configurer la vérification en deux étapes lors de la connexion aux serveurs Sandbox et ajoutez des certificats clients.

Configuration de l'intégration avec Sandbox dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'intégration de l'application avec Sandbox dans les propriétés de la stratégie (**Paramètres de l'application → Configuration des agents intégrés → Sandbox**).

Configuration de l'intégration avec Sandbox dans ligne de commande

Depuis la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec Sandbox à l'aide de la tâche prédéfinie *Intégration avec KATA*.

Par défaut, la tâche *Intégration avec Sandbox* n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

L'exécution de la tâche *Intégration avec Sandbox* est impossible si le certificat du serveur n'est pas ajouté.

Si la tâche *Intégration avec Sandbox* est en cours d'exécution, vous pouvez envoyer des fichiers à Sandbox pour analyse dans la ligne de commande.

Pour envoyer des fichiers à Sandbox pour analyse, exécutez la commande suivante :

```
kesl-control [-X] --sandbox <chemin>
```

où `<chemin>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

Vous pouvez configurer les paramètres d'intégration avec Sandbox en modifiant les paramètres d'une tâche prédéfinie.

À l'aide des commandes de gestion des paramètres d'intégration avec Sandbox, vous pouvez gérer les certificats utilisés pour se connecter aux serveurs qui assurent l'interaction avec Sandbox.

Paramètres d'intégration avec Sandbox

Le tableau ci-dessous décrit tous les paramètres disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez spécifier pour la tâche *Intégration avec Sandbox*.

Paramètres de la tâche Intégration avec Sandbox

Paramètre	Description	Valeur
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. Si la vérification du certificat client est activée du côté serveur Sandbox, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche *Intégration avec Sandbox*.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur Sandbox. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur en secondes.	Valeur par défaut : `10`.
`RequestTimeout`	Durée maximale d'attente de la réponse du serveur en secondes.	Valeur par défaut : `10`.
`SendingMode`	Mode d'envoi du fichier pour analyse à Sandbox.	`AutoOnly` (valeur par défaut) : envoi automatiquement des fichiers pour analyse dès qu'ils sont consultés. `Manual` : envoi manuel des fichiers pour analyse. `AutoAndManual` : envoi des fichiers à analyser, que ce soit automatique ou manuel.
`QuarantineFile`	Place un fichier en quarantaine lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : en cas de menace détectée, supprimer le fichier original et mettre la copie en quarantaine. `No` : ne pas placer le fichier en quarantaine en cas de menace détectée.

Paramètre	Description	Valeur
`ScanCriticalAreas`	Exécution de l'analyse des zones critiques en cas de menace détectée.	`Yes` (valeur par défaut) : lorsqu'une menace est détectée, effectuer une analyse des zones critiques. `No` : ne pas lancer d'analyse des zones critiques lorsqu'une menace est détectée.
`CreateIocScanTask`	Créer une tâche d'analyse IOC lorsqu'une menace est détectée.	`Yes` (valeur par défaut) : créer une tâche d'analyse IOC lorsqu'une menace est détectée. `No` : ne pas créer de tâche d'analyse IOC lorsqu'une menace est détectée.
`QuarantineFileOnIocDetected`	Mise en quarantaine d'un objet lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, supprimer l'objet original et mettre en quarantaine la copie de l'objet. `No` : ne pas mettre l'objet en quarantaine lorsqu'un indicateur de compromission est détecté.
`ScanCriticalAreasOnIocDetected`	Exécution de l'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.	`Yes` (valeur par défaut) : lorsqu'un indicateur de compromission est détecté, exécuter une analyse des zones critiques. `No` : ne pas exécuter d'analyse des zones critiques lorsqu'un indicateur de compromission est détecté.
`Drives`	Domaines de recherche d'indicateurs de compromission.	`Critical` (valeur par défaut) : vérifier les fichiers dans les répertoires utilisateur et système. `System` : analyser tous les fichiers du système de fichiers racine.
`ScheduleMode`	Mode de lancement de la tâche d'analyse IOC.	`Manually` (valeur par défaut) : exécuter manuellement la tâche d'analyse IOC. `AfterTreatDetected` : exécuter la tâche d'analyse IOC après la détection d'une menace.
La section **[Servers.item_#]** contient les paramètres du serveur Sandbox.		
`Address`	Adresse du serveur. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur.	Valeur par défaut : `127.0.0.1`.
`Port`	Port de connexion au serveur.	Valeur par défaut : `443`.
La section **[SandboxTransferSettings]** contient les paramètres de transfert des fichiers à analyser dans Sandbox.		
`SandboxQueue`	Taille maximale du répertoire de stockage de la file d'attente des demandes d'analyse en mégaoctets.	Valeur par défaut : `1024`.

Gestion des certificats pour la connexion au serveur Sandbox

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez gérer, à l'aide de commandes, les certificats utilisés pour les connexions aux serveurs OSMP ou aux serveurs Central Node responsables de l'interaction avec Sandbox (ci-après également appelés serveurs Sandbox). Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;

- ajouter ou remplacer un certificat client ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-X] --add-sandbox-server-certificate <fichier>
```

où `<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande :

   ```
   kesl-control [-X] --add-sandbox-client-certificate <fichier>
   ```

   où `<fichier>` est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour renforcer la protection de la connexion au serveur Sandbox si la vérification du certificat client est activée dans les paramètres du serveur Sandbox et si, dans les paramètres de la tâche *Intégration avec Sandbox*, `UseClientCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat, exécutez la commande suivante :

- pour le certificat du serveur :

  ```
  kesl-control [-X] --query-sandbox-server-certificate
  ```

- pour le certificat client :

  ```
  kesl-control [-X] --query-sandbox-client-certificate
  ```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Intégration avec Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum est une solution conçue pour protéger l'infrastructure informatique d'une organisation contre les menaces telles que les exploits, les ransomwares, les attaques sans fichier et l'utilisation de fichiers système légitimes par des outils malveillants pour endommager les appareils ou les données.

Kaspersky Endpoint Detection and Response Optimum surveille et analyse l'évolution de la menace et fournit également au responsable de la sécurité ou à l'administrateur les informations sur une attaque potentielle nécessaires pour prendre des mesures de réponse en temps opportun.

Kaspersky Endpoint Detection and Response Optimum utilise les outils d'analyse des menaces suivants (Threat Intelligence) :

- L'infrastructure de services cloud Kaspersky Security Network (ci-après également KSN), donnant accès à la base de connaissances opérationnelles de Kaspersky sur la réputation des fichiers, des sites et des logiciels.
- Intégration avec le portail Kaspersky Threat Intelligence Portal, qui contient et affiche des informations sur la réputation des fichiers et des sites.
- Base de données des menaces de Kaspersky Threats.

L'application Kaspersky Endpoint Security 12.4 for Linux est compatible avec Kaspersky Endpoint Detection and Response Optimum version 3.1.

En interagissant avec Kaspersky Endpoint Detection and Response Optimum, l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

- Envoyer les données d'événements sur les appareils vers Kaspersky Security Center. Kaspersky Endpoint Security envoie à Kaspersky Security Center des données de surveillance sur les processus, les connexions réseau ouvertes et les fichiers modifiés, ainsi que des données sur les menaces détectées par l'application et des données sur les résultats du traitement de ces menaces.
- Effectuer les actions de réponse visant à garantir les fonctions de sécurité sur la base des commandes reçues de Kaspersky Security Center.

L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response Optimum (ci-après, *EDR Optimum*).

Pour utiliser la fonctionnalité de Kaspersky Endpoint Detection and Response Optimum, vous devez activer le module EDR Optimum. Si la licence principale sous laquelle vous utilisez l'application Kaspersky Endpoint Security n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, vous devez acheter une licence distincte pour cette fonctionnalité et ajouter la clé de licence EDR Optimum à l'application.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant des clés de licence à la SVM.

L'intégration avec Kaspersky Endpoint Detection and Response Optimum comprend les étapes suivantes :

1. **Activation des modules requis de Kaspersky Endpoint Security**

   Assurez-vous que les modules suivants de l'application Kaspersky Endpoint Security sont activés et fonctionnent :

   - Protection contre les fichiers malicieux.
   - Protection contre les menaces Internet.
   - Détection comportementale.

   Vous pouvez également activer la prévention du lancement des objets.

2. **Activer la moyens d'analyse des menaces**

   Assurez-vous que Kaspersky Security Network est activé en mode standard ou avancé.

   Pour un fonctionnement plus efficace de Kaspersky Endpoint Detection and Response Optimum, il est recommandé d'utiliser Kaspersky Security Network en mode avancé.

3. **Activation du module EDR Optimum**

   Assurez-vous que l'une des conditions suivantes est remplie :

   - Vous utilisez l'application Kaspersky Endpoint Security sous une licence qui inclut la fonctionnalité Kaspersky Endpoint Detection and Response Optimum.
   - Vous avez acheté une licence distincte pour utiliser la fonctionnalité Kaspersky Endpoint Detection and Response Optimum et ajouté à l'application une clé de licence EDR Optimum.

     Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, une clé de licence pour activer des fonctionnalités supplémentaires est ajoutée à la SVM.

4. **Installation du plug-in d'administration de Kaspersky Endpoint Detection and Response Optimum**

   Le plug-in d'administration de Kaspersky Endpoint Detection and Response Optimum est un plug-in unique permettant de travailler avec des agents sous Windows, Mac et Linux et est requis pour afficher et visualiser les détails des alertes.

5. **Activation du module EDR Optimum**

Par défaut, EDR Optimum est désactivé. Vous pouvez activer et désactiver le module et configurer les paramètres d'intégration :

- à l'aide de Web Console ;
- À l'aide de la ligne de commande.

> La gestion du module EDR Optimum à l'aide de la Console d'administration de Kaspersky Security Center n'est pas prise en charge.

Vous pouvez vérifier l'état de fonctionnement du module EDR Optimum :

- Utilisation du *Rapport sur l'état des modules de l'application* dans Web Console.

  Le module **Endpoint Detection and Response Optimum** a été ajouté à la liste des modules de Kaspersky Endpoint Security. Pour des informations détaillées sur l'utilisation des rapports, consultez l'aide de Kaspersky Security Center.
- Dans les propriétés de l'appareil dans Web Console.
- À l'aide de la ligne de commande.

6. **Activation du transfert de données vers le Serveur d'administration**

   Pour que toutes les fonctionnalités de Kaspersky Endpoint Detection and Response Optimum fonctionnent, vous devez configurer les paramètres suivants :

   - Activez l'envoi des informations sur les fichiers dans la sauvegarde et dans la quarantaine vers le stockage de Kaspersky Security Center. Pour ce faire, vous devez cocher les cases dans les propriétés de la stratégie :
     - **À propos des fichiers de la sauvegarde**.
     - **À propos des fichiers de quarantaine**.
   - Autoriser l'affichage de la liste d'alertes Pour ce faire, vous devez activer le commutateur **Afficher les alertes EDR** dans la fenêtre principale de Web Console dans la section **Paramètres** → **Paramètres de l'interface**.

     > Paramètre **Afficher les alertes EDR** non disponible dans les versions de Web Console inférieures à 15.1.

Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum

Vous pouvez activer et désactiver le module EDR Optimum :

- à l'aide de Web Console ;
- À l'aide de la ligne de commande.

> La gestion des paramètres d'intégration avec Kaspersky Endpoint Detection and Response Optimum via la Console d'administration n'est pas prise en charge.

Activation ou désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans Web Console

Dans Web Console, vous pouvez activer et désactiver le module EDR Optimum et configurer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Optimum :

- dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Endpoint Detection and Response**) ;
- Dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Detection and Response** → **Endpoint Detection and Response Optimum**).

  L'activation et la désactivation du module EDR Optimum dans les propriétés de l'appareil ne sont pas disponibles si l'appareil est couvert par une stratégie.

  Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Optimum dans les propriétés de l'appareil

Paramètre	Description
Endpoint Detection and Response Optimum activé/désactivé	Active ou désactive le module EDR Optimum, requis pour intégrer l'application Kaspersky Endpoint Security à la solution Kaspersky Endpoint Detection and Response Optimum. Le bouton bascule est désactivé par défaut.
Isolation réseau	Cliquer sur le lien **Configurer le déverrouillage de l'appareil** pour ouvrir la fenêtre **Configuration du déverrouillage de l'appareil** dans laquelle vous pouvez configurer la durée de déverrouillage de l'appareil.
Exclusions	Le lien **Configurer les exclusions** ouvre la fenêtre **Exclusions**, dans laquelle vous pouvez configurer des exclusions de l'isolement du réseau.

Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans la ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver le module EDR Optimum à l'aide du paramètre `UseEdrOptimum` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Pour activer le module EDR Optimum à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Pour désactiver le module EDR Optimum à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Consultation de l'état d'intégration avec Kaspersky Endpoint Detection and Response (KATA)

Afficher l'état de l'intégration dans Web Console

Vous pouvez consulter l'état de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans Web Console en sélectionnant la section **Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Général** → **Modules**.

Afficher l'état de l'intégration dans la ligne de commande

Vous pouvez afficher l'état de l'intégration avec Kaspersky Endpoint Detection and Response Optimum à l'aide de la ligne de commande en exécutant la commande `kesl-control --app-info`.

États de l'intégration

Le module EDR Optimum affiche l'un des états suivants :

- *En cours d'exécution*.

  Cet état s'affiche lorsque les conditions suivantes sont simultanément remplies :

  - ajout d'une clé de licence requise pour le fonctionnement d'EDR Optimum ;
  - la date actuelle ne dépasse pas la date d'expiration de la licence ;
  - un ou plusieurs modules de Kaspersky Endpoint Security requis pour le fonctionnement d'EDR Optimum sont activés ;
  - l'intégration avec Kaspersky Endpoint Detection and Response Optimum est activée sur l'appareil.

- *Arrêté (Stopped)*.

  Cet état s'affiche dans les cas suivants :

  - l'intégration avec Kaspersky Endpoint Detection and Response Optimum est désactivée ;
  - L'application Kaspersky Endpoint Security s'est arrêtée.

- *Non prise en charge par la licence*.

  Cet état s'affiche dans les cas suivants :

  - la date actuelle dépasse la date d'expiration de la licence ;
  - la licence actuelle n'inclut pas la fonctionnalité EDR Optimum.

- *Accident (Malfunction)*.

  Cet état s'affiche lorsque les conditions suivantes sont simultanément remplies :

  - la date actuelle ne dépasse pas la date d'expiration de la licence ;
  - une erreur s'est produite lors du fonctionnement d'un ou plusieurs modules de Kaspersky Endpoint Security requis pour le fonctionnement d'EDR Optimum.

Afficher des informations sur la menace détectée et les actions de réponse

Pour afficher toutes les informations sur une menace détectée et effectuer des actions pour répondre à cette menace, vous pouvez utiliser la fenêtre des détails de l'alerte, qui contient :

- graphique de la chaîne de développement des menaces
- des recommandations pour répondre à une menace avec la capacité d'effectuer l'action sélectionnée
- des informations générales sur la détection des menaces (par exemple, le mode de détection) ;
- des informations sur l'appareil protégé ;
- informations relatives à l'objet détecté
- l'historique des fichiers apparaissant sur l'appareil
- des informations sur les actions entreprises par l'application pour répondre à la menace détectée.

Dans la fenêtre des détails de l'alerte, vous pouvez effectuer les actions de réponse suivantes :

- isoler l'appareil sur lequel la menace est détectée
- Mettre un fichier en quarantaine
- créer une tâche *Analyse IOC*

> La durée de conservation des détails des alertes est de 30 jours. Passé ce délai, les anciens enregistrements sont automatiquement supprimés.

Pour plus d'informations sur l'utilisation des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Intégration avec la solution Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response est une solution permettant de détecter et d'analyser automatiquement les incidents de sécurité dans votre infrastructure à l'aide de la télémétrie et de technologies avancées d'apprentissage automatique. Les informations sur l'incident sont transmises aux experts de Kaspersky, qui peuvent ensuite traiter l'incident eux-mêmes ou fournir des recommandations pour sa résolution.

En interagissant avec Kaspersky Managed Detection and Response, l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

- Envoyer des données de télémétrie à Kaspersky Managed Detection and Response pour la détection des menaces.
- Effectuer les actions de réponse visant à garantir les fonctions de sécurité sur la base des commandes reçues de Kaspersky Managed Detection and Response.

L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est assurée par le module de l'application : Managed Detection and Response (ci-après également appelé MDR).

Pour utiliser la fonctionnalité Kaspersky Managed Detection and Response, vous devez activer le module MDR de l'une des manières suivantes :

- En ajoutant une clé de licence à l'aide d'un fichier clé ou d'un code d'activation. Vous pouvez activer l'application Kaspersky Endpoint Security avec une licence qui inclut la fonctionnalité Kaspersky Managed Detection and Response (pour plus de détails, consultez l'aide de Kaspersky Managed Detection and Response). Si la licence principale sous laquelle vous utilisez l'application n'inclut pas la fonctionnalité Kaspersky Managed Detection and Response, vous devez acheter une licence distincte pour cette fonctionnalité et ajouter la clé de licence MDR à l'application.

  Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant des clés de licence à la SVM.

  La licence qui permet l'activation de la fonctionnalité Kaspersky Managed Detection and Response doit être préenregistrée sur le portail MDR.

- En téléchargeant un *fichier BLOB MDR* sur l'appareil, qui contient des informations sur la licence Kaspersky Managed Detection and Response. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR. Vous pouvez télécharger un fichier BLOB dans Web Console, dans la Console d'administration ou dans la ligne de commande.

Si votre configuration ne répond pas aux exigences de fonctionnement sans fichiers de configuration KPSN, vous devez télécharger le fichier de configuration KPSN sur le Serveur d'administration de Kaspersky Security Center pour l'intégration avec Kaspersky Managed Detection and Response. Ce fichier contient les paramètres nécessaires à l'envoi de télémétrie. Le fichier de configuration KPSN est un fichier avec l'extension .pkcs7 et se trouve dans l'archive ZIP du fichier de configuration MDR. Pour plus d'informations, consultez l'aide de Kaspersky Managed Detection and Response.

L'intégration avec Kaspersky Managed Detection and Response comprend les étapes suivantes :

1. **Activation des modules requis de Kaspersky Endpoint Security**

   Assurez-vous que les modules suivants de l'application Kaspersky Endpoint Security sont activés et fonctionnent :

   - Protection contre les fichiers malicieux.
   - Détection comportementale.

   Si ces modules sont désactivés, l'appareil aura un état rouge dans Kaspersky Managed Detection and Response.

   Il est également recommandé d'activer les modules Protection contre les menaces Internet et Protection contre les menaces réseau. Si ces modules sont désactivés, l'appareil aura un état jaune dans Kaspersky Managed Detection and Response.

   Pour en savoir plus sur les états, consultez l'aide de la solution Kaspersky Managed Detection and Response.

2. **Activation de l'utilisation de Kaspersky Security Network en mode avancé**

   La fonctionnalité Kaspersky Managed Detection and Response n'est pas disponible si Kaspersky Security Network est désactivé ou utilisé en mode standard. Vous pouvez configurer l'utilisation de Kaspersky Security Network dans Web Console , dans la Console d'administration ou dans la ligne de commande.

3. **Activation du module MDR**

   Si vous utiliser le module MDR sous une licence, assurez-vous que l'une des conditions suivantes est remplie :

   - Vous utilisez l'application Kaspersky Endpoint Security sous une licence qui inclut la fonctionnalité Kaspersky Managed Detection and Response.
   - Vous avez acheté une licence distincte pour utiliser la fonctionnalité Kaspersky Managed Detection and Response et ajouté à l'application une clé de licence MDR.

     Si l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels, une clé de licence pour activer des fonctionnalités supplémentaires est ajoutée à la SVM.

   Si vous activez le module MDR à l'aide d'un fichier BLOB MDR, vous devez télécharger le fichier BLOB dans Web Console, dans la Console d'administration ou dans la ligne de commande.

4. **Chargement du fichier de configuration KPSN**

   Si votre configuration ne répond pas aux exigences de fonctionnement sans fichiers de configuration KPSN, vous devez télécharger le fichier de configuration KPSN sur le Serveur d'administration de Kaspersky Security Center.

5. **Activation du module MDR**

   Le module MDR est désactivé par défaut. Vous pouvez activer et désactiver le module :

   - à l'aide de Web Console ;
   - à l'aide de la Console d'administration ;
   - À l'aide de la ligne de commande.

Vous pouvez vérifier l'état de fonctionnement du module EDR :

- dans les propriétés de l'appareil dans Web Console ou dans la Console d'administration ;
- Via la ligne de commande.

Recommandations pour la création d'une image de référence en vue d'une intégration correcte avec MDR

Nous ne recommandons pas d'inclure l'application Kaspersky Endpoint Security for Linux dans l'image de référence.

Si Kaspersky Endpoint Security for Linux a été inclus dans l'image de référence, procédez comme suit sur chaque appareil basé sur cette image :

1. Pour créer une tâche, exécutez la commande suivante :
2. Désinstallez Kaspersky Endpoint Security for Linux, puis réinstallez-le.

Si vous ne suivez pas ces étapes, il se peut que les appareils ne soient pas identifiés correctement.

Téléchargement du fichier de configuration KPSN pour l'intégration avec Kaspersky Managed Detection and Response

Si votre configuration ne répond pas aux exigences de fonctionnement sans fichiers de configuration KPSN, vous devez télécharger le *fichier de configuration KPSN* sur le Serveur d'administration de Kaspersky Security Center pour l'intégration avec Kaspersky Managed Detection and Response. Ce fichier contient les paramètres nécessaires à l'envoi de télémétrie. Le fichier de configuration KPSN est un fichier avec l'extension .pkcs7 et se trouve dans l'archive ZIP du fichier de configuration MDR. Pour plus d'informations, consultez l'aide de Kaspersky Managed Detection and Response.

Vous pouvez télécharger le fichier de configuration KPSN dans Web Console ou dans la Console d'administration.

En chargeant le fichier de configuration KPSN, vous acceptez de transférer automatiquement les données de l'appareil sur lequel Kaspersky Endpoint Security est installé à Kaspersky à des fins de traitement. Ne chargez pas le fichier de configuration si vous n'acceptez pas le traitement des données transférées. Pour une description détaillée des données transmises, consultez la documentation de Kaspersky Managed Detection and Response.

Pour télécharger le fichier de configuration KPSN dans Web Console :

1. Dans la fenêtre principale de Web Console, ouvrez la fenêtre des propriétés du Serveur d'administration.
2. Dans la liste de gauche, sélectionnez la section **Configuration du serveur proxy KSN**.
3. Activer la fonction **Activer le serveur proxy KSN sur le Serveur d'administration** pour activer le service du serveur proxy KSN.
4. Activez le bouton bascule **Utiliser Kaspersky Private Security Network**.

5. Dans la fenêtre qui s'ouvre pour vous avertir des particularités de l'utilisation du serveur proxy KSN sur des points de distribution sur lesquels est installée une ancienne version de l'Agent d'administration, cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **Fichier avec les paramètres du serveur proxy KSN**.

7. Sélectionnez le fichier de configuration KSN (fichier avec l'extension .pkcs7) et cliquez sur le bouton **Ouvrir**.

8. Acceptez les Conditions du KPSN et cliquez sur le bouton **Enregistrer**.

Pour télécharger le fichier de configuration KPSN dans la Console d'administration :

1. Dans l'arborescence de la Console d'administration, ouvrez la fenêtre des propriétés du Serveur d'administration.

2. Sélectionnez la section **Serveur proxy KSN → Paramètres du serveur proxy KSN**.

3. Cochez la case **Utiliser le Serveur d'administration comme serveur proxy** pour activer le service du serveur proxy KSN.

4. Cochez la case **Configurer KPSN**.

5. Dans la fenêtre qui s'ouvre pour vous avertir des particularités de l'utilisation du serveur proxy KSN sur des points de distribution sur lesquels est installée une ancienne version de l'Agent d'administration, cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **Fichier avec les paramètres du serveur proxy KSN**.

7. Sélectionnez le fichier de configuration KSN (fichier avec l'extension .pkcs7) et cliquez sur le bouton **Ouvrir**.

8. Acceptez les Conditions du KPSN et cliquez sur le bouton **Appliquer**.

Configuration de l'intégration avec Kaspersky Managed Detection and Response dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'intégration avec Kaspersky Managed Detection and Response dans les propriétés de la stratégie (**Paramètres de l'application → Built-in Agents Configuration → Managed Detection and Response**).

Configuration de l'intégration avec Kaspersky Managed Detection and Response dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver le module MDR et charger un fichier BLOB MDR dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Detection and Response → Managed Detection and Response**).

Si vous utilisez une clé de licence pour activer le module MDR, vous n'avez pas besoin de télécharger le fichier BLOB MDR.

Paramètre	Description
Activer Managed Detection and Response	Le case active ou désactive le module MDR, nécessaire pour intégrer l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response. Le module est désactivé par défaut. Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, vous serez invité à accepter les conditions d'utilisation de Kaspersky Security Network pour activer Kaspersky Security Network en mode avancé. Si la modification des paramètres KSN est interdite par la stratégie parent, un message d'erreur s'affiche et le module MDR n'est pas activé.
Charger	En appuyant sur le bouton, vous ouvrez une fenêtre standard de Microsoft Windows dans laquelle vous pouvez sélectionner le fichier MDR BLOB à télécharger.

Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR, inclus avec la solution Kaspersky Managed Detection and Response.

En chargeant le fichier BLOB, vous acceptez de transférer automatiquement les données de l'appareil sur lequel Kaspersky Endpoint Security est installé à Kaspersky à des fins de traitement. Ne chargez pas le fichier si vous n'acceptez pas le traitement des données transférées. Pour une description détaillée des données transmises, consultez l'aide de Kaspersky Managed Detection and Response.

Configuration de l'intégration avec Kaspersky Managed Detection and Response dans la ligne de commande

Sur la ligne de commande, vous pouvez :

- Activer ou désactiver le module MDR.
- Télécharger et supprimer le fichier MDR BLOB, qui contient des informations sur la licence Kaspersky Managed Detection and Response.

  Si vous utilisez une clé de licence pour activer le module MDR, vous n'avez pas besoin de télécharger le fichier BLOB MDR.

- Modifier l'heure de début de la tâche de service *Mdr_Autostart_Scan*, qui est créée automatiquement après l'intégration de Kaspersky Endpoint Security avec Managed Detection and Response.

il est recommander de configurer l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response dans la Console d'administration ou dans Web Console.

Vous pouvez activer ou désactiver le module MDR à l'aide du paramètre `UseMDR` des paramètres généraux de l'application. Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseMDR` peut prendre les valeurs suivantes :

- `Yes` : activer le module MDR.
- `No` : désactiver le module MDR.

Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, un message d'erreur s'affiche et le module MDR n'est pas activé. Pour activer le module MDR, vous devez activer l'utilisation de KSN en mode avancé.

Vous pouvez charger et supprimer le fichier BLOB à l'aide des commandes de gestion des clés de licence. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR.

Pour charger le fichier BLOB, exécutez la commande suivante :

```
kesl-control --load-mdr-blob <chemin d'accès au fichier MDR BLOB>
```

Pour supprimer le fichier BLOB, exécutez la commande suivante :

```
kesl-control --remove-mdr-blob
```

Après avoir activé l'intégration, la tâche de service *Mdr_Autostart_Scan* est créée dans l'application avec un mode de lancement une fois par jour. Si nécessaire, vous pouvez configurer l'heure de début de cette tâche. Les autres paramètres de tâche et les autres paramètres de planification de tâche ne peuvent pas être modifiés.

Isolation réseau

Lorsqu'il est intégré aux solutions Detection and Response, un appareil peut être isolé du réseau dans le cadre d'une action de réponse aux menaces.

Caractéristiques de l'isolement du réseau

Une fois l'isolement du réseau activé, l'application interrompt toutes les connexions réseau TCP/IP actives et bloque toutes les nouvelles connexions réseau TCP/IP sur l'appareil, à l'exception des connexions suivantes :

- Connexions spécifiées dans les exclusions de l'isolement du réseau.
- Connexions initiées par les services de Kaspersky Endpoint Security.
- Connexions initiées par l'Agent d'administration de Kaspersky Security Center.
- Connexions avec la SVM et le Serveur d'intégration si l'application est utilisée en mode Light Agent.
- Connexions à KSN (lorsqu'il est intégré à Kaspersky Managed Detection and Response).

L'isolement du réseau peut être appliqué lorsque l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premise) est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée et le module MDR est activé.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) et avec Kaspersky Managed Detection and Response, l'activation et la désactivation de l'isolement réseau d'un appareil, ainsi que la configuration des exclusions de l'isolement du réseau, sont effectuées du côté de la solution Detection and Response correspondante. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premise), dans l'aide de Kaspersky Anti Targeted Attack Platform ou dans l'aide de Kaspersky Managed Detection and Response. Si nécessaire, vous pouvez désactiver manuellement l'isolation réseau pour l'appareil :

- dans les propriétés de l'appareil dans Web Console (uniquement lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Expert (on-premise) ou à Kaspersky Endpoint Detection and Response (KATA)) ;
- Dans la ligne de commande.

La désactivation manuelle de l'isolement du réseau est disponible, que l'intégration avec les solutions Detection and Response soit activée ou non, et que l'appareil soit couvert par une stratégie ou non.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, l'isolement du réseau peut être appliqué dans l'un des modes suivants :

- Mode automatique de l'isolement du réseau. L'appareil peut être isolé automatiquement du réseau suite à la détection d'indicateurs de compromission. Si, lors de la création et de la configuration des paramètres de la tâche *Analyse IOC* dans le groupe **Actions en cas de détection d'un IOC**, vous avez coché les cases **Appliquer les actions de réponse lorsqu'un IOC est détecté** et **Isoler l'appareil du réseau**, puis l'isolement du réseau est activé automatiquement lorsque l'application détecte des indicateurs de compromission.

  Vous pouvez configurer les paramètres d'isolement du réseau suivants en mode automatique :

  - Modifier la période de temps après laquelle l'isolement du réseau est automatiquement désactivé.
  - Configurer les exclusions de l'isolement du réseau pour les appareils isolés automatiquement.

  > Si un appareil isolé en mode automatique est soumis à une stratégie, les paramètres spécifiés dans la stratégie sont appliqués. Si la stratégie n'est pas appliquée, les paramètres spécifiés dans les propriétés de l'appareil sont appliqués.

- Mode manuel de l'isolement du réseau. L'appareil peut être isolé du réseau pendant que la menace détectée est étudiée. Vous pouvez activer manuellement l'isolement du réseau pour un appareil dans la fenêtre des détails de l'alerte et dans les propriétés de l'appareil dans Web Console.

  Vous pouvez configurer les paramètres d'isolement du réseau suivants en mode manuel :

  - Modifier la période de temps après laquelle l'isolement du réseau est automatiquement désactivé.
  - Configurer les exclusions de l'isolement du réseau pour les appareils isolés manuellement.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez désactiver manuellement l'isolement réseau d'un appareil dans les propriétés de l'appareil dans Web Console et dans la ligne de commande.

Vous pouvez vérifier l'état d'isolement réseau de l'appareil à partir de la ligne de commande.

Un appareil isolé est automatiquement marqué par le tag **ISOLATED FROM NETWORK**. Une fois l'isolement du réseau désactivé, ce tag est automatiquement supprimée.

Pour obtenir des informations générales sur l'obtention d'une liste des appareils isolés par tag, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Limites de l'isolation réseau

Lorsque vous utilisez l'isolement du réseau, il est fortement recommandé de vous familiariser avec les restrictions.

Pour que l'isolation réseau fonctionne, l'application Kaspersky Endpoint Security doit être en cours d'exécution. Lors d'une panne de l'application Kaspersky Endpoint Security (lorsque l'application n'est pas en cours d'exécution), le blocage du trafic lorsque l'isolement du réseau est activée par les solutions Detection and Response n'est pas garanti.

DHCP et DNS ne sont pas automatiquement ajoutés aux exclusions de l'isolation réseau. Par conséquent, si l'adresse réseau d'une ressource a été modifiée pendant l'isolation réseau, l'application Kaspersky Endpoint Security ne pourra pas y accéder. Il en va de même pour les nœuds du serveur tolérant aux pannes KATA. Il n'est pas recommandé de modifier leurs adresses afin que Kaspersky Endpoint Security ne perde pas le contact avec eux.

Le serveur proxy n'est pas non plus automatiquement ajouté aux exclusions de l'isolation réseau, vous devez donc l'ajouter manuellement aux exclusions afin que l'application Kaspersky Endpoint Security ne perde pas la connexion avec le serveur qui assure l'intégration.

L'exclusion des processus de l'isolement du réseau par nom est prise en charge sur les appareils dotés d'un noyau version 4.18 ou ultérieure avec eBPF, la prise en charge de BTF et les fonctions tracepoints et kprobes activées pour le traçage du noyau.

Si Kaspersky Endpoint Security est utilisé en mode standard ou en mode Endpoint Detection and Response Agent, lors de l'utilisation de l'isolement du réseau, il est recommandé :

- Utiliser le serveur proxy KSN pour interagir avec Kaspersky Security Network.
- Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation de l'application.

  S'il est impossible d'utiliser Kaspersky Security Center comme serveur proxy, il faut configurer les paramètres du serveur proxy requis et les ajouter aux exclusions.
- Spécifier Kaspersky Security Center comme source des mises à jour des bases de données.

Ces recommandations ne s'appliquent pas si l'application Kaspersky Endpoint Security est utilisé en mode Light Agent.

Activer ou désactiver manuellement l'isolation réseau d'un appareil dans Web Console

Vous pouvez activer l'isolement réseau d'un appareil à l'aide de Web Console uniquement lorsqu'il est intégré à Kaspersky Endpoint Detection and Response Optimum.

Activer ou désactiver manuellement l'isolation réseau des appareils lorsqu'ils sont intégrés à la solution Kaspersky Endpoint Detection and Response Optimum

Pour activer ou désactiver manuellement l'isolement du réseau pour un appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response** et cliquez sur le lien **Endpoint Detection and Response Optimum**.

7. Dans la fenêtre qui s'ouvre, dans le groupe de paramètres **isolement du réseau**, effectuez l'une des opérations suivantes :

   - Cliquez sur le bouton **Isoler l'appareil du réseau**, pour activer l'isolement réseau de l'appareil.

     Lorsque vous cliquez sur ce bouton, l'application isole l'appareil pendant la période que vous avez définie dans les propriétés de la tâche *Activation de l'isolement réseau (NetworkIsolationStart)*.

   - Cliquez sur le bouton **Débloquer un appareil isolé** pour désactiver l'isolation réseau de l'appareil.

8. Cliquez sur le bouton **OK**.

Si vous avez activé l'isolement réseau de l'appareil, Kaspersky Endpoint Security attribuera le tag **ISOLATED FROM NETWORK** à l'appareil. Si vous avez désactivé l'isolation réseau d'un appareil, Kaspersky Endpoint Security supprimera ce tag de l'appareil.

Désactivation manuelle de l'isolement réseau d'un appareil lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou Kaspersky Endpoint Detection and Response (KATA)

Pour désactiver manuellement l'isolation réseau pour un appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil dont vous avez besoin dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response**.

7. Dans le groupe **Isolement du réseau (EDR Expert (on-premise))**, cliquez sur le bouton **Débloquer un appareil isolé** pour désactiver l'isolement réseau de l'appareil.

Après avoir désactivé l'isolation réseau d'un appareil, Kaspersky Endpoint Security supprimera le tag **ISOLATED FROM NETWORK** de l'appareil.

Configuration de la durée d'isolement du réseau en mode automatique

Vous pouvez configurer des exclusions de l'isolement du réseau en mode automatique uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum.

L'isolement du réseau des appareils isolés à la suite de la tâche *Analyse IOC* est automatiquement désactivée après une période de temps spécifiée. Vous pouvez configurer cette période dans Web Console dans les propriétés de l'appareil et dans les propriétés de la stratégie. Les paramètres de l'isolement du réseau dans les propriétés de la stratégie de Web Console sont décrits dans l'Annexe 5. Les paramètres de l'isolement du réseau dans les propriétés de l'appareil administré sont décrits dans le tableau ci-dessous.

Si un appareil est couvert par une stratégie, les paramètres spécifiés dans la stratégie sont appliqués ; le paramètre d'arrêt automatique de l'isolation réseau n'est pas disponible dans les propriétés de l'appareil. Si l'appareil n'est pas couvert par la stratégie, les paramètres spécifiés dans les propriétés de l'appareil sont appliqués.

Par défaut, l'application désactive l'isolation réseau 5 heures après son activation. Après avoir désactivé l'isolement du réseau, l'appareil peut fonctionner sur le réseau sans restrictions.

Configuration de la désactivation automatique de l'isolation réseau dans les propriétés de l'appareil

Pour configurer la désactivation automatique de l'isolement réseau de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response** et cliquez sur le lien **Endpoint Detection and Response Optimum**.

7. Dans le groupe de paramètres **Isolation réseau**, cliquez sur le lien **Configurer le déverrouillage de l'appareil**.

8. Dans la fenêtre ouverte **Configuration du déverrouillage de l'appareil**, cochez la case **Débloquer un appareil automatiquement isolé après** et dans le champ de saisie ci-dessous, indiquez la période en heures après laquelle l'appareil sera automatiquement déverrouillé.

9. Enregistrez vos modifications.

Configuration des paramètres de l'isolation réseau en mode manuel

Vous pouvez isoler manuellement un appareil du réseau uniquement lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum.

Si vous activez manuellement l'isolement du réseau pour un appareil, vous pouvez préconfigurer les paramètres d'isolement du réseau à l'aide de la tâche locale *Activation de l'isolement du réseau* (*NetworkIsolationStart*). Vous pouvez configurer des exclusions de l'isolation réseau et la durée de l'isolation réseau pour un appareil.

La tâche *Activation de l'isolation réseau* est préinstallée et ne s'exécute automatiquement que dans les cas suivants :

- Si vous avez cliqué sur le bouton **Isoler l'appareil du réseau** dans les propriétés de l'appareil.
- Si vous avez activé l'isolement réseau de l'appareil à partir de la fenêtre des détails de l'alerte.

Vous ne pouvez pas créer une nouvelle instance de la tâche *Activation de l'isolement du réseau* à l'aide du bouton **Ajouter** ou l'exécuter en cliquant sur le bouton **Exécuter**. La tâche est uniquement disponible dans les propriétés de l'appareil, où vous pouvez modifier ses paramètres avant d'activer l'isolement réseau de l'appareil.

Paramètres de la tâche *Activation de l'isolement du réseau* s'appliquent indépendamment du fait que l'appareil soit couvert ou non par la stratégie.

Pour configurer les paramètres de l'isolement réseau de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil géré qui s'ouvre, accédez à l'onglet **Tâches**.

5. Dans la liste des tâches, cliquez sur la tâche *Activation de l'isolement du réseau*.

   La fenêtre des propriétés de la tâche s'ouvre.

6. Accédez à l'onglet **Paramètres de l'application**.

7. Cliquez sur le lien **Configurer les exclusions** pour ouvrir la fenêtre **Exclusions**.

8. Dans la fenêtre qui s'ouvre, utilisez les boutons au-dessus du tableau pour effectuer l'action souhaitée :

   - Si vous souhaitez ajouter des informations sur une connexion réseau exclue, faites-le de l'une des manières suivantes :

     - cliquer sur le bouton **Ajouter** et saisir les informations sur la connexion réseau;

     - cliquez sur le bouton **Ajouter à partir d'un profil** et sélectionner un profil réseau dans le dictionnaire.

   - Si vous souhaitez supprimer les informations sur une connexion réseau à exclure, cochez la case en regard de la connexion réseau à supprimer et cliquez sur le bouton **Supprimer**.

9. Cliquez sur le bouton **OK**.

10. Saisissez la durée requise d'isolement réseau de l'appareil en heures dans le champ **Isoler l'appareil pour**.

    La durée d'isolement du réseau par défaut est de 5 heures.

    La durée minimale d'isolement du réseau ne peut être inférieure à 1 heure.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

Configuration des exclusions de l'isolement du réseau dans Web Console

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, la configuration des exclusions de l'isolement du réseau est exécutée du côté de la solution Detection and Response correspondante. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premise), dans l'aide de Kaspersky Anti Targeted Attack Platform ou dans l'aide de Kaspersky Managed Detection and Response.

Lors de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez configurer les exclusions de l'isolement du réseau des manières suivantes :

- Dans les propriétés de la stratégie dans Web Console. Les exclusions configurées dans la stratégie sont appliquées lorsque l'isolement du réseau est automatiquement activé pour un appareil sous la stratégie.
- Dans les propriétés de l'appareil dans Web Console. Les exclusions configurées dans les propriétés de l'appareil sont appliquées lorsque l'isolement du réseau est automatiquement activé pour un appareil qui n'est pas couvert par la stratégie.
- Dans les paramètres de la tâche locale *Activation de l'isolement du réseau* (*NetworkIsolationStart*). Les exclusions configurées dans les propriétés de cette tâche sont appliquées lorsque vous activez manuellement l'isolement du réseau pour un appareil. Les paramètres de la tâche *Activation de l'isolement du réseau* s'appliquent, qu'une stratégie soit appliquée ou non à l'appareil.

Pour configurer les exclusions de l'isolement du réseau, l'application fournit une liste de *profils de réseau standard*. Les profils réseau sont constitués de règles qui garantissent le fonctionnement ininterrompu des appareils dotés des rôles du serveur DNS/DHCP et du client DNS/DHCP. Vous pouvez modifier les paramètres des profils de réseau standard et définir des exclusions manuellement.

Configuration des exclusions de l'isolement du réseau en mode automatique

Vous pouvez configurer des exclusions d'isolation réseau pour les appareils isolés automatiquement dans les propriétés de la stratégie ou dans les propriétés de l'appareil. Les paramètres de l'isolement du réseau dans les propriétés de la stratégie de Web Console sont décrits dans l'Annexe 5.

Vous pouvez configurer des exclusions de l'isolation réseau uniquement lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum.

L'ajout ou la suppression des exclusions de l'isolation réseau dans les propriétés de l'appareil n'est pas disponible si l'appareil est couvert par une stratégie.

Pour ajouter ou supprimer une exclusion de l'isolation réseau dans les propriétés de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil souhaité dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response** et cliquez sur le lien **Endpoint Detection and Response Optimum**.

7. Dans la fenêtre qui s'ouvre, dans le groupe des paramètres **Exclusions**, cliquez sur le lien **Configurer les exclusions** et ouvrez la fenêtre **Exclusions**.

8. Dans la fenêtre qui s'ouvre, utilisez les boutons au-dessus du tableau pour effectuer l'action souhaitée :

   - Si vous souhaitez ajouter des informations sur une connexion réseau exclue, faites-le de l'une des manières suivantes :

     - cliquer sur le bouton **Ajouter** et saisir les informations sur la connexion réseau;

     - cliquez sur le bouton **Ajouter à partir d'un profil** et sélectionner un profil réseau dans le dictionnaire.

   - Si vous souhaitez supprimer les informations sur une connexion réseau à exclure, cochez la case en regard de la connexion réseau à supprimer et cliquez sur le bouton **Supprimer**.

9. Cliquez sur le bouton **OK** pour enregistrer vos modifications.

Ajouter une fenêtre d'exclusion de l'isolement du réseau

Dans cette fenêtre, vous pouvez saisir des informations sur la connexion réseau qui n'a pas besoin d'être bloquée une fois l'isolation réseau activée.

Paramètres de connexion réseau

Paramètre	Description
Nom	Champ de saisie pour le nom de la connexion réseau.
Direction	Dans la liste déroulante, vous pouvez sélectionner la direction de la connexion réseau : • **Sortant**. • **Entrant**. • **Entrant/Sortant**.

Paramètre	Description
Protocole.	Dans la liste déroulante, vous pouvez sélectionner le protocole utilisé par la connexion réseau : • **Quelconque**. • **Personnalisé**. • **ICMP**. • **IPv6_ICMP**. • **TCP**. • **UDP**. • **IGMP**. • **GRE**. • **IPv4**. • **IPv6**.
Nombre	Champ de saisie du numéro de connexion réseau. Le champ est disponible si la valeur **Personnalisé** est sélectionnée dans la liste déroulante **Protocole**.
Ports/plages locaux	La case ajoute les numéros de port local ou les plages de ports locaux répertoriés dans le champ ci-dessous à la liste des exclusions d'isolement du réseau.
Ports/plages à distance	La case ajoute les numéros de port à distance ou les plages de ports distants répertoriés dans le champ ci-dessous à la liste des exclusions d'isolement du réseau.
Adresse à distance	La case ajoute l'adresse IP de l'appareil à distance spécifiée dans le champ ci-dessous à la liste des exclusions d'isolement du réseau.
Applications	La case ajoute les applications répertoriées dans le tableau sous la case à la liste des exclusions de l'isolement du réseau. Vous pouvez ajouter un chemin vers une application dont la connexion réseau n'a pas besoin d'être bloquée en cliquant sur le bouton **Ajouter**. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès à l'application dans le champ **Chemin d'accès à l'application** et enregistrez les modifications. Vous pouvez supprimer une application du tableau en cochant la case en regard de l'application à supprimer, puis en cliquant sur le bouton **Supprimer**. Ces paramètres s'appliquent aux appareils avec une version de noyau à partir de 4.18 prenant en charge eBPF avec BTF et avec les fonctions tracepoints et kprobes activées pour le traçage du noyau.

Fenêtre Dictionnaire des profils réseau

Dans cette fenêtre, vous pouvez sélectionner un ou plusieurs profils de connexion réseau exclus.

Profils de connexion réseau

Profil de connexion réseau	Description
Serveur DNS	Service qui fournit une résolution de noms DNS en répondant aux demandes d'adresse IP et aux demandes de mise à jour d'enregistrement DNS.
Client DNS	Service qui fournit une résolution de noms DNS en effectuant des requêtes de noms DNS.
Services de certificats Active Directory	Services utilisés pour créer, vérifier et révoquer des certificats des clés publiques à usage interne au sein d'une organisation.
Services de fédération Active Directory	Services utilisés pour fournir aux utilisateurs un accès à plusieurs services Web ou ressources réseau à l'aide d'un seul ensemble d'informations d'identification stockées de manière centralisée.
Services Active Directory d'accès léger à l'annuaire	Services qui fournissent les mêmes fonctionnalités que les services de domaine Active Directory mais ne nécessitent pas la création de domaines ou de contrôleurs de domaine.
Services d'administration des droits Active Directory	Services utilisés pour contrôler l'accès des utilisateurs aux documents.
DHCP	Service qui utilise le protocole DHCP (Dynamic Host Configuration Protocol) pour distribuer automatiquement les adresses IP.
Protocole de transfert de fichiers (FTP)	Protocole réseau standard utilisé pour transférer des fichiers entre un client et un serveur sur un réseau.
Centre de distribution de clés Kerberos	Service réseau utilisé pour fournir des tickets (TGS) et des clés de session temporaires aux utilisateurs et aux appareils d'un domaine Active Directory.

Profil de connexion réseau	Description
Shell sécurisé (SSH)	Protocole qui permet l'administration à distance du système d'exploitation et la tunnelisation des connexions TCP.
Modules système Linux	Les services système réseau de Linux, tels que NetworkManager.

Gestion de l'isolation réseau des appareils à partir de la ligne de commande

Lors de l'intégration avec les solutions Detection and Response, vous pouvez effectuer les actions suivantes à l'aide de la ligne de commande :

- vérifier l'état d'isolement réseau d'un appareil et afficher la liste des exclusions d'isolement du réseau ;
- désactiver l'isolement réseau de l'appareil.

Pour désactiver l'isolement réseau d'un appareil, exécutez la commande suivante :

```
kesl-control [-R] --isolation-off
```

Pour vérifier l'état de l'isolement du réseau et afficher la liste des exclusions de l'isolement du réseau, exécutez la commande suivante :

```
kesl-control [-R] --isolation-stat
```

Pour l'isolement du réseau, l'un des états suivants s'affiche :

- *Isolement du réseau activé*.
- *Isolation réseau désactivée*.

Travailler avec la quarantaine

La *quarantaine* est un stockage spécial sur l'appareil où sont placés les fichiers qui peuvent être infectés par des virus ou qui sont incurables au moment de la détection. La quarantaine vous permet d'isoler un fichier pour une analyse plus approfondie. Les fichiers mis en quarantaine sont stockés chiffrés et ne menacent pas la sécurité de l'appareil. Contrairement à la quarantaine, la sauvegarde est conçu pour stocker des copies de sauvegarde des fichiers dans lesquels un code malveillant a été détecté et qui ont été supprimés ou modifiés au cours du processus de traitement.

L'application utilise la quarantaine uniquement lorsqu'elle est intégrée avec les solutions Detection and Response pour effectuer les actions de réponse aux menaces recommandées. Lors de l'intégration de l'application avec Kaspersky Endpoint Detection and Response Optimum ou avec Kaspersky Managed Detection and Response, vous pouvez également mettre manuellement en quarantaine les fichiers que vous considérez comme dangereux pour votre appareil.

Par défaut, le répertoire /var/opt/kaspersky/kesl/common/objects-backup/ est utilisé pour stocker les fichiers mis en quarantaine. Ce répertoire stocke également les objets de la sauvegarde. Vous pouvez modifier le répertoire dans lequel les objets de sauvegarde et de quarantaine sont stockés à l'aide de la ligne de commande.

Les fichiers en quarantaine peuvent contenir des données personnelles. L'accès root est requis pour accéder aux fichiers mis en quarantaine.

Vous pouvez configurer les paramètres de quarantaine sur un appareil à l'aide d'une stratégie dans Web Console ou dans la Console d'administration, ou à l'aide de la ligne de commande. Vous pouvez configurer les paramètres suivants de la quarantaine :

- Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Par défaut, un événement est généré lorsque la quarantaine est pleine à 90 %.
- Volume maximal de la quarantaine en mégaoctets. Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime automatiquement les fichiers les plus anciens de la quarantaine. Par défaut, la taille maximale de la quarantaine est de 200 Mo si l'application est utilisée en mode standard ou mode EDR Agent, et de 100 Mo si l'application est utilisée en mode Light Agent.
- Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine (ce paramètre est configurable uniquement à l'aide de la ligne de commande).

Mise en quarantaine des fichiers

Certains fichiers peuvent être critiques pour le fonctionnement du système d'exploitation et de l'application. La mise en quarantaine de ces fichiers peut perturber le fonctionnement du système.

Vous ne pouvez pas mettre en quarantaine les objets critiques du système (SCO). SCO comprend les fichiers nécessaires au fonctionnement du système d'exploitation et de l'application Kaspersky Endpoint Security.

La mise en quarantaine d'un fichier n'est possible que si l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premise) est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Managed Detection and Response est activée et le module MDR est activé.

Le répertoire pour stocker les objets de quarantaine doit être accessible en écriture.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), les fichiers sont mis en quarantaine de l'une des manières suivantes :

- Suite à l'exécution d'une tâche configurée du côté de la solution Detection and Response correspondante. Pour plus d'informations, consultez l'aide de Kaspersky Endpoint Detection and Response Expert (on-premise) ou l'aide de la Kaspersky Anti Targeted Attack Platform.
- Suite à l'exécution de la tâche d'analyse YARA de la mémoire du processus.

Lorsqu'ils sont intégrés à Kaspersky Managed Detection and Response, les fichiers sont mis en quarantaine de l'une des manières suivantes :

- Suite à l'exécution d'une tâche configurée du côté de Kaspersky Managed Detection and Response.
- Suite à l'exécution de la commande de gestion de la quarantaine sur l'appareil.

Pour plus d'informations sur l'utilisation de la quarantaine lors de l'intégration avec Kaspersky Managed Detection and Response, consultez l'aide de Kaspersky Managed Detection and Response.

Lorsqu'ils sont intégrés à Kaspersky Endpoint Detection and Response Optimum, les fichiers sont mis en quarantaine de l'une des manières suivantes :

- Automatiquement suite à la détection d'indicateurs de compromission.
- Suite à l'exécution de la tâche *Mettre en quarantaine un fichier*, que vous pouvez créer dans Web Console.
- Suite à l'exécution de la commande de gestion de la quarantaine sur l'appareil.
- Suite à l'exécution de la recommandation des détails de l'alerte.

Pour plus d'informations sur l'utilisation de la quarantaine lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Travailler avec des fichiers en quarantaine

Vous pouvez travailler avec des fichiers en quarantaine :

- Dans Kaspersky Security Center, dans la liste générale des fichiers mis en quarantaine par les applications Kaspersky.

  Pour effectuer des actions sur les fichiers en quarantaine dans Kaspersky Security Center, vous devez activer le transfert de données sur les fichiers en quarantaine vers le Serveur d'administration.

- Localement sur l'appareil à l'aide de la ligne de commande.

Vous pouvez afficher des informations sur les fichiers en quarantaine, supprimer et restaurer les fichiers depuis la quarantaine.

La restauration, la suppression et la récupération d'un fichier de quarantaine sont disponibles, que l'intégration avec les solutions Detection and Response soit activée ou non, et que l'appareil soit couvert par une stratégie ou non.

Une liste générale des fichiers mis en quarantaine par les applications de Kaspersky sur les appareils clients est générée dans Kaspersky Security Center et est disponible dans la Console d'administration (**Avancés** → **Stockages** → **Quarantaine**) et dans Web Console (**Opérations** → **Stockages** → **Quarantaine**). Kaspersky Security Center ne copie pas les fichiers depuis les stockages de la quarantaine vers le Serveur d'administration ; tous les fichiers sont placés dans les stockages de la quarantaine sur les appareils clients. Pour obtenir des informations détaillées sur la gestion des fichiers en quarantaine dans Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Le fichier mis en quarantaine est restauré à son emplacement d'origine selon les paramètres spécifiés. L'étiquette de mandat (uniquement sur les appareils exécutant Astra Linux) et les attributs (y compris immutable et append-only) du fichier source sont conservés lors de la restauration. Un fichier doté des attributs immutable et append-only ne peut être restauré uniquement qu'à un emplacement spécifié où le fichier original n'existe pas, ou à l'emplacement original mais avec un autre nom. La restauration d'un fichier mis en quarantaine vers un autre répertoire ou vers son emplacement d'origine sous un nom différent nécessite les privilèges root.

Une fois la récupération terminée, l'application supprime la copie du fichier récupéré de la quarantaine.

La restauration d'un fichier depuis la quarantaine échoue avec une erreur dans les cas suivants :

- Le fichier à restaurer est introuvable dans le stockage de la quarantaine.
- Le nom du fichier en cours de restauration est mal orthographié ou dans une casse incorrecte.
- L'identifiant du fichier est incorrect.
- Le répertoire de destination a été supprimé, déplacé, renommé ou vous n'êtes pas autorisé à y accéder.

  Dans ce cas, l'application déplace le fichier vers le répertoire /var/opt/kaspersky/kesl/common/restored/. Vous pouvez déplacer manuellement le fichier de ce répertoire vers le répertoire souhaité.
- Un fichier du même nom existe déjà au chemin spécifié.
- Il n'y a pas assez d'espace sur l'appareil.
- Sur les appareils exécutant Astra Linux uniquement : l'étiquette de capacité du fichier est supérieure à celle du répertoire de destination.
- Uniquement sur les appareils exécutant le système d'exploitation Astra Linux : le niveau de capacité du fichier est inférieur à celui du répertoire de destination, et l'indicateur ccnr n'est pas défini pour ce répertoire.

La suppression d'un fichier depuis la quarantaine échoue avec une erreur dans les cas suivants :

- Le fichier à supprimer est introuvable dans le stockage de la quarantaine.
- Le nom du fichier à supprimer est mal orthographié ou dans une casse incorrecte.
- L'identifiant du fichier est incorrect.

Mise en quarantaine d'un fichier à l'aide de Web Console

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez mettre des fichiers en quarantaine à l'aide de la tâche *Mettre un fichier en quarantaine* dans Web Console.

Vous pouvez créer et exécuter une tâche de mise en quarantaine de fichiers pour tous les appareils gérés ou pour un appareil spécifique.

La tâche est effectuée pour les fichiers spécifiés dans les propriétés de la tâche sous l'onglet **Paramètres de l'application** dans le tableau **Mettre un fichier en quarantaine**. Le tableau contient les informations suivantes sur les fichiers qui doivent être mis en quarantaine :

- **Chemin d'accès** : chemin d'accès au répertoire sur l'appareil où se trouve le fichier.
- **Type de somme de contrôle** : type de vérification de la somme de contrôle du fichier.

À l'aide des boutons au-dessus du tableau, vous pouvez ajouter ou supprimer des informations sur les fichiers que vous souhaitez mettre en quarantaine.

Pour ajouter des informations sur le fichier qui doit être mis en quarantaine, vous devez cliquer sur le bouton **Ajouter** et spécifier les paramètres de la tâche dans la fenêtre qui s'ouvre.

Paramètres de la tâche Mettre un fichier en quarantaine

Paramètre	Description
Spécifiez le fichier que vous souhaitez mettre en quarantaine	Dans la liste déroulante, vous pouvez sélectionner comment spécifier le chemin d'accès au fichier mis en quarantaine : • **Spécifier le fichier par chemin complet**. • **Spécifier le fichier par chemin de répertoire et par de somme de contrôle**.
Chemin d'accès complet au fichier	Champ de saisie pour le chemin complet au fichier mis en quarantaine. Ce champ s'affiche si, dans la liste déroulante **Spécifiez le fichier que vous souhaitez mettre en quarantaine** vous avez sélectionné la valeur **Spécifier le fichier par chemin complet**. Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier commençant par les caractères `//`. Par exemple, vous pouvez saisir le chemin `//server_ip/shared_folder`.
Type de somme de contrôle	Dans la liste déroulante, vous pouvez sélectionner le type de somme de contrôle du fichier à mettre en quarantaine : • **MD5**. • **SHA256**. Cette liste déroulante s'affiche si, dans la liste déroulante **Spécifiez le fichier que vous souhaitez mettre en quarantaine** vous avez sélectionné la valeur **Spécifier le fichier par chemin de répertoire et par de somme de contrôle**.
Somme de contrôle du fichier	Champ permettant de saisir la somme de contrôle du fichier mis en quarantaine. Ce champ s'affiche si, dans la liste déroulante **Spécifiez le fichier que vous souhaitez mettre en quarantaine** vous avez sélectionné la valeur **Spécifier le fichier par chemin de répertoire et par de somme de contrôle**.
Chemin d'accès au fichier.	Champ permettant de saisir le chemin d'accès au répertoire du fichier mis en quarantaine. Ce champ s'affiche si, dans la liste déroulante **Spécifiez le fichier que vous souhaitez mettre en quarantaine** vous avez sélectionné la valeur **Spécifier le fichier par chemin de répertoire et par de somme de contrôle**. Si le fichier se trouve sur un disque réseau, saisissez le chemin d'accès au fichier commençant par les caractères `//`. Par exemple, vous pouvez saisir le chemin `//server_ip/shared_folder`.

La tâche *Mettre en quarantaine un fichier* peut échouer avec l'erreur *Pas assez d'espace dans le stockage de la quarantaine* si vous essayez de mettre en quarantaine un fichier volumineux. Dans ce cas, vous pouvez effacer la quarantaine ou augmenter la taille de la quarantaine, puis réessayer.

Vous pouvez afficher le résultat de la tâche dans les propriétés de la tâche dans Web Console dans la section **Résultats**.

Configuration des paramètres de la quarantaine dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de la quarantaine dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Rapports et stockage**) et dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Paramètres des stockages**).

Les paramètres de la quarantaine dans les propriétés de l'appareil administré sont décrits dans le tableau ci-dessous.

Paramètres de la quarantaine dans les propriétés de l'appareil

Paramètre	Description
Limiter la taille de la quarantaine à (Mo)	Champ de saisie pour spécifier la taille maximale de la quarantaine (en mégaoctets). Si la case est décochée, la taille de la quarantaine est illimitée. Valeur par défaut : 200.
Notifier lorsque la quarantaine est pleine à (%)	Un champ de saisie permettant de spécifier le pourcentage de plénitude de la quarantaine auquel un événement concernant la plénitude de la quarantaine est généré. Si la case n'est pas cochée, l'événement de quarantaine complète n'est pas généré. Valeurs admises : 1 à 100. Valeur par défaut : 90.

Configuration des paramètres de la quarantaine dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de la quarantaine dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres des stockages**) et dans les propriétés de l'appareil administré (**Appareils administrés** → onglet **Appareils** → fenêtre des propriétés de l'appareil → section **Applications** → fenêtre des propriétés de l'application → **Paramètres des stockages**).

Paramètres de quarantaine

Paramètre	Description
Limiter la taille de la quarantaine à (Mo)	La case active ou désactive la limitation de la taille maximale de la quarantaine par la valeur spécifiée (en mégaoctets). Si la case est décochée, la taille de la quarantaine est illimitée. Valeurs admises : 1 à 999999. La valeur par défaut et de 200 si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent, et de 100 si l'application est utilisée en mode Light Agent.
Notifier lorsque la quarantaine est pleine à (%)	La case active ou désactive la limite du pourcentage de plénitude de la quarantaine à laquelle un événement sur la plénitude de la quarantaine est généré. Si la case n'est pas cochée, l'événement de quarantaine complète n'est pas généré. Valeurs admises : 1 à 100. Valeur par défaut : 90.

Configuration des paramètres de la quarantaine dans la ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de la quarantaine à l'aide des paramètres `QuarantineSizeLimit`, `QuarantineFillingNotification` et `QuarantineBackupFolder` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Paramètre	Description	Valeur
`QuarantineFillingNotification`	Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Pour désactiver la génération des événements sur la quarantaine complète, spécifiez la valeur 0.	0 – 100 0 : la génération des événements concernant le remplissage de la quarantaine est désactivée. Valeur par défaut : 90.
`QuarantineSizeLimit`	Volume maximal de la quarantaine (en mégaoctets). Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime les fichiers les plus anciens. Pour supprimer la limite de taille de la quarantaine, saisissez la valeur 0.	0 – 999999 0 : la taille de la quarantaine est illimitée. La valeur par défaut et de 200 si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent, et de 100 si l'application est utilisée en mode Light Agent.
`QuarantineBackupFolder`	Chemin vers le répertoire où sont stockés les objets de sauvegarde et de quarantaine. Vous pouvez définir un répertoire autre que celui défini par défaut. Les répertoires de n'importe quel appareil peuvent être utilisés comme répertoire pour stocker des objets de sauvegarde et de quarantaine. Il est déconseillé de désigner des répertoires qui se trouvent sur des appareils à distance, par exemple des répertoires montés via les protocoles Samba et NFS. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : /var/opt/kaspersky/kesl/common/objects-backup/ L'accès au répertoire par défaut requiert les privilèges root.

Travailler avec des fichiers de quarantaine dans la ligne de commande

Lorsqu'il est intégré avec les solutions Detection and Response, vous pouvez effectuer les actions suivantes à l'aide des commandes de gestion de la quarantaine :

- Placer les fichiers en quarantaine (uniquement lorsqu'ils sont intégrés à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response).
- Afficher des informations sur les fichiers mis en quarantaine.
- Supprimer tous les fichiers spécifiés ou uniquement ceux spécifiés de la quarantaine.
- Restauration d'un fichier depuis la quarantaine.

La restauration d'objets infectés peut infecter l'appareil.

Mettre un fichier en quarantaine

Pour mettre un fichier en quarantaine, exécutez la commande suivante :

```
kesl-control [-Q] --put <chemin d'accès au fichier> [--md5] [--sha256] [--save-original-file]
```

où :

- `< chemin d'accès au fichier >` est le chemin d'accès au fichier que vous souhaitez mettre en quarantaine.
- `--md5` : somme de hachage MD5 du fichier que vous souhaitez mettre en quarantaine ;
- `--sha256` : somme de hachage SHA256 du fichier que vous souhaitez mettre en quarantaine ;
- `--save-original-file` : ne pas supprimer le fichier d'origine. Si vous ne spécifiez pas cette clé, le fichier d'origine sera supprimé.

  Le fichier d'origine est supprimé uniquement si le compte utilisateur dispose de l'autorisation de supprimer des objets. Si les droits sont insuffisants, un message d'erreur concernant la suppression du fichier s'affiche.

Vous ne pouvez utiliser cette commande que lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response.

Afficher des informations sur les fichiers mis en quarantaine

Pour afficher des informations sur les fichiers mis en quarantaine, exécutez la commande suivante :

```
kesl-control -Q --query ["< conditions de filtrage >"] [-n < nombre >] [--json]
```

où :

- `< conditions de filtrage >` spécifient une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtrage, l'application affichera des informations sur tous les fichiers mis en quarantaine.
- `< nombre >` est le nombre de fichiers les plus récemment mis en quarantaine que vous souhaitez afficher. Si vous ne spécifiez pas la clé `-n`, les 30 derniers fichiers seront affichés. Pour afficher tous les fichiers, saisissez la valeur 0.
- `--json` : afficher les données au format JSON.

La ligne `ObjectId` affichera l'identifiant numérique que l'application a attribué au fichier lors de sa mise en quarantaine. Cet identifiant est utilisé pour effectuer des actions sur le fichier, telles que la restauration ou la suppression du fichier de la quarantaine.

Restaurer les fichiers depuis la quarantaine

Pour restaurer un fichier mis en quarantaine avec son nom d'origine vers son emplacement d'origine, exécutez la commande suivante :

```
kesl-control -Q --restore <identifiant de l'objet>
```

où `<identifiant de l'objet>` est un identifiant numérique que l'application a attribué au fichier lors de sa mise en quarantaine.

Pour restaurer un fichier avec un nouveau nom de la quarantaine vers le répertoire spécifié, exécutez la commande suivante :

```
kesl-control -Q --restore <identifiant de l'objet> --file <chemin d'accès au fichier>
```

où `--file <chemin d'accès au fichier>` est le nouveau nom du fichier et le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier.

Vous ne pouvez restaurer un fichier de la quarantaine vers un autre répertoire que si votre compte dispose des droits root. S'il n'y a pas assez de privilèges, le fichier ne peut être restauré qu'à son emplacement d'origine.

Sur les appareils exécutant le système d'exploitation Astra Linux, en mode environnement logiciel fermé, vous ne pouvez restaurer un fichier que sous le compte sous lequel il a été placé dans la sauvegarde.

Mettre un fichier en quarantaine

Pour supprimer les fichiers sélectionnés de la quarantaine, exécutez la commande suivante :

```
kesl-control -Q --mass-remove --query "<conditions de filtrage>"
```

où `<conditions de filtrage>` correspond à une ou plusieurs expressions logiques au format `<champ> <opérateur de comparaison> '<valeur>'`, combinées à l'aide de l'opérateur logique `and` pour limiter les résultats.

Exemples :
Pour supprimer les fichiers qui contiennent "test" dans leur nom ou chemin :

```
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

Pour supprimer tous les fichiers de la quarantaine, exécutez la commande suivante :

```
kesl-control -Q --mass-remove
```

Démarrage du processus

Lors de l'intégration de Kaspersky Endpoint Security avec les solutions Detection and Response, vous pouvez lancer à distance des processus et des fichiers exécutables sur un appareil protégé à l'aide de la tâche de lancement du processus (*Run process*).

Vous pouvez créer et exécuter des tâches de lancement des processus dans Web Console uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

À l'aide de la tâche *Démarrage du processus*, vous pouvez démarrer :

- Processus arrêtés en raison d'une activité malveillante sur l'appareil.
- Processus que vous avez arrêtés. Par exemple, vous pouvez démarrer à distance un processus que vous avez terminé à l'aide de la tâche *Mettre fin au processus*.
- Scripts. Par exemple, vous pouvez exécuter un script pour collecter des données sur un appareil afin d'enquêter sur une menace.
- Utilitaires. Par exemple, vous pouvez exécuter un utilitaire qui enregistre les informations de configuration de l'appareil dans un fichier.
- Annexes.

Si SELinux est installé sur votre système d'exploitation en mode `Enforcing`, alors pour exécuter la tâche *Démarrer le processus*, vous devez configurer en plus le système SELinux.

Vous pouvez créer et exécuter la tâche *Démarrage du processus*, ainsi que modifier ses paramètres dans la Web Console : la tâche *Démarrage du processus* ne peut pas être gérée sur la ligne de commande.

Paramètre	Description
Commande exécutable	Champ de saisie de la commande de démarrage du processus. Par exemple, si vous souhaitez exécuter l'utilitaire `klnagchk`, qui vérifie la connexion au Serveur d'administration, saisissez `/< chemin absolu vers le répertoire contenant l'utilitaire >/klnagchk` puis, si nécessaire, remplissez les autres champs décrits dans le tableau ci-dessous.
Arguments de ligne de commande (facultatif)	Un champ de saisie des arguments de la ligne de commande permettant de transmettre des informations supplémentaires au script, à l'utilitaire ou à l'application lors de son lancement. Par exemple, vous pouvez saisir l'argument `-logfile /tmp/klnagchk.log`. Cet argument indique à l'outil d'enregistrer le résultat dans un fichier nommé `klnagchk.log` dans `/tmp`. Si vous devez transmettre plusieurs arguments, vous devez les séparer par des espaces. Par exemple, vous pouvez saisir les arguments `-logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer`. Ces arguments indiquent à l'utilitaire d'enregistrer le résultat dans un fichier nommé `klnagchk.log` dans le répertoire `tmp`, et d'enregistrer le certificat utilisé pour vérifier l'accès au Serveur d'administration dans le fichier `certificate.cer` dans le répertoire `/home/user/`.
Chemin d'accès au répertoire de travail (facultatif)	Champ destiné au chemin d'accès au répertoire de travail dans lequel la commande du champ **Commande exécutable** est exécutée. Par exemple, vous pouvez saisir `/tmp` et exécuter l'utilitaire `klnagchk` avec les arguments suivants : `-logfile klnagchk.log -savecert certificate.cer`. Dans ce cas, les deux fichiers sont créés dans `tmp`.

Vous pouvez afficher le résultat de la tâche *Démarrage du processus* dans les propriétés de la tâche dans Web Console dans la section **Paramètres de l'application → Résultats d'exécution**.

Le tableau affiche une liste des appareils sur lesquels la tâche *Démarrage du processus* a été exécutée, ainsi que les résultats de la tâche. Dans la liste déroulante **Appareil**, vous pouvez choisir l'affichage des résultats de la tâche pour tous les appareils gérés sur lesquels la tâche a été exécutée ou pour un appareil spécifique.

Le tableau contient les informations suivantes :

- **État** : état d'exécution de la tâche.
- **Appareil** : nom de l'appareil sur lequel la tâche a été lancée.
- **Heure** : date et heure d'exécution de la tâche.
- **Résultats** – Résultat de l'exécution de la tâche sous la forme d'un code de retour. Le lien associé au code de retour ouvre la fenêtre **Résultats de la tâche**, qui affiche les informations suivantes :
  - état d'exécution des tâches ;
  - heure de début du processus ;
  - temps de fin du processus ;
  - nom de l'appareil sur lequel le processus a été lancé ;
  - commande exécutable ;
  - arguments de la ligne de commande ;
  - chemin d'accès au répertoire de travail ;
  - code de retour.

À l'aide du lien **Télécharger les données du flux STDOUT** dans la fenêtre **Résultats du lancement de la tâche**, vous pouvez télécharger un rapport sur la réussite de la tâche au format TXT. Si la tâche *Démarrage du processus* échoue, un message d'erreur s'affichera lorsque vous tenterez de télécharger ce rapport.

À l'aide du lien **Télécharger les données du flux STDERR** dans la fenêtre **Résultats du lancement de la tâche**, vous pouvez télécharger un rapport sur les erreurs survenues lors de l'exécution de la tâche au format TXT. Si la tâche *Démarrage du processus* échoue, un message d'erreur s'affichera lorsque vous tenterez de télécharger ce rapport.

Terminer le processus

Lors de l'intégration de Kaspersky Endpoint Security avec les solutions Detection and Response, vous pouvez terminer à distance les processus sur un appareil protégé à l'aide de la tâche de fin du processus (*Terminate process*).

Vous pouvez créer et exécuter des tâches de fin des processus dans Web Console uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

À l'aide de la tâche *Arrêt du processus*, vous pouvez terminer :

- Processus exécutés sur l'appareil à la suite d'une activité malveillante.
- Processus que vous avez démarrés. Par exemple, vous pouvez mettre fin à distance à un processus que vous avez démarré à l'aide de la tâche *Démarrage du processus*.
- Scripts. Par exemple, vous pouvez mettre fin à distance à un script que vous avez démarré à l'aide de la tâche *Démarrage du processus*.
- Utilitaires. Par exemple, vous pouvez mettre fin à distance à un utilitaire de test de vitesse Internet que vous avez démarré à l'aide de la tâche *Démarrage du processus*.
- Annexes.

Les processus des objets critiques du système (SCO) ne peuvent pas être terminés. SCO comprend les fichiers nécessaires au fonctionnement du système d'exploitation et de l'application Kaspersky Endpoint Security.

Vous pouvez créer et exécuter la tâche *Arrêt du processus*, ainsi que modifier ses paramètres dans la Web Console : la tâche *Arrêt du processus* ne peut pas être gérée sur la ligne de commande.

Paramètres de la tâche Mettre fin au processus

Paramètre	Description
Spécifiez le fichier dont vous souhaitez terminer les processus	Dans la liste déroulante, vous pouvez choisir comment spécifier le chemin d'accès au fichier : • **Par chemin d'accès au répertoire et par somme de contrôle** ; • **Par chemin complet**. • **Par PID**. La valeur **Par PID** s'affiche dans la liste déroulante uniquement pour les tâches créées dans les propriétés de l'appareil.

Paramètre	Description
Chemin d'accès complet au fichier	Champ de saisie pour le chemin complet du fichier. Ce champ apparaît uniquement si vous avez sélectionné **Par chemin complet** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus**.
Type de somme de contrôle	Dans la liste déroulante, vous pouvez sélectionner le type de somme de contrôle du fichier : • **MD5**. • **SHA256**. Cette liste déroulante s'affiche si vous sélectionnez **Par chemin d'accès au répertoire et somme de contrôle** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez arrêter les processus**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier. Ce champ s'affiche si vous avez sélectionné **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus** et dans la liste déroulante **Type de somme de contrôle**, la valeur est **MD5**.
Chemin d'accès au répertoire	Champ de saisie pour le chemin d'accès au répertoire de fichiers. Ce champ s'affiche si vous avez sélectionné **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus**.
ID du processus.	Champ de saisie de l'identifiant de processus (PID). Ce champ apparaît si vous avez sélectionné la valeur **Par PID** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus**.

Vous pouvez afficher le résultat de la tâche *Arrêt du processus* dans les propriétés de la tâche dans Web Console dans la section **Résultats**.

Reception d'un fichier depuis un appareil

Lors de l'intégration de Kaspersky Endpoint Security avec les solutions Detection and Response, vous pouvez recevoir des fichiers d'un appareil protégé à l'aide de la tâche de réception du fichier (*Get file*).

Vous pouvez créer et exécuter des tâches pour recevoir un fichier à partir d'un appareil dans Web Console uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise), avec Kaspersky Endpoint Detection and Response (KATA) ou avec Kaspersky Managed Detection and Response, les tâches sont créées et lancées du côté de la solution Detection and Response correspondante.

Par exemple, vous pouvez recevoir un fichier journal des événements généré par une application tierce.

Vous pouvez créer et exécuter la tâche *Réception d'un fichier depuis un appareil*, ainsi que modifier ses paramètres dans la Web Console : la tâche *Recevoir un fichier depuis un appareil* ne peut pas être gérée sur la ligne de commande.

La tâche *Réception d'un fichier depuis un appareil* est effectuée pour les fichiers spécifiés dans les propriétés de la tâche sous l'onglet **Paramètres de l'application** du tableau **Réception d'un fichier**.

Le tableau contient les informations suivantes sur les fichiers qui doivent être obtenus à la suite d'exécution la tâche :

- **Chemin d'accès au répertoire** : chemin d'accès au répertoire sur l'appareil où se trouve le fichier.
- **Type de vérification de la somme de contrôle** : type de vérification de la somme de contrôle du fichier.

À l'aide des boutons au-dessus du tableau, vous pouvez ajouter, modifier ou supprimer des informations sur les fichiers que vous souhaitez récupérer depuis l'appareil.

Pour ajouter des informations sur le fichier que vous souhaitez recevoir, vous devez cliquer sur le bouton **Ajouter** et spécifier les paramètres de la tâche dans la fenêtre **Réception d'un fichier** qui s'ouvre.

Paramètres de la tâche Réception d'un fichier depuis un appareil

Paramètre	Description
Spécifiez le fichier que vous souhaitez recevoir	Dans la liste déroulante, vous pouvez choisir comment spécifier le chemin d'accès au fichier : • **Par chemin d'accès au répertoire et par somme de contrôle** ; • **Par chemin complet**.
Chemin d'accès complet au fichier	Champ de saisie pour le chemin complet du fichier. Ce champ apparaît si vous avez sélectionné **Par chemin complet** dans la liste déroulante **Spécifiez le fichier que vous souhaitez recevoir**.
Type de somme de contrôle	Dans la liste déroulante, vous pouvez sélectionner le type de somme de contrôle du fichier : • **MD5**. • **SHA256**. Cette liste déroulante s'affiche si vous sélectionnez **Par chemin d'accès au répertoire et somme de contrôle** dans la liste déroulante **Spécifiez le fichier à recevoir**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier. Ce champ s'affiche si vous avez sélectionné **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Spécifiez le fichier que vous souhaitez recevoir**.
Chemin d'accès au répertoire contenant le fichier	Champ de saisie pour le chemin d'accès au répertoire de fichiers. Ce champ s'affiche si, dans la liste déroulante **Spécifiez le fichier à recevoir**, vous avez sélectionné **Par chemin d'accès au répertoire et somme de contrôle**.

Suite à l'exécution de la tâche *Réception d'un fichier depuis un appareil*, une copie du fichier est mise en quarantaine sur l'appareil. Vous pouvez télécharger cette copie depuis la quarantaine via Web Console vers l'appareil à partir duquel vous avez lancé le téléchargement

La taille du fichier ne doit pas dépasser 100 Mo.

Le fichier d'origine sur l'appareil de l'utilisateur reste dans le répertoire d'origine.

Dans Kaspersky Security Center, dans la liste des fichiers mis en quarantaine, tous les fichiers reçus via la tâche *Réception d'un fichier depuis un appareil* auront l'état *Infecté*, quels que soient les résultats de l'analyse des fichiers.

La tâche *Réception d'un fichier depuis un appareil* échoue avec une erreur si :

- le fichier spécifié n'a pas été trouvé ;
- les données du fichier sont incorrectes (nom de fichier ou somme de contrôle) ;
- les privilèges sont insuffisants pour effectuer des actions sur le fichier spécifié ;
- le fichier spécifié est bloqué ;
- il n'y pas assez d'espace dans la quarantaine ;
- le fichier spécifié est trop volumineux (plus de 100 Mo).

Vous pouvez afficher le résultat de la tâche dans les propriétés de la tâche dans Web Console dans la section **Résultats**.

Suppression d'un fichier de votre appareil

Lors de l'intégration de Kaspersky Endpoint Security avec les solutions Detection and Response, vous pouvez supprimer des fichiers d'un appareil protégé à l'aide de la tâche de suppression du fichier (*Delete file*).

Vous pouvez créer et exécuter des tâches de suppression de fichiers dans Web Console uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response (KATA), les tâches sont créées et lancées du côté de Kaspersky Endpoint Detection and Response (KATA).

Les objets critiques du système (SCO) ne peuvent pas être supprimés. SCO comprend les fichiers nécessaires au fonctionnement du système d'exploitation et de l'application Kaspersky Endpoint Security.

Vous pouvez créer et exécuter la tâche *Supprimer un fichier de l'appareil*, ainsi que modifier ses paramètres dans la Web Console : la tâche *Supprimer un fichier de l'appareil* ne peut pas être gérée sur la ligne de commande.

Paramètres de la tâche Suppression d'un fichier depuis un appareil

Paramètre	Description
Spécifiez le fichier à supprimer	Dans la liste déroulante, vous pouvez sélectionner comment spécifier le chemin d'accès au fichier à supprimer : • **Par chemin et somme de contrôle** ; • **Par chemin complet**.
Chemin d'accès complet au fichier	Champ de saisie du chemin complet du fichier à supprimer. Ce champ apparaît si vous avez sélectionné **Par chemin complet** dans la liste déroulante **Spécifiez le fichier à supprimer**.
Type de somme de contrôle	Dans la liste déroulante, vous pouvez sélectionner le type de somme de contrôle du fichier à supprimer : • **MD5**. • **SHA256**. Cette liste déroulante s'affiche si, dans la liste déroulante **Spécifiez le fichier à supprimer**, vous avez sélectionné **Par chemin d'accès au répertoire et somme de contrôle**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier à supprimer. Ce champ s'affiche si vous avez sélectionné **Par chemin et somme de contrôle** dans la liste déroulante **Spécifiez le fichier à supprimer**.
Chemin d'accès au répertoire	Champ de saisie du chemin d'accès au répertoire du fichier à supprimer. Ce champ s'affiche si vous avez sélectionné **Par chemin et somme de contrôle** dans la liste déroulante **Spécifiez le fichier à supprimer**.
Inclure les répertoires joints	La case à cocher active ou désactive les répertoires joints.

Si le fichier est verrouillé par un autre processus, la tâche sera affichée avec l'état *Terminé*, mais le fichier lui-même ne sera supprimé qu'après le redémarrage de l'appareil. Après avoir redémarré votre appareil, assurez-vous que le fichier est supprimé.

La tâche *Suppression d'un fichier de votre appareil* peut échouer avec une erreur *L'accès est interdit* si vous essayez de supprimer un fichier exécutable en cours d'exécution. Dans ce cas, vous devez créer et exécuter la tâche *Arrêt du processus* pour ce fichier, puis réessayer.

Vous pouvez afficher le résultat de la tâche dans les propriétés de la tâche dans Web Console dans la section **Résultats**.

Trouver des indicateurs de compromission

Indicateur de compromission (Indicator of Compromise, IOC) est un ensemble de données sur un objet ou une activité qui indique un accès non autorisé à un appareil (compromission de données). Par exemple, un indicateur de compromission pourrait être un nombre élevé de tentatives de connexion échouées. En intégrant Kaspersky Endpoint Security avec les solutions Detection and Response, vous pouvez détecter les indicateurs de compromission sur les appareils protégés et prendre des mesures pour répondre aux menaces.

La fonctionnalité d'analyse IOC est disponible dans l'application Kaspersky Endpoint Security si l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premise) est activé.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), l'Analyse IOC est exécutée du côté de la solution correspondante.

Lorsqu'elle est intégrée avec Kaspersky Endpoint Detection and Response Optimum, l'analyse IOC est effectuée à l'aide de la tâche d'analyse IOC (*IOC Scan*). Vous pouvez créer des tâches d'analyse IOC :

- dans Web Console ;
- depuis la fenêtre avec les détails de l'alerte ;
- Dans la ligne de commande.

Lors de l'exécution de la tâche Analyse IOC, l'analyse des termes IOC (propriétés de l'objet IOC, par exemple, somme de hachage du fichier) est effectuée uniquement dans l'espace de noms principal du système d'exploitation. La tâche *Analyse IOC* ne calcule pas les sommes de hachage des fichiers de plus de 200 Mo.

Pour rechercher des *indicateurs de compromission*, Kaspersky Endpoint Security utilise les fichiers IOC préparés par l'utilisateur. Si vous souhaitez ajouter manuellement un indicateur de compromission, veuillez consulter les exigences du fichier IOC. Si le fichier IOC ne répond pas aux exigences, l'application ne pourra pas l'utiliser.

Les identifiants de tous les fichiers IOC utilisés dans une seule tâche d'analyse IOC doivent être uniques. Si vous téléchargez plusieurs fichiers IOC avec les mêmes ID, l'application n'utilise qu'un seul de ces fichiers IOC. Les fichiers IOC restants seront automatiquement exclus.

Rechercher des indicateurs de compromission dans Web Console

Vous pouvez rechercher des indicateurs de compromission à l'aide de la tâche d'analyse IOC dans Web Console uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), l'Analyse IOC est exécutée du côté de la solution Detection and Response correspondante.

Vous pouvez créer et exécuter une tâche *Analyse IOC*, ainsi que modifier ses paramètres dans Web Console.

Pour la tâche *Analyse IOC*, la fonctionnalité Wake-on-LAN dans les paramètres de planification n'est pas disponible. Assurez-vous que l'appareil est allumé pour terminer la tâche.

Vous pouvez modifier les paramètres généraux de la tâche *Analyse IOC* dans les propriétés de la tâche sous l'onglet **Paramètres de l'application → Paramètres de l'analyse IOC**.

Paramètres de la tâche *Analyse IOC*

Paramètre	Description
Redéfinir les fichiers IOC	Cliquer sur ce bouton ouvre le panneau **Redéfinir les fichiers IOC**. Lorsque vous cliquez sur le bouton **Ajouter les fichiers IOC** situé dans le panneau **Redéfinir les fichiers IOC**, une fenêtre s'ouvre dans laquelle vous pouvez sélectionner et télécharger sur l'appareil les fichiers IOC nécessaires pour rechercher des indicateurs de compromission. Après avoir téléchargé les fichiers IOC, vous pouvez consulter la liste des indicateurs des fichiers IOC.
Exporter la collection IOC	En cliquant sur le bouton, les fichiers IOC sont téléchargés sur l'appareil.

Paramètre	Description
Appliquer les actions de réponse lorsqu'un IOC est détecté	La case active ou désactive l'application d'actions de réponse lorsque des indicateurs de compromission sont détectés. Si la case est cochée, lorsque des indicateurs de compromission sont détectés, l'application effectue les actions que vous sélectionnez : • **Exécuter une analyse des zones critiques**. Si la case est cochée, lorsque des indicateurs de compromission sont détectés, l'application exécute la tâche *Analyse des zones critiques*. Par défaut, Kaspersky Endpoint Security vérifie la mémoire du noyau, les processus en cours d'exécution, les secteurs de démarrage et d'autres **domaines importants**. ◦ /lib/systemd ◦ /lib/udev ◦ /lib/dbus-1.0 ◦ /usr/local/lib/systemd/user ◦ /usr/share/dbus-1 ◦ /usr/share/gdm/autostart ◦ /usr/share/gnome/autostart ◦ /var/spool/at ◦ /var/spool/at/spool ◦ /var/spool/anacron ◦ /var/spool/cron ◦ /boot ◦ /bin ◦ /sbin ◦ /lib ◦ /lib32 ◦ /lib64 ◦ /libx32 ◦ /usr/lib ◦ /usr/lib32 ◦ /usr/lib64 ◦ /usr/libx32 ◦ ~/.config/autostart ◦ ~/.config/autostart-scripts ◦ ~/.config/plasma-workspace/env ◦ ~/.config/plasma-workspace/shutdown ◦ ~/.config/lxsession ◦ ~/.fluxbox/startup ◦ ~/.kde/Autostart ◦ /etc • **Placer la copie en quarantaine, supprimer l'objet**. Si la case est cochée, lorsque des indicateurs de compromission sont détectés, l'application met en quarantaine une copie de l'objet et supprime l'objet d'origine.

Paramètre	Description
	• **Isoler l'appareil du réseau**. Si cette case est cochée, lorsque des indicateurs de compromission sont détectés, l'application isole l'appareil du réseau pour empêcher la menace de se propager. Vous pouvez configurer le temps d'isolation. Si l'appareil isolé est couvert par la stratégie, les paramètres de désactivation automatique de l'isolation après une période spécifiée sont appliqués, ainsi que les paramètres d'exclusion de l'isolation réseau spécifiés dans les propriétés de la stratégie. Si l'appareil isolé n'est pas couvert par la stratégie, les paramètres spécifiés dans les propriétés de l'appareil sont appliqués. Si la case n'est pas cochée, l'application ne prend aucune action de réponse aux menaces lorsque des indicateurs de compromission sont détectés. Les informations sur la détection des indicateurs de compromission sont affichées dans la fenêtre des détails de l'alerte et dans les propriétés de la tâche.

Vous pouvez modifier des paramètres supplémentaires de la tâche *Analyse IOC* dans les propriétés de la tâche sous l'onglet **Paramètres de l'application → Avancés**.

La section **Avancés** est disponible pour modification si vous avez chargé un fichier IOC dans le panneau **Redéfinir les fichiers IOC**.

Paramètres supplémentaires de la tâche *Analyse IOC*

Paramètre	Description
Types de données (documents IOC) à analyser pendant l'analyse IOC	Les cases de la section **Avancés** ajoutent les types de données suivants (documents IOC) pour analyse lors d'une analyse IOC : • **Processus - ProcessItem**. • **Fichiers - FileItem**. • **Documents IOC**. Le lien vers les **documents IOC** est disponible si vous avez téléchargé un fichier IOC dans le panneau **Redéfinir les fichiers IOC**. En utilisant ce lien, vous pouvez accéder à la fenêtre **Paramètres d'analyse de fichiers – FileItem**, où vous pouvez ajouter des zones d'analyse. • **Tableaux ARP - ArpEntryItem**. • **Ports réseau - PortItem**. • **Comptes utilisateurs - UserItem**. • **Objets système - SystemItem**.
Rechercher des IOC dans les domaines suivants	La case active ou désactive l'analyse des zones suivantes : • **Fichiers sur tous les disques de l'appareil**. • **Fichiers sur les disques système de l'appareil**. • **Zones critiques sur l'appareil**. Cette option est sélectionnée par défaut. • **Ne pas analyser les zones prédéfinies**.
Analyser les zones indiqués	La case ajoute les zones répertoriées dans le tableau sous la case à la liste des zones d'analyse. Vous pouvez ajouter le chemin à la zone que vous souhaitez vérifier en cliquant sur le bouton **Ajouter**. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès à la zone dans le champ **Zone** et enregistrez les modifications. Vous pouvez supprimer une zone du tableau en cochant la case à côté de la zone à supprimer puis en cliquant sur le bouton **Supprimer**. Vous ne pouvez pas décocher la case si l'option **Ne pas analyser les zones prédéfinies** est sélectionnée dans la liste **Rechercher des IOC dans les domaines suivants**.

Il n'est pas recommandé d'ajouter ou de supprimer des fichiers IOC une fois la tâche démarrée. Cela peut entraîner un affichage incorrect des résultats de l'analyse IOC pour les exécutions des tâches précédentes. Pour rechercher des indicateurs de compromission dans les nouveaux fichiers IOC, il est recommandé de créer de nouvelles tâches.

Vous pouvez afficher le résultat de la tâche *Analyse IOC* dans les propriétés de la tâche dans Web Console dans la section **Paramètres de l'application → Résultats de l'analyse IOC**. Le tableau affiche une liste des appareils sur lesquels la tâche *Analyse IOC* a été exécutée, ainsi que les résultats de la tâche. Dans la liste déroulante **Appareil**, vous pouvez choisir l'affichage des résultats de la tâche pour tous les appareils gérés sur lesquels la tâche a été exécutée ou pour un appareil spécifique.

Le tableau contient les informations suivantes :

- **État** : état de détection des indicateurs de compromission, affiché sous forme d'icône.
- **Appareil** : nom de l'appareil sur lequel la tâche a été lancée.
- **Heure** : date et heure d'exécution de la tâche.
- **Résultats** : informations sur le résultat d'exécution de la tâche *Analyse IOC*. L'un des états suivants peut être affiché :
  - *IOC détecté* : affiché sous forme de lien qui, lorsque vous cliquez dessus, ouvre une fenêtre avec les détails de l'alerte ;
  - *Aucun IOC détecté*.

La période de conservation des résultats de l'analyse IOC est de 30 jours. Passé ce délai, Kaspersky Endpoint Security supprime automatiquement les anciens enregistrements.

Trouver des indicateurs de compromission dans la ligne de commande

Vous pouvez rechercher des indicateurs de compromission à l'aide de la tâche d'analyse IOC dans la ligne de commande uniquement lorsqu'elle est intégrée à Kaspersky Endpoint Detection and Response Optimum. Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec Kaspersky Endpoint Detection and Response (KATA), l'Analyse IOC est exécutée du côté de la solution Detection and Response correspondante.

Pour créer, configurer et exécuter la tâche Analyse IOC dans la ligne de commande, exécutez la commande suivante :

```
kesl-control [-T] --scan-ioc --path <chemin d'accès au répertoire ou au fichier> [--process on|off] [--hint <expression régulière>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <liste des exclusions>] [--scope <liste des répertoires>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

où :

- `--path <chemin d'accès au répertoire ou au fichier>` est le chemin d'accès au fichier IOC ou au répertoire contenant des fichiers IOC portant l'extension .IOC ou .XML, à utiliser pour effectuer l'analyse.

  Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces. Vous pouvez également spécifier les deux types de chemins (fichier et répertoire).

- `--process` : activation de l'analyse des processus en cours d'exécution sur l'appareil.

  Arguments possibles :

  - `on` : activer l'analyse des processus en cours d'exécution sur l'appareil (valeur par défaut).
  - `off` : désactiver l'analyse des processus en cours d'exécution sur l'appareil.

  Si vous n'indiquez pas la clé `--process`, l'application effectue une analyse de processus uniquement si le fichier IOC utilisé contient les données de processus (`ProcessItem`).

- `--hint <expression régulière>` est l'expression régulière qui correspond au chemin complet du fichier (`FileItem`) ou du fichier exécutable du processus (`ProcessItem`) à analyser.

  Vous pouvez utiliser les éléments d'expressions régulières suivants :

  - métacaractères : `. ^ $ |`
  - classes de caractères : chiffre, alpha, inférieur, supérieur, cntrl
  - quantificateurs : `* + ? {n} {n,} {n, m}`
  - négation : `[^a-c]`
  - caractères d'échappement : `\a \e \f`, `\n \r \t \v \b`

- `--arpentry` : activation de l'analyse des enregistrements dans la tableau ARP (`ArpEntryItem`).

  Arguments possibles :

  - `on` : activer l'analyse des enregistrements dans le tableau ARP (valeur par défaut).
  - `off` : désactiver l'analyse des enregistrements dans le tableau ARP.

  Si vous n'indiquez pas la clé `--arpentry`, l'application analyse la tableau ARP uniquement si le fichier IOC utilisé contient les données de la table (`ArpEntryItem`).

  `--ports` : activation de l'analyse des ports ouverts pour la connexion.

  Arguments possibles :

  - `on` : activer l'analyse des ports ouverts pour les connexions et vérifier les connexions actives sur l'appareil (valeur par défaut).
  - `off` : désactiver l'analyse des ports ouverts pour les connexions et ne pas vérifier les connexions actives sur l'appareil.

Si vous n'indiquez pas la clé `--ports`, l'application effectue une analyse de ports uniquement si le fichier IOC utilisé contient les données de ports (`PortItem`).

- `--system` : activation de l'analyse de l'environnement système.

  Arguments possibles :

  - `on` : activation de l'analyse de l'environnement système (valeur par défaut).
  - `off` : désactivation de l'analyse de l'environnement système.

  Si vous n'indiquez pas la clé `--system`, l'application effectue une analyse de l'environnement système uniquement si les informations sur l'environnement système (`SystemInfoItem`) sont spécifiées dans le fichier IOC utilisé.

- `--files` : activation de l'analyse des fichiers.

  Arguments possibles :

  - `on` : activation de l'analyse des fichiers (valeur par défaut).
  - `off` : désactivation de l'analyse des fichiers.

  Si vous n'indiquez pas la clé `--files`, l'application effectue une analyse de fichiers uniquement si le fichier IOC utilisé contient les données de fichiers (`FileItem`).

- `--drives` : zones à analyser.

  Arguments possibles :

  - `all` : analyser toutes les zones de fichiers disponibles.
  - `system` : analyser tous les fichiers du système de fichiers racine.
  - `critical` : analyser les fichiers dans les répertoires utilisateur et système (valeur par défaut).
  - `custom` : analyser uniquement les fichiers dans les zones que vous spécifiez.

  Si vous ne spécifiez pas la clé `--drives`, l'application analyse les fichiers dans les répertoires utilisateur et système.

- `--excludes <liste des exclusions>` est la liste des chemins exclus des analyses.

  Les exclusions spécifiées par cette clé sont globales et s'appliquent quel que soit le type de zone ou de liste de répertoires. Ces exclusions ont la priorité sur les autres options de ligne de commande, notamment `--hint` et `--scope`.

  > Les exclusions sont spécifiées sous forme de chemins, mais ne peuvent pas contenir des éléments récursifs ni de caractères de masque (par exemple, `*`).

  Si vous ne spécifiez pas la clé `--excludes`, l'analyse est effectuée sans exclusion.

  Vous pouvez spécifier plusieurs exclusions, séparées par des espaces.

- `--scope <liste des répertoires>` est la liste des répertoires supplémentaires à analyser.

  Cette option est obligatoire si vous avez spécifié l'argument `--drives` pour l'option `custom`.

- `--action` : action effectuée lorsque des indicateurs de compromission sont détectés.

  Arguments possibles :

  - `Skip` : l'application n'effectuera aucune action avec l'objet détecté, mais les informations le concernant seront enregistrées dans les résultats de la tâche (valeur par défaut).
  - `QuarantineFile` : l'application mettra en quarantaine l'objet détecté.
  - `IsolateHost` : l'application isole du réseau l'appareil sur lequel l'objet est détecté.
  - `ScanCriticalAreas` : l'application analysera les **zones critiques**.
    - /lib/systemd
    - /lib/udev
    - /lib/dbus-1.0
    - /usr/local/lib/systemd/user
    - /usr/share/dbus-1
    - /usr/share/gdm/autostart
    - /usr/share/gnome/autostart
    - /var/spool/at
    - /var/spool/at/spool
    - /var/spool/anacron
    - /var/spool/cron
    - /boot
    - /bin
    - /sbin
    - /lib
    - /lib32
    - /lib64
    - /libx32
    - /usr/lib

- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Vous pouvez spécifier plusieurs actions séparées par des espaces.

> Si vous avez spécifié l'argument `Skip`, vous n'avez pas besoin d'ajouter d'autres arguments. L'argument `Skip` ne peut être utilisé que de manière indépendante.

Exigences pour les 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 l'extension .IOC et .XML du standard ouvert pour décrire les indicateurs de compromission OpenIOC versions 1.0 et 1.1.
- Les erreurs sémantiques et les termes et tags IOC non pris en charge dans les fichiers IOC ne provoquent pas d'erreurs d'exécution de la tâche. Dans ces sections des fichiers IOC, l'application enregistre l'absence de concordance.
- Les identifiants de tous les fichiers IOC utilisés dans une seule tâche d'analyse IOC 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.
- Il est recommandé de créer un fichier IOC pour chaque menace. Cela facilite la lecture des résultats de la tâche *Analyse IOC*.

Le fichier, qui peut être téléchargé à partir du lien ci-dessous, contient un tableau avec une liste complète des termes IOC de la norme OpenIOC.

TÉLÉCHARGER LE FICHIER IOC TERMS.XLSX

Les fonctionnalités et limitations de la prise en charge des applications pour la norme OpenIOC sont présentées dans le tableau ci-dessous.

Fonctionnalités et limitations de la prise en charge des versions 1.0 et 1.1 du standard OpenIOC.

Conditions prises en charge	OpenIOC 1.0 : • `is` • `isnot` (à titre d'exclusion parmi les nombreux) • `contains` • `containsnot` (à titre d'exclusion parmi les nombreux) OpenIOC 1.1 : • `is` • `contains` • `starts-with` • `ends-with` • `matches` • `greater-than` • `less-than`
Attributs des conditions prises 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"` : nombre entier (conditions applicables : `is`, `greater-than`, `less-than`) `"string"` : ligne (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"`, `"base64Binary"` sont interprétés comme une ligne (string).
	L'application prend en charge l'interprétation du paramètre `Content` pour les types de données `int` et `date`, spécifiés 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 de 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 spécifiés au format `ISO 8601, Zulu time zone, UTC`.

Prévention de l'exécution des objets

Lorsqu'il est intégré avec les solutions Detection and Response dans le cadre d'une action de réponse aux menaces, l'application Kaspersky Endpoint Security peut contrôler le lancement de fichiers exécutables et de scripts, ainsi que l'ouverture de fichiers des applications office sur l'appareil. La prevention de lancement des objets prend en charge un ensemble spécifique d'extensions des fichiers des applications Office et un ensemble spécifique d'interpréteurs de script. Suite à la prévention du lancement des objets, la propagation de la menace peut être stoppée.

La prévention du lancement des objets fonctionne sur la base des règles d'interdiction de démarrage. Une *règle d'interdiction de démarrage* est un ensemble de critères que l'application Kaspersky Endpoint Security prend en compte lorsqu'elle répond au démarrage d'un objet. Un objet doit répondre à tous les critères d'une règle d'interdiction de démarrage pour que l'application bloque son exécution. 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.

La fonctionnalité de prévention du lancement des objets est disponible dans l'application Kaspersky Endpoint Security si l'une des conditions suivantes est remplie :

- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et le module EDR Optimum est activé.
- L'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) ou avec le module Kaspersky Endpoint Detection and Response (KATA) est activée, et le module EDR Expert (on-premise) est activé.

Si le mode de blocage de l'interception des opérations sur les fichiers n'est pas activé, la prévention du lancement des objets fonctionne en mode de notification, quel que soit le mode de fonctionnement défini.

Par défaut, la prévention du lancement des objets est désactivée.

L'activation de la prévention du lancement des objets peut affecter la vitesse de lancement des applications dans le système d'exploitation.

Pour que la prévention du lancement des objets fonctionne, vous devez activer l'application des règles de prévention du lancement des objets.

Fonctionnalités de la prévention du lancement des objets lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou Kaspersky Endpoint Detection and Response (KATA)

Lors de l'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou avec le module Kaspersky Endpoint Detection and Response (KATA), l'application utilise les *règles de la prévention du lancement des objets du module Endpoint Detection and Response Expert (on-premises)*. L'application reçoit ces règles de Kaspersky Endpoint Detection and Response Expert (on-premises) ou de Kaspersky Endpoint Detection and Response (KATA).

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou Kaspersky Endpoint Detection and Response (KATA), vous pouvez :

- Activer ou désactiver l'application des règles de prévention du lancement des objets du module EDR Expert (on-premises) dans Web Console, dans la Console d'administration ou dans la ligne de commande.

  Lorsqu'une règle de la prévention du lancement est déclenchée, Kaspersky Endpoint Security envoie un rapport à Kaspersky Endpoint Detection and Response Expert (on-premises) ou à Kaspersky Anti Targeted Attack Platform. Pour plus de détails, consultez l'aide de la solution correspondante.

- Afficher dans ligne de commande la liste des règles de la prévention du lancement des objets du module EDR Expert (on-premises).

Fonctionnalités de la prévention du lancement des objets lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum

Lors de l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Endpoint Detection and Response (KATA), l'application utilise les *règles de la prévention du lancement des objets du module EDR Optimum*. Vous créez ces règles manuellement dans Web Console. Vous pouvez également créer des règles de la prévention du lancement automatiquement à partir de la fenêtre des détails de l'alerte.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez :

- Activer ou désactiver l'application des règles de prévention du lancement des objets du module EDR Optimum dans Web Console ou dans la ligne de commande.
- Créer et configurer des règles de prévention du lancement des objets du module EDR Optimum dans Web Console.

  Vous pouvez également créer une règle de la prévention du lancement de l'objet automatiquement en interdisant le lancement d'un fichier dans la fenêtre des détails de l'alerte. La règle de la prévention du lancement sera ajoutée à la stratégie du groupe d'administration auquel appartient l'appareil.

  > Vous pouvez bloquer l'exécution des fichiers dans la fenêtre des détails de l'alerte uniquement si l'appareil est couvert par une stratégie.

- Afficher dans ligne de commande la liste des règles de la prévention du lancement des objets du module DR Optimum.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response Optimum, la prévention du lancement des objets peut fonctionner selon l'un des deux modes suivants :

- **Bloquer**. Dans ce mode, l'application bloque le lancement des objets ou l'ouverture de documents répondant aux critères des règles de refus, et enregistre un événement dans le journal concernant les tentatives de lancement des objets ou d'ouverture de documents.

  > L'application Kaspersky Endpoint Security bloque l'exécution d'un script interdit par la règle de prévention du lancement, même s'il est importé par un script autorisé.

- **Informer**. Dans ce mode, l'application enregistre dans le journal un événement relatif aux tentatives de lancement des objets exécutables ou d'ouverture de documents répondant aux critères des règles de refus, mais ne bloque pas leur lancement ou leur ouverture. Ce mode est sélectionné par défaut.

Limites de prévention du lancement des objets

Les restrictions suivantes existent pour empêcher le lancement des objets :

- Kaspersky Endpoint Security ne bloque pas les objets spécifiés dans les règles de prévention du lancement avant le lancement de l'application.
- Kaspersky Endpoint Security ne bloque pas les fichiers ouverts avant la création ou la modification de la règle de prévention du lancement.

- L'application Kaspersky Endpoint Security ne bloque pas le travail avec les objets qui ont été lancés avant la création ou la modification de la règle de prévention du lancement et qui relèvent des règles nouvellement définies.
- Certains fichiers peuvent être critiques pour le fonctionnement du système d'exploitation et de l'application. Prévention de lancement de tels fichiers peut perturber le fonctionnement du système.
- Il n'est pas recommandé de créer plus de 50000 règles de démarrage car cela pourrait entraîner une instabilité du système.

Configurer la prévention du lancement des objets dans Web Console

Configuration de la prevention du lancement des objets EDR Expert (on-premise).

Si l'intégration avec la solution Kaspersky Endpoint Detection and Response Expert (on-premise) ou le module Kaspersky Endpoint Detection and Response (KATA) est activée, vous pouvez activer ou désactiver la prévention de l'exécution des objets dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Endpoint Detection and Response Expert (on-premise)**).

Le commutateur **Prévention du lancement** active ou désactive l'application de règles de prévention du lancement des objets du module EDR Expert (on-premise).

Configuration de la prévention du lancement des objets EDR Optimum

Si l'intégration avec Kaspersky Endpoint Detection and Response Optimum est activée, vous pouvez activer et désactiver la prévention du lancement des objets et configurer les règles de prévention du lancement des objets du module EDR Optimum :

- dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Endpoint Detection and Response**) ;
- Dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Detection and Response** → **Endpoint Detection and Response Optimum**).

L'activation et la désactivation de la prévention du lancement des objets dans les propriétés de l'appareil ne sont pas disponibles si l'appareil est couvert par une stratégie.

Paramètres de la prévention du lancement des objets EDR Optimum dans les propriétés de l'appareil

Paramètre	Description
La prévention du lancement des objets est activée/désactivée	Active ou désactive l'application de règles de prévention du lancement des objets du module EDR Optimum. Par défaut, l'application des règles est désactivée.
Action lors du démarrage ou de l'ouverture d'un objet	Vous pouvez sélectionner le mode de fonctionnement de la prevention du lancement des objets : • **Bloquer**. Dans ce mode, l'application bloque le lancement des objets ou l'ouverture de documents répondant aux critères des règles de refus, et enregistre dans le journal des événements un événement concernant les tentatives de lancement des objets ou d'ouverture de documents. • **Informer**. Dans ce mode, l'application enregistre dans le journal des événements un événement relatif aux tentatives de lancement des objets exécutables ou d'ouverture de documents répondant aux critères des règles de refus, mais ne bloque pas leur lancement ou leur ouverture. Ce mode est sélectionné par défaut.
Liste des règles de prévention du lancement des objets	Le lien **Ajouter** ouvre une fenêtre dans laquelle vous pouvez configurer une règle de prévention du lancement des objets du module EDR Optimum. Si nécessaire, vous pouvez supprimer une règle de la liste à l'aide du bouton **Supprimer**.

Pour ajouter à la liste une règle de prévention du lancement des objets du module EDR Optimum dans les propriétés de l'appareil :

1. Cliquez sur le bouton **Ajouter** situé au-dessus de la liste des règles de prévention du lancement des objets.
2. Dans la fenêtre qui s'ouvre, saisissez le nom de prévention de lancement.
3. Spécifiez l'état de fonctionnement de la règle de prévention du lancement en plaçant le commutateur sur la position appropriée :
   - **Activée** : la règle est activée, l'application applique cette règle pendant le fonctionnement.
   - **Inactif** : la règle est désactivée et n'est pas prise en compte lors du fonctionnement de l'application.

   Vous pouvez activer ou désactiver la règle créée à tout moment.
4. Dans la liste déroulante **Type**, sélectionnez le type d'objet que vous souhaitez bloquer :
   - **Fichier exécutable**.
   - **Script**.
   - **Fichier de l'application Office**.

   Si vous sélectionnez le mauvais type d'objet, l'application ne bloquera pas le fichier ou le script.
5. Pour ajouter un objet, spécifiez le chemin d'accès à l'objet et/ou la somme de contrôle de l'objet.

   Pour spécifier le chemin d'accès à l'objet, sélectionnez **Utiliser le chemin** et saisissez le chemin d'accès à l'objet.

   Pour spécifier une somme de contrôle d'objet, sélectionnez l'option **SHA256** ou **MD5** et saisissez la somme de contrôle de l'objet.
6. Cliquez sur le bouton **OK**.

   La règle créée est ajoutée à la liste des règles dans le groupe de paramètres **Prévention du lancement des objets**.

Configuration de la prévention du lancement des objets dans la Console d'administration

Vous pouvez activer ou désactiver la prévention du lancement des objets dans la Console d'administration uniquement si l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premises) ou Kaspersky Endpoint Detection and Response (KATA) est activée.

Vous pouvez activer ou désactiver la prévention de l'exécution pour les objets dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres de l'application → Detection and Response → EDR Expert (on-premise)**).

La case **Activer la prévention du lancement des objets** dans le groupe des paramètres **Prévention du lancement des objets** active ou désactive l'application des règles de prévention du lancement des objets du module EDR Expert (on-premises).

Contrôler la prévention du lancement des objets dans la ligne de commande

Dans la ligne de commande, vous pouvez démarrer et arrêter l'application des règles de prévention du lancement des objets à l'aide des tâches prédéfinies suivantes :

- *Prevention du lancement des objets (EDR Expert (on-premise))* (*KATAEDR_Prevention*).
- *Prévention du lancement des objets* (*EDRO_Prevention*).

Par défaut, les tâches *Prévention du lancement des objets (EDR Expert (on-premise))* et *Prévention du lancement des objets (EDR Optimum)* ne sont pas lancées. Vous pouvez démarrer et arrêter ces tâches manuellement.

Vous pouvez lancer la tâche *Prévention du lancement des objets (EDR Expert (on-premise))* uniquement si l'intégration avec Kaspersky Endpoint Detection and Response Expert (on-premise) ou Kaspersky Endpoint Detection and Response (KATA) est activée.

Vous pouvez exécuter la tâche *Prévention du lancement des objets (EDR Optimum)* uniquement si l'intégration avec Kaspersky Endpoint Detection and Response Optimum est activée.

À l'aide des commandes d'administration des règles de prévention du lancement des objets, vous pouvez consulter la liste des règles de prévention du lancement des objets du module EDR Expert (on-premise) et des règles de prévention du lancement des objets du module EDR Optimum.

Pour afficher la liste des règles de prévention du lancement des objets du module EDR Expert (on-premise), exécutez la commande suivante :

```
kesl-control [-T] --get-prevention-state --kata
```

Pour afficher la liste des règles de prévention du lancement des objets du module EDR Optimum, exécutez la commande suivante :

```
kesl-control [-T] --get-prevention-state --edro
```

Cloud Sandbox

Cloud Sandbox est une technologie qui vous permet de détecter des menaces complexes sur votre appareil. Kaspersky Endpoint Security envoie automatiquement les fichiers détectés à Cloud Sandbox pour analyse. Cloud Sandbox exécute ces fichiers dans un environnement isolé pour détecter les activités malveillantes et prend des décisions concernant la réputation de ces fichiers. Ensuite, les données sur ces fichiers sont transmises à Kaspersky Security Network. Ainsi, si Cloud Sandbox détecte un fichier malveillant, l'application Kaspersky Endpoint Security prendra des mesures pour éliminer la menace sur tous les appareils sur lesquels ce fichier est détecté.

Pour que Cloud Sandbox fonctionne, vous devez activer Kaspersky Security Network.

Si vous utilisez Kaspersky Private Security Network, la technologie Cloud Sandbox n'est pas disponible.

La technologie Cloud Sandbox est toujours activée et disponible pour tous les utilisateurs de Kaspersky Security Network, quel que soit le type de licence que vous utilisez.

Si Kaspersky Endpoint Detection and Response Optimum est déployé, vous pouvez activer un compteur distinct dans Web Console pour les menaces détectées à l'aide de Cloud Sandbox :

- dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Endpoint Detection and Response**) ;
- Dans les propriétés de l'appareil administré (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Applications** → lien <nom de l'application Kaspersky Endpoint Security> → onglet **Paramètres de l'application** → section **Detection and Response** → **Endpoint Detection and Response Optimum**).

En outre, le nombre de menaces détectées par Cloud Sandbox est affiché dans les rapports de l'interface utilisateur graphique. Vous pouvez utiliser ce compteur pour compiler des statistiques lors de l'analyse des menaces détectées.

Pour activer le compteur Cloud Sandbox dans Web Console dans les propriétés de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Stratégies et profils de stratégies**.

   La liste des stratégies s'ouvre.

2. Sélectionnez le groupe d'administration contenant l'appareil dont vous avez besoin. Pour cela, cliquez sur le lien dans le champ **Chemin actuel** situé au dessus de la liste des appareils administrés et sélectionnez un groupe d'administration dans la fenêtre qui s'ouvre.

   Seuls les appareils administrés du groupe d'administration sélectionné seront affichés dans la liste.

3. Recherchez l'appareil dont vous avez besoin dans la liste et cliquez sur son nom.

4. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

5. Dans la liste des applications installées sur l'appareil, cliquez sur le nom de l'application Kaspersky Endpoint Security.

6. Dans la fenêtre des propriétés de l'application qui s'ouvre, sous l'onglet **Paramètres de l'application**, sélectionnez la section **Detection and Response** et cliquez sur le lien **Endpoint Detection and Response Optimum**.

7. Dans fenêtre ouverte, dans le groupe de paramètres **Cloud Sandbox**, activez le commutateur **Cloud Sandbox**.

8. Cliquez sur le bouton **OK**.

Intégration avec Kaspersky Unified Monitoring and Analysis Platform

L'application Kaspersky Endpoint Security est compatible avec la solution Kaspersky Unified Monitoring and Analysis Platform (ci-après également KUMA).

Kaspersky Unified Monitoring and Analysis Platform est une solution logicielle complète qui combine les fonctionnalités suivantes :

- recevoir, traiter et stocker des événements de sécurité des informations (télémétrie) ;
- analyse et corrélation des données entrantes ;
- recherche par événements reçus ;
- créer des notifications sur l'identification des signes de menaces pour la sécurité des informations.

Pour plus d'informations sur la solution, consultez l'aide de Kaspersky Unified Monitoring and Analysis Platform.

Lors de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform, les appareils dotés de Kaspersky Endpoint Security établissent des connexions sécurisées avec le serveur KUMA. Les certificats suivants émis par le serveur KUMA sont utilisés pour sécuriser la connexion :

- Certificat du serveur Sandbox. La connexion est chiffrée à l'aide du certificat TLS du serveur. Vous pouvez augmenter le niveau de sécurité de la connexion en activant la vérification du certificat du serveur du côté de Kaspersky Endpoint Security. Pour ce faire, vous devez ajouter le certificat du serveur KUMA avant d'activer l'intégration avec Kaspersky Unified Monitoring and Analysis Platform.

- Certificat client. Ce certificat est utilisé pour sécuriser davantage la connexion avec une vérification en deux étapes (analyse des appareils avec Kaspersky Endpoint Security par le serveur KUMA). Le même certificat client peut être utilisé par plusieurs appareils. Par défaut, le serveur KUMA n'effectue pas la validation du certificat client, mais la vérification en deux étapes peut être activée du côté de Kaspersky Unified Monitoring and Analysis Platform. Dans ce cas, vous devez activer la vérification en deux étapes dans les paramètres de l'intégration avec Kaspersky Unified Monitoring and Analysis Platform et ajouter un certificat client (cryptoconteneur avec le certificat et la clé privée).

Les certificats permettant de sécuriser la connexion au serveur KUMA sont fournis par l'administrateur de Kaspersky Unified Monitoring and Analysis Platform.

Un serveur proxy est utilisé pour se connecter au serveur KUMA si l'utilisation d'un serveur proxy est configurée dans les paramètres généraux de l'application Kaspersky Endpoint Security.

Par défaut, l'intégration avec Kaspersky Unified Monitoring and Analysis Platform est désactivée. Vous pouvez activer et désactiver l'intégration et configurer les paramètres d'intégration suivants à l'aide de la ligne de commande, de Web Console et de la Console d'administration :

- Configurer les paramètres généraux de connexion aux serveurs KUMA.
- Ajouter et supprimer des certificats de serveur KUMA.
- Configurer la vérification en deux étapes lors de la connexion aux serveurs KUMA et ajoutez des certificats clients.
- Configurer les paramètres de transmission des événements.

Avant d'activer l'intégration avec Kaspersky Unified Monitoring and Analysis Platform, assurez-vous que l'une des conditions suivantes est remplie :

- Vous utilisez l'application Kaspersky Endpoint Security sous une licence qui inclut les fonctionnalités de Kaspersky Unified Monitoring and Analysis Platform.
- Vous avez acheté une licence distincte pour utiliser les fonctionnalités de Kaspersky Unified Monitoring and Analysis Platform et ajouté une clé de licence pour des fonctionnalités supplémentaires (clé KUMA) à l'application.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'activation est effectuée du côté du Serveur de protection (un module de la solution Kaspersky Security for Virtualization Light Agent) en ajoutant des clés de licence à la SVM.

Configuration de l'intégration avec KUMA dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'intégration de l'application avec Kaspersky Unified Monitoring and Analysis Platform dans les propriétés de la stratégie (**Paramètres de l'application** → **Configuration des agents intégrés** → **Intégration KUMA**).

Configuration de l'intégration avec KUMA dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver l'intégration de Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform et gérer les paramètres d'intégration dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Intégration KUMA** → **Intégration KUMA**).

Paramètre	Description
Activer l'intégration avec KUMA	Active ou désactive l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Unified Monitoring and Analysis Platform. Par défaut, l'intégration avec KUMA est désactivée.
Utiliser une connexion chiffrée	La case active ou désactive l'utilisation de l'analyse du certificat du serveur pour sécuriser davantage la connexion au serveur KUMA. Pour vérifier le certificat du serveur, vous devez cocher cette case et ajouter le certificat du serveur dans la fenêtre **Serveur KUMA**. La case est décochée par défaut.
Serveurs KUMA	Le bouton **Configurer** ouvre la fenêtre **Serveurs KUMA**. Cette fenêtre permet de configurer la connexion aux serveurs KUMA, ainsi que visualiser la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion au serveur KUMA	Cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Paramètres de connexion au serveur** dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs KUMA, ajouter un certificat du serveur et configurer la vérification en deux étapes lors de la connexion aux serveurs KUMA.
Durée d'attente maximale pour l'envoi des événements (en secondes)	Délai maximum en secondes pour l'envoi des événements au serveur KUMA. Valeur par défaut : `30`.

Fenêtre Serveurs KUMA

Cette fenêtre affiche le tableau contenant les paramètres de connexion aux serveurs KUMA. Pour chaque serveur auquel une connexion est configurée, le tableau indique :

- L'adresse IP (IPv4 ou IPv6) ou le nom de domaine complet (FQDN) du serveur. Si dans la fenêtre de configuration de l'intégration avec KUMA, vous avez cochez la case **Utiliser une connexion chiffrée**, vous devez spécifier le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat d'une licence pour utiliser KUMA.
- Port de connexion au serveur KUMA.
- Le protocole utilisé pour se connecter au serveur KUMA.

Les boutons et le menu au-dessus du tableau permettent de réaliser les actions suivantes :

- Ajouter des paramètres de connexion au serveur KUMA.
- Modifier ou supprimer les paramètres de connexion configurés.
- Exporter ou importer une liste de paramètres de connexion configurés.

Fenêtre Serveur KUMA

Dans cette fenêtre, vous pouvez spécifier les paramètres de connexion au serveur KUMA.

Paramètres de connexion au serveur KUMA

Paramètre	Description
Adresse	Vous pouvez spécifier l'adresse du serveur KUMA, l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Si dans la fenêtre de configuration de l'intégration avec KUMA, vous avez coché la case **Utiliser une connexion chiffrée**, vous devez spécifier le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat d'une licence pour utiliser KUMA.
Port	Port de connexion au serveur KUMA. Valeur par défaut : `443`.
Protocole.	Protocole de connexion au serveur KUMA : TCP ou UPD. Lorsque vous sélectionnez le protocole UDP, l'utilisation de certificats pour la sécurité de la connexion n'est pas prise en charge et il n'y a aucun événement de connexion avec le serveur KUMA. Valeur par défaut : TCP.

Fenêtre Paramètres de connexion aux serveurs KUMA

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs KUMA.

Paramètres de connexion au serveur KUMA

Paramètre	Description
Durée d'attente maximale de la connexion au serveur (en secondes)	Durée maximale d'attente de la demande de connexion au serveur KUMA en secondes. Valeur par défaut : `5`.
Certificat de serveur	Le groupe de paramètres contient des boutons permettant d'ajouter et de supprimer un certificat du serveur.
Ajouter (certificat du serveur)	Ouvre la fenêtre d'ajout de certificat du serveur. Le bouton s'affiche si le certificat du serveur n'a pas encore été ajouté.
Supprimer (certificat du serveur)	Supprime le certificat du serveur. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.
Paramètres de la protection avancée	Le groupe de paramètres contient des éléments de l'interface permettant de configurer une sécurité de connexion supplémentaire à l'aide de la vérification en deux étapes.
Utiliser la vérification en deux étapes	La case active ou désactive l'utilisation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client. L'authentification bidirectionnelle doit être activée du côté du serveur KUMA.
Ajouter (certificat client)	Ouvre la fenêtre d'ajout d'un certificat client pour sécuriser la connexion au serveur KUMA. Le bouton s'affiche si le certificat client n'a pas encore été ajouté. Si vous souhaitez renforcer la sécurité de connexion, vous devez activer la validation des certificats client du côté du serveur KUMA et cocher la case **Utiliser la vérification en deux étapes** dans cette fenêtre.
Supprimer (certificat client)	Supprime le certificat client. Le bouton s'affiche uniquement si le certificat client a été ajouté.
Utiliser la vérification en deux étapes	Active ou désactive l'utilisation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client. L'authentification bidirectionnelle doit être activée du côté du serveur KUMA.

Fenêtre d'ajout d'un certificat de serveur

Cette fenêtre permet d'ajouter un certificat du serveur KUMA de l'une des manières suivantes :

- Indiquer le chemin d'accès au fichier de certificat dans le champ **Ajouter à partir d'un fichier**. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Indiquer le chemin d'accès à un fichier contenant un certificat au format DER ou PEM.
- Copiez le contenu du fichier de certificat dans le champ **Saisir les détails du certificat**.

Si un certificat serveur a été ajouté, ce certificat est vérifié côté Kaspersky Endpoint Security. Cela renforce la sécurité de la connexion.

Fenêtre d'ajout d'un certificat client

Cette fenêtre permet d'ajouter un certificat client pour sécuriser davantage la connexion au serveur KUMA.

> Si vous souhaitez renforcer la sécurité de connexion, vous devez activer la validation des certificats client du côté du serveur KUMA et cocher la case **Utiliser la vérification en deux étapes** dans la fenêtre **Paramètres de connexion aux serveurs KUMA**.

Pour ajouter un certificat client, indiquez le chemin d'accès au cryptocontainer (archive au format PFX) contenant le certificat client et la clé privée. Le bouton **Parcourir** ouvre une fenêtre standard de sélection de fichier. Si l'archive est protégée par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe de conteneur de chiffrement**.

Configuration de l'intégration avec KUMA dans la ligne de commande

À partir de la ligne de commande, vous pouvez gérer l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform à l'aide de la tâche prédéfinie *Intégration avec Kaspersky Unified Monitoring and Analysis Platform* .

Par défaut, la tâche *Intégration avec Kaspersky Unified Monitoring and Analysis Platform* n'est pas lancée. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Unified Monitoring and Analysis Platform en modifiant les paramètres d'une tâche prédéfinie.

À l'aide des commandes de gestion des paramètres d'intégration avec Kaspersky Unified Monitoring and Analysis Platform, vous pouvez gérer les certificats utilisés pour se connecter aux serveurs KUMA.

Paramètres de la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform

Le tableau ci-dessous décrit tous les paramètres et valeurs disponibles par défaut pour tous les paramètres que vous pouvez définir pour la tâche *Intégration à Kaspersky Endpoint Detection and Response (KATA)*.

Paramètres de la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform

Paramètre	Description	Valeur
`UseTls`	Activation ou désactivation de l'analyse du certificat du serveur pour sécuriser davantage la connexion au serveur KUMA.	`Yes` : utiliser le certificat pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser le certificat pour sécuriser la connexion au serveur KUMA.
`UseClientCertificate`	Activation et désactivation de la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. Si l'analyse du certificat client est activée du côté serveur KUMA, vous devez activer l'utilisation du certificat client et ajouter le certificat client avant d'exécuter la tâche Intégration avec Kaspersky Unified Monitoring and Analysis Platform.	`Yes` : utiliser la vérification en deux étapes pour sécuriser davantage la connexion au serveur KUMA. `No` (valeur par défaut) : ne pas utiliser la vérification en deux étapes.
`ConnectionTimeout`	Durée maximale d'attente de la demande de connexion au serveur KUMA en secondes.	Valeur par défaut : `5`.
La section **[Servers.item_#]** contient les paramètres du serveur KUMA.		
`ServerAddress`	Adresse du serveur KUMA. Vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) ou le nom de domaine entièrement qualifié (FQDN) du serveur. Si vous définissez `UseTls=Yes`, vous devez fournir le nom de domaine complet (FQDN) du serveur à partir du certificat que vous avez reçu lors de l'achat de votre licence KUMA.	Valeur par défaut : `127.0.0.1`.
`ServerPort`	Port de connexion au serveur KUMA.	Valeur par défaut : `443`.
`ServerProtocol`	Protocole pour se connecter au serveur KUMA.	`tcp` (valeur par défaut) : utiliser le protocole TCP pour la connexion au serveur KUMA. `udp` : utiliser le protocole UPD pour la connexion au serveur KUMA. Lorsque le protocole UDP est sélectionné, l'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge (les valeurs des paramètres `UseTls`, `UseClientCertificate` et `ConnectionTimeout` sont ignorées), et il n'y a aucun événement concernant la connexion au serveur KUMA.
La section **[SiemTransferSettings]** contient des paramètres permettant de transférer des événements vers le serveur KUMA.		
`EventTransferTimeMax`	Délai maximum en secondes pour l'envoi des événements au serveur KUMA.	Valeur par défaut : `30`.

Gestion des certificats pour la connexion au serveur KUMA

Lorsque le protocole UDP est sélectionné, l'utilisation de certificats pour sécuriser la connexion n'est pas prise en charge.

Pour gérer les certificats, des droits d'utilisateur avec le rôle Administrateur sont requis.

Vous pouvez utiliser des commandes pour gérer les certificats utilisés pour la connexion au serveur KUMA. Vous pouvez effectuer les opérations suivantes avec les certificats :

- ajouter ou remplacer un certificat du serveur ;
- afficher des informations sur un certificat de serveur ;
- supprimer le certificat du serveur ;
- ajouter ou remplacer un certificat client ;
- afficher des informations sur le certificat client ;
- supprimer le certificat client.

Pour ajouter ou modifier un certificat client, exécutez la commande suivante :

```
kesl-control [-M] --add-kuma-server-certificate <chemin d'accès au fichier>
```

où <chemin d'accès au fichier> est le chemin d'accès au fichier DER ou PEM contenant le certificat du serveur.

Pour ajouter ou remplacer un certificat client :

1. Exécutez la commande :

   ```
   kesl-control [-M] --add-kuma-client-certificate <chemin d'accès au fichier>
   ```

   où <chemin d'accès au fichier> est le chemin d'accès au conteneur cryptographique (archive PFX) contenant le certificat client et la clé privée.

2. Si le cryptocontainer est protégé par un mot de passe, saisissez le mot de passe à l'invite.

Le certificat client est utilisé pour assurer une protection supplémentaire de la connexion au serveur KUMA si la vérification du certificat client est activée dans les paramètres du serveur KUMA et si, dans les paramètres de la tâche *Intégration avec Kaspersky Unified Monitoring and Analysis Platform*, le paramètre `UseClientCertificate` est défini sur `yes`.

Pour afficher les informations relatives au certificat, exécutez la commande suivante :

- pour le certificat du serveur :

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- pour le certificat client :

  ```
  kesl-control [-M] --query-kuma-client-certificate
  ```

La commande fournit les informations suivantes sur le certificat :

- Numéro de série du certificat
- Objet du certificat
- Émetteur de certificat
- Date de début de validité du certificat
- Date de fin de validité du certificat
- Empreintes des certificats SHA1 et SHA256.

Pour supprimer un certificat du serveur, exécutez la commande suivante :

```
kesl-control [-M] --remove-kuma-server-certificate
```

Pour supprimer un certificat client, exécutez la commande suivante :

```
kesl-control [-M] --remove-kuma-client-certificate
```

Configuration des paramètres d'utilisation de l'application en mode Light Agent

Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Pour faire fonctionner l'application Kaspersky Endpoint Security en mode Light Agent, une interaction constante entre le Light Agent et le Serveur de protection installé sur la SVM est requise. S'il n'y a pas de connexion au serveur de protection, le Light Agent ne peut pas transférer les fragments de fichiers au serveur de protection pour analyse ; l'analyse n'est pas effectuée.

Pour interagir avec le Serveur de protection, le Light Agent établit et maintient une connexion avec la SVM sur laquelle ce Serveur de protection est installé.

Vous pouvez configurer les paramètres de connexion du Light Agent à la SVM dans Web Console ou dans la Console d'administration. Les paramètres ne sont pas disponibles sur la ligne de commande, vous pouvez uniquement consulter les informations sur l'utilisation de l'application en mode Light Agent.

Vous pouvez configurer les paramètres suivants pour connecter le Light Agent à SVM :

- Mode de détection de la SVM. Vous pouvez choisir le mode qui sera utilisé par les Light Agents pour découvrir les SVM disponibles auxquelles se connecter. Le Light Agent peut découvrir les SVM exécutées sur le réseau de l'une des manières suivantes :

  - À l'aide du Serveur d'intégration. Les SVM transmettent des informations les concernant au serveur d'intégration. Le serveur d'intégration génère une liste de SVM disponibles pour la connexion et la fournit aux Light Agents.

    Pour utiliser ce mode de détection de la SVM, la SVM et les Light Agents doivent être connectés au Serveur d'intégration.

    Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

  - Utilisation de la liste d'adresses SVM. Vous pouvez spécifier une liste d'adresses SVM auxquelles les Light Agents peuvent se connecter.

- Algorithme de sélection des SVM pour la connexion. Après avoir reçu des informations sur les SVM disponibles, le Light Agent sélectionne la SVM optimale pour la connexion conformément à l'algorithme de sélection de SVM. Vous pouvez spécifier quel algorithme les Light Agents doivent utiliser lors du choix d'une SVM à laquelle se connecter.

- Tags pour la connexion. Vous pouvez réguler la connexion des Light Agents au SVM à l'aide de tags de connexion. Si vous utilisez des tags de connexion, Light Agent peut uniquement se connecter aux SVM configurées pour utiliser ce tag de connexion.

- Protection de connexion entre le Light Agent et le Serveur de protection. Vous pouvez protéger la connexion entre les Light Agents et les Serveurs de Protection à l'aide du chiffrement.

Pour plus d'informations sur les paramètres de connexion du Light Agent à la SVM, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Configuration des paramètres du Light Agent dans Web Console

Dans la Web Console, vous pouvez gérer les paramètres de connexion du Light Agent aux SVM dans les propriétés de la stratégie (**Paramètres de l'application** → **Mode Light Agent**).

Configuration des paramètres du Light Agent dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de connexion du Light Agent aux SVM dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Mode Light Agent**).

Connexion au serveur d'intégration

> Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Une connexion au Serveur d'intégration est requise si vous souhaitez que les Light Agents reçoivent des informations sur la SVM via le Serveur d'intégration, ou si vous souhaitez sécuriser la connexion entre le Serveur de sécurité et le Light Agent.

Cette fenêtre affiche les paramètres actuels de connexion des Light Agents au Serveur d'intégration : adresse et port de connexion. En cliquant sur le bouton **Modifier**, la fenêtre **Connexion au serveur d'intégration** s'ouvre, dans laquelle vous pouvez configurer la connexion au Serveur d'intégration.

Fenêtre Connexion au serveur d'intégration

Dans cette fenêtre, vous pouvez spécifier ou modifier les paramètres de connexion des Light Agents au Serveur d'intégration.

Paramètres de connexion au Serveur d'intégration

Paramètre	Description
Adresse	L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center fait partie d'un domaine, le champ par défaut indique le nom de domaine de cet appareil. Si l'appareil sur lequel est installée la Console d'administration de Kaspersky Security Center ne fait pas partie d'un domaine ou si le Serveur d'intégration est installé sur un autre appareil, le champ doit être rempli manuellement. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.
Port	Port de connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.

Si votre infrastructure déploie un cluster de Serveurs d'intégration à haute disponibilité basé sur Linux, vous devez spécifier l'adresse et le port du répartiteur de charge comme adresse et port pour vous connecter au Serveur d'intégration. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Fenêtre Vérification du certificat du Serveur d'intégration

Cette fenêtre s'affiche si le certificat SSL reçu du Serveur d'intégration contient une erreur ou n'est pas approuvé.

À l'aide du lien dans la fenêtre, vous pouvez afficher des informations sur le certificat reçu.

Si vous rencontrez des problèmes avec un certificat SSL, il est recommandé de vous assurer que le canal de transmission de données que vous utilisez est sécurisé.

Pour continuer à vous connecter au Serveur d'intégration, cliquez sur le bouton **Ignorer**. Le certificat reçu sera installé en tant que certificat de confiance sur l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée.

Fenêtre Authentification sur le Serveur d'intégration

Cette fenêtre s'affiche si l'appareil sur lequel la Console d'administration de Kaspersky Security Center est installée ne fait pas partie d'un domaine ou si votre compte n'est pas membre du groupe KLAdmins local ou du domaine ou du groupe des administrateurs locaux.

Spécifiez le mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`) et cliquez sur le bouton **OK**.

Il est recommandé de s'assurer que la complexité du mot de passe et les mécanismes anti-force brute garantissent que le mot de passe ne peut pas être deviné dans un délai de 6 mois.

Après la connexion au Serveur d'intégration avec des droits d'administrateur, la stratégie reçoit automatiquement le mot de passe de l'`agent` utilisé pour connecter les Light Agents au Serveur d'intégration.

Paramètres de détection des SVM

Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Dans cette fenêtre, vous pouvez sélectionner le mode utilisé par les Light Agents pour détecter les SVM disponibles pour la connexion.mode

Paramètres de détection des SVM

Paramètre	Description
Utiliser le Serveur d'intégration	Si cette option est sélectionnée, le Light Agent se connecte au Serveur d'intégration pour obtenir une liste des SVM disponibles pour la connexion et des informations les concernant. Si vous souhaitez utiliser le Serveur d'intégration, vous devez configurer les paramètres de connexion des Light Agents au Serveur d'intégration.
Utiliser la liste d'adresses des SVM définie manuellement	Si cette option est sélectionnée, vous pouvez spécifier une liste de SVM auxquelles les Light Agents sous le contrôle de cette stratégie peuvent se connecter. Les agents légers se connecteront uniquement aux SVM spécifiées dans la liste.
Liste des SVM	Une liste d'adresses IP au format IPv4 ou de noms de domaine complets (FQDN) de la SVM auxquels les Light Agents sous contrôle de stratégie peuvent se connecter. En cliquant sur le bouton **Ajouter**, une fenêtre s'ouvre dans laquelle vous pouvez spécifier l'adresse IP au format IPv4 ou le nom de domaine complet (FQDN) de la SVM. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne. Il vous suffit de spécifier des noms de domaine complets (FQDN) qui correspondent à une seule adresse IP. L'utilisation d'un nom de domaine pleinement qualifié qui correspond à plusieurs adresses IP peut entraîner des erreurs dans l'application. Vous pouvez supprimer les adresses sélectionnées dans la liste en cliquant sur le bouton **Supprimer**. La liste des adresses SVM s'affiche si l'option **Utiliser la liste d'adresses des SVM définie manuellement** est sélectionnée.

Si vous avez sélectionné l'option **Utiliser la liste d'adresses des SVM définie manuellement** et pour Light Agent, un algorithme de sélection des SVM étendu est utilisé et le mode de protection SVM pour les grandes infrastructures est activé (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Dans la section **Algorithme de sélection des SVM**, vous devez spécifier la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

Tag de connexion à la SVM

Dans cette fenêtre, vous pouvez permettre au Light Agent d'utiliser des tags et attribuer un tag que le Light Agent utilisera pour se connecter.

Assurez-vous que l'utilisation des tags pour les connexions est également configurée dans les paramètres du Serveur de protection : pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent. Les Light Agents dotés d'un tag ne peuvent se connecter qu'aux SVM autorisées à se connecter aux Light Agents avec ce tag.

Paramètres d'utilisation des tags pour la connexion

Paramètre	Description
Utiliser le tag de connexion	La case active ou désactive l'utilisation des tags par le Light Agent pour se connecter à SVM.
Tag	Un tag attribué aux Light Agents. 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 `;`. Le champ est disponible si la case **Utiliser le tag de connexion** est cochée.

Algorithme de sélection des SVM

Dans cette fenêtre, vous pouvez spécifier quel algorithme de sélection des SVM les Light Agents doivent utiliser et configurer les paramètres d'utilisation de l'algorithme de sélection des SVM avancé.

Algorithme de sélection des SVM

Paramètre	Description
Utiliser l'algorithme standard de sélection des SVM	Si cette option est sélectionnée, après l'installation et l'exécution sur une machine virtuelle, Light Agent choisit de se connecter à une SVM locale sur Light Agent. Pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization 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. Cette option est sélectionnée par défaut.
Utiliser l'algorithme étendu de sélection des SVM	Si cette option est sélectionnée, vous pouvez utiliser le curseur **Emplacement des SVM** pour spécifier comment l'emplacement de la SVM dans l'infrastructure virtuelle sera pris en compte lors de la détermination de la localité de la SVM par rapport au Light Agent. Le Light Agent ne pourra se connecter qu'aux SVM locales. Vous pouvez également spécifier que l'emplacement de la SVM dans l'infrastructure virtuelle ne doit pas être pris en compte lors de la sélection d'une SVM à laquelle se connecter. Lors de la sélection d'une SVM, les Light Agents prennent en compte le nombre de Light Agents connectés à cette SVM pour garantir une répartition uniforme des Light Agents parmi les SVM disponibles auxquelles se connecter.

Paramètre	Description

Emplacement des SVM	Permet de préciser le type d'emplacement de la SVM dans l'infrastructure virtuelle, qui est pris en compte lors du choix d'une SVM à laquelle se connecter :
	• **Hyperviseur**. Le Light Agent sélectionne pour se connecter une SVM qui répond aux critères (selon le type d'infrastructure virtuelle) :
	  • La SVM est déployée sur le même hyperviseur que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plate-forme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Scala-R, 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 fonctionnant sur la plateforme OpenStack, VK Cloud (VK Private Cloud) ou TIONIX Cloud Platform).
	  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) :
	  • La SVM est déployée dans le même cluster d'hyperviseurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plate-forme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Scala-R, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
	  • La SVM est déployée dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle fonctionnant sur la plateforme OpenStack, VK Cloud (VK Private Cloud) ou TIONIX Cloud Platform).
	  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) :
	  • La SVM est déployée dans le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plate-forme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, Scala-R, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
	  • La SVM se trouve dans la même zone de disponibilité que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle fonctionnant sur la plateforme OpenStack, VK Cloud (VK Private Cloud) ou TIONIX Cloud Platform).
	  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 ne prend pas en compte son emplacement lors du choix d'un SVM.
	Par défaut, la valeur **Hyperviseur** est sélectionnée.
	Le paramètre est disponible si l'option **Utiliser l'algorithme étendu de sélection des SVM** est sélectionnée.

Si un algorithme avancé de sélection de SVM est utilisé pour Light Agent et que la liste des adresses SVM est sélectionnée comme mode de détection de SVM et que le mode de protection pour les grandes infrastructures est activé sur la SVM (pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent), alors la connexion du Light Agent à cette SVM n'est possible que si la localisation de la SVM n'est pas prise en compte. Vous devez définir la valeur **Ignorer** pour le paramètre **Emplacement des SVM**. S'il est défini sur une autre valeur, le Light Agent ne peut pas se connecter à la SVM.

Protection de la connexion

Dans cette fenêtre, vous pouvez activer le chiffrement du canal de transmission des données entre le Light Agent et le Serveur de protection.

Assurez-vous que le chiffrement du canal de transmission de données entre le Light Agent et le Serveur de protection est activé dans les paramètres du Serveur de protection sur la SVM. Pour plus de détails, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent.

Paramètre	Description
Chiffrer le canal de données entre Light Agent et le Serveur de protection	Sécurisez la connexion entre les Light Agents et le Serveur de protection à l'aide du chiffrement. Si la case est cochée, une connexion chiffrée est établie entre le Light Agent, qui est sous contrôle de stratégie, et le Serveur de protection sur la SVM à laquelle le Light Agent se connecte. Un Light Agent dont la protection de connexion est activée peut uniquement se connecter à une SVM sur laquelle la protection de connexion est également activée ou qui autorise une connexion non chiffrée au Serveur de protection. Si la case est décochée, une connexion non chiffrée est établie entre le Light Agent et le Serveur de protection sur la SVM à laquelle le Light Agent se connecte. La case est décochée par défaut.

Afficher des informations sur l'utilisation d'une application en mode Light Agent dans la ligne de commande

Dans la ligne de commande, vous pouvez afficher les informations suivantes sur l'utilisation de l'application en mode Light Agent pour protéger les environnements virtuels :

- à propos des paramètres d'utilisation de l'application en mode Light Agent ;
- sur la connexion du Light Agent au Serveur d'intégration ;
- sur la connexion du Light Agent à la SVM.

Pour afficher des informations sur les paramètres d'utilisation d'une application en mode Light Agent, exécutez la commande suivante :

```
kesl-control [-V] --ksvla-info
```

La commande affiche les informations suivantes sur la console :

- Mode Light Agent pour la protection des environnements virtuels : activé / désactivé.

  Si le mode Light Agent est activé, l'application est utilisée comme Light Agent dans le cadre de la solution Kaspersky Security for Virtualization Light Agent.

- Mode de protection de l'infrastructure VDI : activé / désactivé.

  Le mode de protection de l'infrastructure VDI vous permet d'optimiser le fonctionnement de l'application Kaspersky Endpoint Security sur les machines virtuelles temporaires. Lorsque le mode de protection VDI est activé, les mises à jour nécessitant un redémarrage de la machine virtuelle protégée ne sont pas installées sur les machines virtuelles temporaires. Lors de la réception de mises à jour nécessitant un redémarrage, le Light Agent installé sur une machine virtuelle temporaire envoie un message à Kaspersky Security Center concernant la nécessité de mettre à jour le modèle des machines virtuelles protégées.

- Type de machine virtuelle protégée : temporaire ou permanente.
- Le rôle de la machine virtuelle protégée dans l'infrastructure virtuelle : serveur ou poste de travail.
- Identifiant (UUID) de la machine virtuelle protégée.

Pour afficher les informations sur la connexion du Light Agent au Serveur d'intégration, exécutez la commande suivante :

```
kesl-control [-V] --viis-info
```

La commande affiche les informations suivantes sur la console :

- Adresse et port du Serveur d'intégration auquel le Light Agent se connecte.

  Si votre infrastructure déploie un cluster tolérant aux pannes des Serveurs d'intégration basé sur Linux, l'adresse et le port du répartiteur de charge sont affichés. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

- Statut de connexion au Serveur d'intégration.
- Date et heure de la dernière connexion du Light Agent avec le Serveur d'intégration.

Pour afficher les informations sur la connexion du Light Agent à la SVM, exécutez la commande suivante :

```
kesl-control [-V] --svm-info
```

La commande affiche les informations suivantes sur la console :

- L'adresse de la SVM à laquelle le Light Agent est connecté, et l'emplacement de la SVM dans l'infrastructure virtuelle par rapport au Light Agent : local ou non local.
- 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 d'adresses SVM, si la liste d'adresses SVM est sélectionnée comme mode de détection SVM.
- Tag pour connecter le Light Agent à la SVM.
- Algorithme de sélection des SVM : standard ou avancé. Si l'algorithme de sélection SVM avancé est utilisé, le type d'emplacement de la SVM dans l'infrastructure virtuelle est également affiché.
- Disponibilité d'une protection de connexion entre le Light Agent et le Serveur de Protection.

Pour plus d'informations sur les paramètres de connexion des Light Agents au Serveur d'intégration et à la SVM, consultez l'aide de la solution Kaspersky Security for Virtualization Light Agent.

Afficher les événements et les rapports

Différents *événements* se produisent pendant le fonctionnement de l'application. Ils peuvent avoir un caractère informatif ou revêtir une importance plus grande. Ainsi, l'application peut utiliser les événements pour signaler la réussite de la mise à jour des bases de données de l'application ou signaler une erreur dans le fonctionnement d'un module qu'il faudra rectifier.

Kaspersky Endpoint Security vous permet de saisir des informations sur les événements survenus pendant le fonctionnement de l'application dans les journaux suivants :

- Journal des événements de l'application. Par défaut, l'application enregistre les informations relatives aux événements dans la base de données /var/opt/kaspersky/kesl/private/storage/events.db. Vous pouvez configurer les paramètres du journal des événements de l'application à partir de la ligne de commande.

- Journal du système d'exploitation (syslog). Par défaut, le journal du système d'exploitation n'est pas utilisé. Vous pouvez activer l'enregistrement des événements dans ce journal.

Les privilèges root sont requis pour accéder au journal des événements de l'application et au journal du système d'exploitation.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les informations sur les événements peuvent être transmises au Serveur d'administration de Kaspersky Security Center. Certains événements ont des règles d'agrégation. Si de nombreux événements du même type sont générés pendant une courte période pendant le fonctionnement de l'application, l'application passe en mode d'agrégation d'événements et envoie un événement agrégé avec une description des paramètres de ces événements à Kaspersky Security Center. Différentes règles d'agrégation peuvent être utilisées pour différents événements. Pour plus d'informations sur les événements, consultez l'aide de Kaspersky Security Center.

Vous pouvez recevoir des informations sur les événements de l'application des manières suivantes :

- Dans la Console d'administration et dans Web Console.

- En ligne de commande (Affichage des événements en ligne de commande, Affichage des événements dans Kaspersky Security Center)

- Lors de l'utilisation de l'interface utilisateur graphique de l'application, dans les notifications contextuelles, si l'affichage des notifications est activé dans les propriétés de la stratégie ou les paramètres généraux de l'application.

En fonction des événements qui se produisent pendant l'exécution de l'application, vous pouvez générer divers *rapports*. Les rapports enregistrent des informations sur le fonctionnement de chaque module de l'application Kaspersky Endpoint Security, les résultats de chaque tâche et le fonctionnement de l'ensemble de l'application dans son ensemble.

Vous pouvez consulter les rapports d'une des manières suivantes :

- Les rapports de Kaspersky Security Center sont disponibles dans la Console d'administration et dans Web Console. Avec leur aide, vous pouvez, par exemple, obtenir des informations sur les fichiers infectés, l'utilisation des clés et des bases de données de l'application. Pour en savoir plus sur l'utilisation des rapports de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

- Des rapports sur le fonctionnement de l'application, de ses modules et de ses tâches sont disponibles dans l'interface utilisateur graphique de Kaspersky Endpoint Security.

Contenu des rapports et des événements

Les rapports et les événements peuvent contenir les données personnelles suivantes :

- noms et identifiants des utilisateurs dans le système d'exploitation ;
- chemins d'accès aux fichiers utilisateur ;
- adresses IP des appareils distants analysés par le module Protection contre le chiffrement ;
- adresses IP des expéditeurs et des destinataires des paquets réseau vérifiés par le module Gestion du pare-feu ;
- adresses Internet des sources de mises à jour ;
- valeurs des paramètres généraux de l'application ;
- noms et paramètres des tâches de la ligne de commande ;
- adresses Internet malveillantes, de phishing, publicitaires et adresses Internet contenant des applications légitimes que les intrus peuvent utiliser pour endommager vos appareils ou vos données ;
- noms des conteneurs et des images ;
- chemins d'accès aux conteneurs et images ;
- noms et identifiants des appareils ;
- noms des catégories des applications ;
- adresses Internet des référentiels ;
- noms de fichiers, chemins d'accès aux fichiers et sommes de hachage des fichiers exécutables des applications.

Règles d'échappement des caractères dans les chemins de fichiers

Certains événements peuvent contenir des chemins d'accès aux fichiers. Lors de l'affichage, le chemin d'accès au fichier est traité comme une chaîne codée en UTF-8. Si l'un des octets du chemin n'est pas conforme aux règles de codage UTF-8, il est alors remplacé par le caractère `?`. Une séquence de quatre octets codant le code des caractères en dehors de la plage Unicode (supérieure à 0x10FFFF) est également remplacée par le caractère `?`. Les caractères spéciaux sont échappés (remplacés) d'une manière spécifique.

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lors de l'affichage à l'aide de la commande `kesl-control -E --query` :

- les caractères '\a', '\b', '\t', '\n', ' \v', '\f', '\r' sont remplacés par deux caractères comme suit :

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

'\n' -> "\\n"

'\v' -> "\\v"

'\f' -> "\\f"

'\r' -> "\\r"

- tous les autres caractères spéciaux sont affichés inchangés.

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lors de l'affichage à l'aide de la commande `kesl-control -E --query --json` :

- les caractères '\b', '\f', '\n', '\r', '\t', '"', '\\' sont échappés, selon le format JSON, comme suit :

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- tous les autres caractères spéciaux sont échappés conformément aux règles générales d'échappement des caractères spéciaux pour le format JSON ('\a' -> '\u0007').

Règles d'échappement des caractères dans les chemins de fichiers dans les événements lorsqu'ils sont envoyés à syslog :

- les caractères '\b', '\f', '\n', '\r', '\t', '"', '\\' sont échappés, selon le format JSON, comme suit :

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\\""

  '\\' -> "\\\\"

- tous les autres caractères spéciaux sont échappés conformément aux règles générales d'échappement des caractères spéciaux pour le format JSON ('\a' -> '\u0007').

La première barre oblique de la séquence lors de la description des règles est un caractère d'échappement.

Exemples :
`'\a'` est un caractère (administrateur) ;

`'\\a'` est composé de deux caractères (barre oblique inverse + caractère `a`) ;

`'\\'` représente un caractère (barre oblique inverse).

`'\\\\'` représente deux caractères (barre oblique inverse + barre oblique inverse).

Configuration d'enregistrement des événements dans le journal du système d'exploitation

Les événements survenus lors du fonctionnement de l'application Kaspersky Endpoint Security peuvent être enregistrés dans le journal du système d'exploitation. Vous pouvez activer ou désactiver l'enregistrement des événements dans ce journal à l'aide de Web Console, de la Console d'administration ou de la ligne de commande.

Si vous utilisez la ligne de commande pour gérer l'application, l'enregistrement des événements dans le journal du système d'exploitation est désactivé par défaut.

Si vous utilisez Kaspersky Endpoint Security en mode standard ou en mode Endpoint Detection and Response Agent et utilisez Kaspersky Security Center pour gérer l'application, les informations sur l'ajout et la suppression de clés de licence et sur l'expiration de la licence sont enregistrées par défaut dans le journal du système d'exploitation. Vous pouvez sélectionner les événements qui seront écrits dans le journal du système d'exploitation dans les propriétés de la stratégie sous laquelle l'application s'exécute.

Configuration dans Web Console

Dans Web Console, vous pouvez activer ou désactiver l'enregistrement des événements dans le journal du système d'exploitation dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres des événements**).

En cliquant sur le bouton **Paramètres** dans le groupe portant le nom du niveau de gravité de l'événement (événements critiques, erreurs de fonctionnement, avertissements, messages d'information), une fenêtre s'ouvre contenant une liste des événements de ce niveau de gravité. Pour chaque événement, vous pouvez configurer l'enregistrement dans le journal du système d'exploitation.

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer l'enregistrement des événements dans le journal du système d'exploitation dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**).

Le lien **Configurer** dans le groupe **Notifications** ouvre la fenêtre **Paramètres des notifications**. Dans cette fenêtre, vous pouvez utiliser des cases pour sélectionner les événements que l'application écrira dans le journal du système d'exploitation.

Vous pouvez sélectionner des types d'événements individuels ou tous les types d'événements d'un certain niveau de gravité (événements critiques, erreurs de fonctionnement, avertissements, messages d'information).

Configuration sur la ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver l'enregistrement des événements dans le journal du système d'exploitation à l'aide de l'option `UseSyslog` des paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `UseSyslog` peut prendre les valeurs suivantes :

- `Yes` : active l'enregistrement des événements dans syslog.
- `No` (valeur par défaut) : désactiver l'enregistrement des événements dans syslog.

Configuration des paramètres du journal des événements de l'application

Par défaut, les informations sur les événements sont stockées dans le journal des événements de l'application situé sur l'appareil.

La base de données du journal des événements contient les fichiers suivants :

- plusieurs fichiers avec des événements. Le nombre de fichiers dépend du nombre actuel d'événements dans le journal des événements et du nombre maximal d'événements que l'application stockera (défini dans le paramètre `MaxEventsNumber`).

  Le nom du fichier d'événements contient le numéro de série de sa création (par exemple, events.db.0001). Les fichiers sont créés au fur et à mesure qu'ils sont remplis. Si tous les fichiers d'événements, à l'exception du fichier le plus ancien, ont un nombre maximal d'événements égal à la valeur spécifiée du paramètre `MaxEventsNumber`, le fichier le plus ancien est supprimé. De cette façon, l'application peut stocker plus d'événements que défini dans le paramètre.

- le fichier principal de la base de données pour la gestion des fichiers des événements, qui stocke des informations sur les fichiers journaux des événements. Ce fichier ne peut pas être supprimé.

À partir de la ligne de commande, vous pouvez gérer les paramètres suivants du journal des événements de l'application à l'aide des paramètres généraux de l'application :

- Modifier le chemin d'accès au fichier principal de la base de données du journal des événements à l'aide du paramètre `EventsStoragePath`. Valeur par défaut : /var/opt/kaspersky/kesl/private/storage/events.db.
- Définissez le nombre maximum d'événements que l'application stockera à l'aide du paramètre `MaxEventsNumber`. Valeur par défaut : 500 000.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Consultation des événements dans Kaspersky Security Center

Une liste de tous les événements liés au fonctionnement de l'application Kaspersky Endpoint Security est affichée dans Web Console et dans la Console d'administration.

Les événements qui surviennent lors du fonctionnement de l'application Kaspersky Endpoint Security sont classés par niveau d'importance selon les types suivants :

- *Les événements critiques* sont des événements qui constituent une menace sérieuse pour la sécurité des appareils (détection d'objets malveillants, vulnérabilités, problèmes de fonctionnement des applications). Un événement critique nécessite votre attention immédiate. Il est recommandé de ne pas désactiver les notifications concernant les événements critiques.

- *Les erreurs de fonctionnement* sont des événements qui se produisent lorsqu'une application dysfonctionne (erreur de traitement, erreur de configuration de tâche). Ces événements ne représentent pas une menace directe pour la sécurité de l'appareil, mais ils nécessitent votre intervention pour que l'application fonctionne correctement.

- *Les avertissements* sont des événements qui ne nécessitent pas d'intervention immédiate de votre part, mais qui peuvent représenter une menace pour la sécurité de votre appareil.

- *Les messages d'information* sont des événements informatifs.

Vous pouvez configurer des notifications d'événements. Une *notification* est un message contenant des informations sur un événement survenu sur un appareil protégé. Grâce aux notifications, vous pouvez recevoir des informations en temps opportun sur les événements de l'application. Vous pouvez configurer l'exécution du script à la réception d'un événement depuis l'application ou à la réception d'une notification par email sur les événements.

Pour plus d'informations sur l'utilisation des notifications de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Affichage des événements en ligne de commande

En ligne de commande, vous pouvez afficher :

- événements d'application en cours ;

- Événements du journal des événements de l'application

Affichage des actualités

Vous pouvez afficher des informations sur la console sur tous les événements d'application en cours ou sur les événements en cours associés au démarrage ou à l'arrêt d'une tâche spécifiée. À l'aide d'un filtre vous pouvez également afficher certains événements en cours, par exemple, des événements d'un type spécifié.

Pour afficher des informations sur tous les événements de l'application en cours sur la console, exécutez la commande suivante :

```
kesl-control -W
```

La commande reprend le nom de l'événement et les informations supplémentaires sur l'événement.

Pour afficher sur la console des informations uniquement sur les événements en cours associés à une tâche en cours d'exécution, exécutez la commande suivante :

```
kesl-control --start-task ID/nom de la tâche> -W
```

Exemple :
Activer l'affichage des événements actuels de la tâche en cours d'exécution avec ID=1 :

```
kesl-control --start-task 1 -W
```

Pour afficher des informations sur les événements en cours qui correspondent aux critères de filtre sur la console, exécutez la commande suivante :

```
kesl-control -W --query "< conditions de filtrage >"
```

Les conditions de filtrage sont définies avec une ou plusieurs expressions logiques au format `< champ >` `< opérateur de comparaison > '< valeur >'`, combinées à l'aide de l'opérateur logique `and`.

Exemple :
Afficher les événements TaskStateChanged :

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Afficher les événements TaskSettingsChanged initiés par l'utilisateur User :

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Affichage des événements à partir du journal des événements

Vous pouvez générer des informations sur les événements du journal des événements de l'application vers la console ou vers un fichier. Vous pouvez utiliser un filtre pour afficher des événements spécifiques.

Pour afficher des informations sur tous les événements du journal des événements de l'application sur la console, exécutez la commande suivante :

```
kesl-control -E --query [--db < fichier de base de données >]
```

où `< fichier de base de données >` correspond au chemin d'accès complet au fichier de base de données du journal des événements à partir duquel afficher les événements. Par défaut, l'application enregistre les informations relatives aux événements dans la base de données /var/opt/kaspersky/kesl/private/storage/events.db. L'emplacement de la base de données est déterminé par le paramètre général de l'application `EventsStoragePath`.

Si le journal des événements se trouve dans la base de données par défaut, vous pouvez afficher des informations sur tous les événements sur la console à l'aide de la commande `kesl-control -E`.

Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés. Par défaut, l'application stocke jusqu'à 500 000 événements. Le nombre maximal d'événements stockés par l'application est déterminé par le paramètre général de l'application `MaxEventsNumber`.

Pour afficher dans la console des informations sur les événements du journal des événements de l'application qui remplissent certaines conditions, exécutez la commande suivante :

```
kesl-control -E --query "< conditions de filtrage >" [--db < fichier de base de données >]
[-n < nombre >] [--json] [--reverse]
```

où :

- `< conditions de filtrage >` spécifient une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête.
- `< nombre >` est le nombre d'événements les plus récents de la sélection (enregistrements comptés à partir de la fin de la sélection) à afficher.
- `--json` – afficher les événements au format JSON.
- `--reverse` : afficher les événements dans l'ordre inverse (de l'événement le plus récent en haut au plus ancien en bas).

Pour afficher dans le fichier des informations sur les événements du journal des événements de l'application qui remplissent certaines conditions, exécutez la commande suivante :

```
kesl-control -E --query "< conditions de filtrage >" [--db < fichier de base de données >]
[-n < nombre >] --file < chemin d'accès au fichier > [--json]
```

où `--file < chemin d'accès au fichier >` est le chemin d'accès complet au fichier dans lequel enregistrer les événements.

Configuration des notifications contextuelles dans l'interface graphique

Dans l'interface graphique de l'application, les informations relatives aux événements s'affichent par défaut sous forme de notifications contextuelles. Vous pouvez activer ou désactiver ces notifications via la Console d'administration ou la ligne de commande.

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver l'affichage des notifications contextuelles dans l'interface graphique dans les propriétés de la stratégie (Administration des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Paramètres généraux** → **Paramètres de l'application**).

La case **Afficher les notifications contextuelles dans l'interface utilisateur graphique** permet d'afficher des notifications contextuelles dans l'interface utilisateur graphique.

La case est cochée par défaut.

Configuration sur la ligne de commande

À partir de la ligne de commande, vous pouvez basculer l'affichage des notifications contextuelles dans l'interface graphique en utilisant le paramètre `ShowPopUpNotifications` dans les paramètres généraux de l'application.

Vous pouvez modifier la valeur du paramètre à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Le paramètre `ShowPopUpNotifications` peut prendre les valeurs suivantes :

- `Yes` (par défaut) : afficher les notifications contextuelles dans l'interface utilisateur graphique.
- `No` : ne pas afficher les notifications contextuelles dans l'interface utilisateur graphique.

Administration de l'application via l'interface graphique

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'interface graphique n'est pas prise en charge.

Grâce à l'interface graphique de l'application Kaspersky Endpoint Security, vous pouvez :

- Afficher des informations sur l'état de sécurité de l'appareil.
- Activer ou désactiver les modules de l'application :
  - Protection contre les fichiers malicieux.
  - Gestion du pare-feu.
  - Protection contre le chiffrement.
  - Analyse des disques amovibles.
  - Protection contre les menaces Internet.
  - Protection contre les menaces par emails.
  - Contrôle des appareils.
  - Protection contre les menaces réseau.
  - Protection BadUSB.
  - Détection comportementale.
  - Protection contre les Exploits.
  - Contrôle des applications.
  - Contrôle Internet.
  - Contrôle de l'intégrité du système.
- Démarrer et arrêter des tâches d'analyse :
  - Analyse des logiciels malveillants.
  - Analyse des zones critiques.
  - Analyse du conteneur.
- Exécuter une analyse personnalisée des fichiers et des répertoires.

- Démarrer et arrêter les tâches de mise à jour et de restauration de la base de données.
- Envoyer un fichier ou un répertoire pour analyse à Sandbox.
- Activer ou désactiver l'utilisation de Kaspersky Security Network.
- Gérer les clés de licence de l'application et afficher des informations sur la licence sous laquelle l'application est utilisée et la clé associée à la licence.
- Demander et obtenir un accès temporaire à un appareil bloqué auprès de l'administrateur du réseau local de l'organisation.
- Afficher les statistiques et les rapports des applications.
- Afficher des informations sur les objets placés dans la sauvegarde.
- Générer des fichiers de trace de l'application.

Si l'application est utilisée en mode EDR Agent, seul un sous-ensemble limité des modules et des tâches de l'application est disponible. Vous pouvez gérer certains modules de protection, activer l'application et mettre à jour les bases de données. Pour en savoir plus sur les particularités du mode EDR Agent, consultez l'article Problèmes connus et limitations.

Lorsque le module ou la tâche de l'application s'exécute en mode informatif, l'interface graphique de l'application affiche l'avertissement *Mode de fonctionnement informatif sélectionné* pour ce module ou pour cette tâche.

Interface graphique

Icône de l'application dans la zone de notification

L'icône de l'application Kaspersky Endpoint Security dans la zone de notification de la barre des tâches permet d'accéder au menu contextuel et à la fenêtre principale de l'interface graphique de l'application.

Sur certains systèmes d'exploitation, l'icône de l'application par défaut peut être manquante après l'installation du paquet d'interface graphique de l'application.

Le menu contextuel de l'icône de l'application reprend les options suivantes :

- **Kaspersky Endpoint Security 12.4 for Linux**. Ouvre la fenêtre principale de l'interface graphique de l'application, qui affiche l'état de la protection de l'appareil et contient les éléments d'interface qui permettent d'accéder aux fonctions de l'application.
- **Quitter**. Quitte l'interface graphique.

Fenêtre principale de l'interface graphique de l'application

Vous pouvez ouvrir la fenêtre principale de l'interface graphique de l'application d'une des manières suivantes :

- En sélectionnant le nom de l'application dans le menu de l'application du gestionnaire de fenêtres du système d'exploitation.
- En utilisant le bouton droit de la souris ou en double-cliquant sur l'icône de l'application dans la zone de notification de la barre des tâches.

La fenêtre principale de l'interface graphique l'application est divisée en plusieurs parties :

- Le haut de la fenêtre principale affiche l'état de protection de l'appareil. Le bouton **Afficher** ouvre la fenêtre **Centre de protection**. Cette fenêtre affiche des informations sur l'état de la protection de l'appareil et des recommandations relatives aux mesures à prendre pour corriger les problèmes de sécurité (le cas échéant).
- Le groupe **Analyse** affiche l'état de la tâche d'analyse des logiciels malveillants et le nombre de menaces détectées. En cliquant sur ce groupe, la fenêtre **Analyse** s'ouvre. Cette fenêtre vous permet de lancer et d'arrêter les tâches *Analyse des logiciels malveillants*, *Analyse des zones critiques* et *Analyse du conteneur*. En outre, vous pouvez afficher des rapports pour ces tâches.
- Le groupe **Mise à jour** affiche l'état de la tâche *Mise à jour*. En cliquant sur ce groupe, la fenêtre **Mise à jour** s'ouvre. Dans cette fenêtre, vous pouvez exécuter les tâches *Mise à jour* et *Annulation de la mise à jour des bases*. En outre, vous pouvez afficher des rapports pour ces tâches.
- La partie inférieure de la fenêtre principale contient les éléments suivants :
  - Bouton **Rapports**. Cliquez sur ce bouton pour accéder à la fenêtre **Rapports**, dans laquelle vous pouvez consulter les statistiques des modules et des tâches et divers rapports.
  - Bouton **Sauvegarde**. Cliquez sur ce bouton pour accéder à la fenêtre **Sauvegarde** qui contient des informations sur les objets dans la sauvegarde.
  - Bouton **Paramètres**. En cliquant sur ce bouton, vous ouvrez la fenêtre **Configuration**, où vous pouvez activer ou désactiver les modules de surveillance de l'application ainsi que configurer l'utilisation de Kaspersky Security Network.
  - Bouton **Accès temporaire**. Un clic sur ce bouton ouvre la fenêtre **Accès temporaire**, dans laquelle vous pouvez demander et obtenir un accès temporaire à l'appareil bloqué.
  - Bouton **Support**. Cliquer sur ce bouton pour ouvrir la fenêtre **Assistance** dans laquelle vous pouvez afficher des informations sur l'application et également créer un fichier de traçage de l'application.
- La partie la plus inférieure de la fenêtre principale de l'application affiche des informations sur la licence et la clé, ainsi que des renseignements sur les problèmes de licence (le cas échéant). En cliquant sur cette zone de la fenêtre, la fenêtre **Licences** s'ouvre, qui affiche des informations détaillées sur la licence. En cliquant sur le bouton **Acheter une licence** dans cette fenêtre, vous pouvez ouvrir la boutique en ligne de Kaspersky, où vous pouvez acheter une licence. Après avoir acheté une licence, vous recevrez un code d'activation ou un fichier clé avec lequel vous devrez activer l'application.

Pour configurer l'interface graphique, des droits d'utilisateur avec le rôle Administrateur (admin) sont requis. Certains éléments de l'interface graphique peuvent ne pas être disponibles pour les utilisateurs ayant d'autres rôles.

Activer ou désactiver les modules de l'application

Vous pouvez activer et désactiver les modules de l'application dans l'interface graphique à l'aide du commutateur.

Par défaut, seuls les modules Protection contre les fichiers malicieux, Contrôle des appareils et Détection comportementale sont activés. Le module Protection contre les menaces Internet peut être activé automatiquement si la gestion locale des paramètres de protection contre les menaces Internet est activée sur l'appareil (la stratégie n'est pas appliquée ou le « cadenas » dans les propriétés de la stratégie n'est pas défini) et l'un des navigateurs pris en charge est détecté dans le système.

Pour activer ou désactiver un module de l'application :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Configuration**.

   La fenêtre **Configuration** s'ouvre.
3. Activez ou désactivez l'interrupteur du module souhaité.

Démarrage et arrêt des tâches d'analyse

Pour démarrer ou arrêter une tâche d'analyse :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la fenêtre principale de l'application, cliquez sur le bouton **Analyse**.

   La fenêtre **Analyse** s'ouvre.
3. Exécutez une des actions suivantes :

   - Si vous voulez démarrer une tâche d'analyse, cliquez sur le bouton **Démarrer** sous la tâche d'analyse que vous voulez démarrer.

     La progression de la tâche d'analyse en cours s'affiche.
   - Si vous souhaitez arrêter une tâche d'analyse, cliquez sur le bouton **Arrêter** sous la tâche d'analyse que vous souhaitez arrêter.

     La tâche d'analyse s'arrête, et des informations sur les objets analysés et les menaces détectées s'affichent.
4. Si vous souhaitez afficher le rapport d'une tâche d'analyse, cliquez sur le bouton **Afficher le rapport**.

Lorsqu'un objet infecté est détecté ou lorsqu'une tâche d'analyse est terminée, une fenêtre pop-up s'affiche dans la zone de notification près de l'icône de l'application dans la partie droite de la barre des tâches.

La fenêtre **Analyse** affiche également la progression et les résultats des tâches temporaires d'analyse des secteurs de démarrage (*Scan_Boot_Sectors_{identifiant}*) et des tâches temporaires d'analyse personnalisée des fichiers (*Scan_File_{identifiant}*). Vous pouvez masquer les informations relatives aux tâches temporaires terminées en cliquant sur la croix ou en fermant la fenêtre **Analyse** (en accédant à la fenêtre principale ou en quittant l'application).

Lancement de l'analyse personnalisée et de l'analyse dans Sandbox

Vous pouvez lancer l'analyse personnalisée des fichiers et des répertoires à l'aide de l'interface graphique.

Pour lancer une analyse personnalisée d'un fichier ou d'un répertoire :

1. En cliquant avec le bouton droit sur le fichier/répertoire que vous souhaitez analyser, ouvrez le menu contextuel.
2. Sélectionnez **Kaspersky Endpoint Security 12.4 for Linux** comme application pour analyser le fichier ou le répertoire.

   Les noms des éléments du menu contextuel peuvent varier en fonction de votre environnement de bureau.

La tâche d'analyse personnalisée et sa progression seront affichées dans l'interface graphique.

Si l'intégration de l'application Kaspersky Endpoint Security avec Sandbox est activée, vous pouvez envoyer un fichier ou un répertoire à analyser vers Sandbox à l'aide de l'interface graphique.

Pour envoyer un fichier ou un répertoire à Sandbox pour analyse :

1. En cliquant avec le bouton droit sur le fichier/répertoire que vous souhaitez envoyer pour analyse, ouvrez le menu contextuel.
2. Sélectionnez **Kaspersky Endpoint Security 12.4 for Linux** comme application pour analyser le fichier ou le répertoire.

   Les noms des éléments du menu contextuel peuvent varier en fonction de votre environnement de bureau.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'option **Envoyer à Sandbox pour analyse**.

Démarrer et arrêter la tâche de mise à jour

Pour lancer ou arrêter la tâche de recherche de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la fenêtre principale de l'application, cliquez sur le bouton **Mise à jour**.

   La fenêtre **Mise à jour** s'ouvre.
3. Exécutez une des actions suivantes :

   - Si vous voulez démarrer une tâche, cliquez sur le bouton **Démarrer** sous la tâche d'analyse que vous voulez démarrer.

     La progression de la tâche de mise à jour en cours s'affiche.

     Si la tâche de mise à jour aboutit, le lien **Annuler la mise à jour** est disponible et vous pouvez restaurer la dernière mise à jour réussie des bases de données.

- Si vous souhaitez arrêter une tâche, cliquez sur le bouton **Arrêter** situé sous la tâche que vous souhaitez arrêter.

  La tâche de mise à jour s'arrête.

4. Si vous souhaitez afficher le rapport d'une tâche, cliquez sur le bouton **Afficher le rapport**.

Pour démarrer une tâche d'annulation de la mise à jour :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la fenêtre principale d'application, cliquez sur la section **Mise à jour**.

   La fenêtre **Mise à jour** s'ouvre.
3. Exécutez la tâche d'annulation de la mise à jour des bases de données à l'aide du lien **Annuler la mise à jour**.

Configuration de l'utilisation de Kaspersky Security Network

Vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network à l'aide de l'interface graphique.

Pour activer l'utilisation de Kaspersky Security Network :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Configuration**.

   La fenêtre **Configuration** s'ouvre.
3. Dans la fenêtre **Configuration**, sélectionnez l'une des options suivantes :

   - **Mode étendu de KSN**, si vous souhaitez utiliser Kaspersky Security Network, obtenir des informations dans la base de connaissance, et envoyer des statistiques anonymes et des informations sur les types et les sources de nouvelles menaces.
   - **Mode KSN de base**, si vous souhaitez utiliser Kaspersky Security Network, obtenir des informations dans la base de connaissance, mais que vous ne souhaitez pas envoyer des statistiques anonymes ni des informations sur les types et les sources de nouvelles menaces.
4. Cliquez sur le bouton **Activer**.

   La fenêtre **Utilisation de Kaspersky Security Network** s'ouvre.
5. Dans la fenêtre **Utilisation de Kaspersky Security Network**, lisez attentivement la Déclaration de Kaspersky Security Network et sélectionnez l'option **Je confirme avoir entièrement lu, compris et accepté les conditions générales de la Déclaration** de **Kaspersky Security Network**.
6. Cliquez sur le bouton **OK**.

   Le bouton **OK** est indisponible si aucune des options n'est sélectionnée dans la fenêtre **Utilisation de Kaspersky Security Network**.

Pour désactiver l'utilisation de Kaspersky Security Network :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Configuration**.

   La fenêtre **Configuration** s'ouvre.
3. Cliquez sur le bouton **Désactiver**.
4. Dans la fenêtre ouverte, cliquez sur **Oui** pour refuser d'utiliser Kaspersky Security Network.

Consulter les rapports

Vous pouvez afficher des rapports sur le fonctionnement des modules et des tâches de l'application à l'aide d'une interface graphique. Les rapports sont affichés dans une fenêtre qui s'ouvre en cliquant sur le bouton **Rapports** situé en bas de la fenêtre principale de l'interface graphique de l'application.

Les données des rapports sont présentées dans un tableau qui contient une liste d'événements. Chaque ligne du tableau contient des informations sur un événement distinct. Les attributs d'événement s'affichent dans les colonnes du tableau. Les événements enregistrés lors du fonctionnement de différents modules et tâches ont un ensemble d'attributs différent.

Les rapports prévoient les gravités suivantes pour les événement :

- *Critique* : événements critiques auxquels vous devez prêter attention, car ils indiquent un problème avec l'application ou une vulnérabilité dans la protection de l'appareil.
- *Élevé.*
- *Moyen.*
- *Faible.*
- *Informatif.*
- *Erreur.*

Les rapports suivants sont disponibles dans l'application :

- **Statistiques**. Ce rapport contient des informations statistiques sur le fonctionnement du module Protection contre les fichiers malicieux et sur les tâches d'analyse. Vous pouvez mettre à jour le rapport affiché en cliquant sur le bouton **Mettre à jour**.
- **Audit du système**. Ce rapport contient des informations sur les événements qui se produisent lors de l'utilisation de l'application et lors de l'interaction de l'utilisateur avec l'application.
- **Protection contre les menaces**. Ces rapports contiennent des informations sur les événements qui sont enregistrés pendant les modules de l'application suivants :
  - Protection contre les fichiers malicieux
  - Analyse des disques amovibles.

- Protection contre le chiffrement
- Protection contre les menaces Internet
- Protection contre les menaces par emails
- Protection contre les menaces réseau
- Protection BadUSB
- Gestion du pare-feu
- Contrôle des applications
- Contrôle des appareils
- Détection comportementale
- Protection contre les Exploits
- Contrôle de l'intégrité du système
- Contrôle Internet

- **Tâches à la demande**. Ce rapport contient des informations sur les événements enregistrés lors des tâches d'analyse, des tâches de mise à jour et des tâches de vérification de l'intégrité du système.
- **Prévention de l'exécution** Ce rapport contient des informations sur les événements enregistrés lors de la prévention de l'exécution des objets par les modules EDR Expert (on-premises) et EDR Optimum.

Pour consulter un rapport :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Rapports**.

   La fenêtre **Rapports** s'ouvre.
3. Sélectionnez le type de rapport requis dans la partie gauche de la fenêtre **Rapports**.

   Le rapport contenant la liste des événements apparaît dans la partie droite de la fenêtre.

   Par défaut, les événements sont triés par ordre croissant de valeurs dans la colonne **Date**.
4. Si vous souhaitez consulter des informations détaillées sur un événement, sélectionnez l'événement souhaité dans le rapport.

   Une section qui contient les attributs de cet événement s'affiche au bas de la fenêtre.

Pour faciliter l'utilisation des rapports, vous pouvez modifier la représentation des données à l'écran d'une des manières suivantes :

- Filtrez la liste des événements par période d'occurrence.
- utiliser la fonction de recherche d'un événement en particulier ;
- consulter l'événement sélectionné dans un groupe distinct ;

Afficher les objets de la sauvegarde

Vous pouvez effectuer les actions suivantes sur les objets de la sauvegarde à l'aide de l'interface graphique :

- Afficher des informations sur les objets placés dans la sauvegarde sur l'appareil.
- Restaurer les objets de la sauvegarde vers leurs répertoires d'origine.
- Supprimer les objets de la sauvegarde. Les objets supprimés ne peuvent être restaurés à l'avenir.

Les informations sur la restauration et la suppression des objets sont enregistrées dans le journal des événements.

Pour afficher les objets dans la sauvegarde :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Sauvegarde**.

   La fenêtre **Sauvegarde** s'ouvre.

La fenêtre affiche les informations suivantes sur les objets de la sauvegarde :

- nom de l'objet
- chemin complet vers un objet
- date à laquelle un objet a été ajouté à la sauvegarde
- la date à laquelle l'objet a été supprimé de la sauvegarde (ce champ est affiché si une limite est fixée sur la durée de conservation des objets dans la sauvegarde)
- taille de l'objet

Gestion des clés de licence

À l'aide de l'interface graphique, vous pouvez ajouter et supprimer des clés de licence de l'application et consulter les informations sur la licence sous laquelle l'application est utilisée et la clé associée à la licence.

Pour activer l'application Kaspersky Endpoint Security sur un appareil protégé, vous devez ajouter une clé de licence de base à l'application.

L'*activation* est une procédure qui permet d'activer une licence qui vous autorise à utiliser une version entièrement fonctionnelle de l'application jusqu'à l'expiration de la licence.

Si la licence de base sous laquelle vous utilisez l'application n'inclut pas les fonctionnalités supplémentaires de l'application Kaspersky Endpoint Security dont vous avez besoin, vous devrez également ajouter une clé de licence à l'application pour les fonctionnalités supplémentaires :

- une clé de licence distincte de « Kaspersky Endpoint Detection and Response Optimum Add-on » (ci-après également dénommée « clé EDR Optimum ») : pour activer le module EDR Optimum ;
- une clé de licence distincte « Kaspersky Unified Monitoring and Analysis Platform Add-on » (ci-après également dénommée « clé KUMA ») : pour activer la fonctionnalité de Kaspersky Unified Monitoring and Analysis Platform ;
- une clé de licence distincte pour « Kaspersky Managed Detection and Response Optimum/Expert Add-on » (ci-après également dénommée « clé MDR ») : pour activer la fonctionnalité du module MDR.

Vous pouvez également ajouter une clé de réserve à l'application pour la fonctionnalité de base et une clé de réserve pour des fonctionnalités supplémentaires. Une clé de réserve devient active lorsque la licence associée à la clé active expire ou lorsque la clé active est supprimée. La disponibilité d'une clé de réserve permet d'éviter la restriction des fonctionnalités de l'application à l'expiration d'une licence.

La clé de réserve ne peut être ajoutée qu'après l'ajout de la clé de licence active.

Ajout d'une clé de licence

Si l'application n'a pas encore été activée (une clé de licence de base active n'a pas été ajoutée), vous pouvez activer l'application à l'aide d'une licence commerciale ou d'une licence d'essai.

Pour activer l'application :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :
   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira. En cliquant sur le bouton **Acheter une licence** dans cette fenêtre, vous pouvez ouvrir la boutique en ligne de Kaspersky, où vous pouvez acheter une licence.
3. Si vous souhaitez activer l'application sous licence commerciale :
   a. Cliquez sur le bouton **Ajouter** dans le groupe **Clé commerciale** et effectuez les actions suivantes en fonction de la méthode d'ajout de la clé :
      - Si vous souhaitez ajouter une clé à l'aide d'un code d'activation, saisissez le code d'activation et cliquez sur le bouton **Suivant**.
      - Si vous souhaitez ajouter une clé à l'aide d'un fichier de clé, ouvrez la fenêtre de sélection de fichier à l'aide du lien **Sélectionner un fichier clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension key.

La fenêtre affichera les informations sur la clé et la licence qui lui est associée.

b. Cliquez sur le bouton **Activer**.

4. Si vous souhaitez activer l'application à l'aide d'une licence d'évaluation, cliquez sur le bouton **Activer** dans le groupe **Clé d'évaluation**. La fenêtre affichera les informations sur la licence d'évaluation et la clé associée.

> Vous ne pouvez utiliser l'application sous une licence d'essai que pour une seule période d'essai.

Après avoir activé l'application, vous pouvez ajouter une clé de licence de base de réserve et, si nécessaire, une clé active et de réserve pour des fonctionnalités supplémentaires de l'application. Les procédures d'ajout d'une clé de base de réserve et de clés pour des fonctionnalités supplémentaires sont les mêmes.

Pour ajouter une ou plusieurs clés de base de réserver pour des fonctionnalités supplémentaires à votre application :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.

   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira. La fenêtre affiche des informations sur les clés de licence précédemment ajoutées.

3. Cliquez sur le bouton **Ajouter** et effectuez les actions suivantes en fonction de la méthode d'ajout de la clé :

   - Si vous souhaitez ajouter une clé à l'aide d'un code d'activation, saisissez le code d'activation et cliquez sur le bouton **Suivant**.

   - Si vous souhaitez ajouter une clé à l'aide d'un fichier de clé, ouvrez la fenêtre de sélection de fichier à l'aide du lien **Sélectionner un fichier clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension key.

   La fenêtre affichera les informations sur la clé et la licence qui lui est associée.

4. Cliquez sur le bouton **Ajouter**.

Si vous ajoutez une clé de licence de base et que l'application est déjà activée, la nouvelle clé est ajoutée en tant que clé de base de réserve.

Si vous ajoutez une clé distincte pour une fonctionnalité supplémentaire, elle est ajoutée comme active, sauf si une clé pour cette fonctionnalité supplémentaire a déjà été ajoutée dans l'application. Une nouvelle clé pour des fonctionnalités supplémentaires est ajoutée en guise de réserve si une clé pour cette fonctionnalité supplémentaire a déjà été ajoutée à l'application.

> Si une clé active et une clé de réserve ont été précédemment ajoutées à l'application, la nouvelle clé remplace la clé de réserve précédemment ajoutée.

Il est impossible d'ajouter la clé de la licence d'évaluation et la clé d'abonnement en guise de clé de réserve.

Suppression de la clé de licence

Pour supprimer une clé de licence ajoutée à une application :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :
   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira.
3. Cliquez sur le bouton **Supprimer** situé à droite des informations sur la clé que vous souhaitez supprimer.
4. Confirmez la suppression dans la fenêtre qui s'ouvre.

Consultation des informations relatives à la licence

Pour consulter les informations sur la licence :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Exécutez une des actions suivantes :
   - Dans la partie inférieure de la fenêtre principale, cliquez dans la zone de la fenêtre qui contient les informations sur la licence ou la clé.
   - Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, cliquez sur le lien dans le champ **Clé de licence** ou à l'aide du lien **Licences** dans la partie inférieure de la fenêtre.

   La fenêtre **Licences** s'ouvrira.

   La fenêtre affiche des informations sur les clés actives et de réserve ajoutées à l'application. Cliquez sur le lien **En savoir plus** pour afficher des informations complètes sur les licences et les clés.

Le groupe **Licences actives** affiche des informations sur les clés actives ajoutées (la clé de base active et la clé active pour des fonctionnalités supplémentaires) et les licences qui leur sont associées :

- Type de licence, restriction de licence et période de validité de la licence.
- **Clé de licence** : séquence alphanumérique unique.
- **État de la clé** : état de la clé ou message relatif à un problème de clé quelconque (le cas échéant).

- **Valide à partir du** : date d'activation de l'application via l'ajout de cette clé.
- **Expire** : nombre de jours avant la date de fin de validité de la licence et date de fin de validité de la licence (UTC).
- **Nom** : nom de l'application que la clé est destinée à activer.
- **Protection** : informations sur les restrictions sur les fonctions de protection et la fonction de mise à jour des bases de données d'application.

Le groupe **Clés de réserve** affiche des informations sur les clés de réserve ajoutées (la clé de base de réserve et la clé de réserve pour des fonctionnalités supplémentaires) et les licences qui leur sont associées :

- Le type de clé de réserve, la restriction de licence et la période de validité de la licence associée à la clé.
- **Clé de licence** : séquence alphanumérique unique.
- **Type de licence** : type de licence associé à la clé de réserve.
- **Nom** : nom de l'application que la clé est destinée à activer.
- **Protection** : informations sur les restrictions sur les fonctions de protection et la fonction de mise à jour des bases de données d'application.

Obtention d'accès temporaire à l'appareil

Lors de la connexion d'un appareil bloqué par le Contrôle des appareils, une fenêtre s'ouvre avec un message vous informant que l'accès à l'appareil est bloqué.

Vous pouvez demander un accès temporaire à un appareil bloqué auprès de l'administrateur réseau local de votre organisation en utilisant l'interface graphique de la manière suivante :

- depuis la fenêtre affichant un message concernant le blocage de l'accès à l'appareil en cliquant sur le bouton **OK**.
- depuis la fenêtre principale de l'interface graphique de l'application.

Pour demander un accès temporaire à un appareil verrouillé :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Accès temporaire**.

   La fenêtre **Accès temporaire** s'ouvrira.

   Vous pouvez également ouvrir la fenêtre **Accès temporaire** à partir de la fenêtre affichant le message concernant le blocage de l'accès à l'appareil en cliquant sur le bouton **OK**.
3. Dans la section **Demander l'accès à un appareil bloqué**, dans la liste des appareils connectés, sélectionnez l'appareil auquel vous souhaitez accéder.
4. Dans le champ **Durée d'accès à l'appareil en heures**, spécifiez la période pendant laquelle vous souhaitez accéder à l'appareil (en heures).
5. Cliquez sur le bouton **Générer le fichier de demande**.

6. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.

7. Transmettez le fichier de demande d'accès à l'administrateur, par exemple par email ou tout autre moyen disponible (l'administrateur peut le préciser dans le modèle de message de blocage).

Une fois que vous aurez reçu la clé d'accès de l'administrateur, vous pourrez la télécharger pour obtenir un accès temporaire à l'appareil verrouillé.

Pour obtenir un accès temporaire à un appareil verrouillé :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.

2. Dans la partie inférieure de la fenêtre principale, cliquez sur bouton **Accès temporaire**.

   La fenêtre **Accès temporaire** s'ouvrira.

3. Dans la section **Accès à l'appareil**, cliquez sur le bouton **Télécharger la clé d'accès**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier contenant la clé d'accès à l'appareil (fichier clé avec l'extension .acode) reçue de l'administrateur du réseau local de l'organisation.

5. Une fenêtre s'ouvre affichant des informations sur l'appareil auquel l'accès a été accordé, ainsi que la durée de cet accès.

6. Cliquez sur le bouton **OK**.

Consultation des informations sur l'application

Vous pouvez afficher des informations sur l'application installée et sur l'appareil avec l'application installée dans la fenêtre **Assistance**, qui s'ouvre en cliquant sur le bouton **Assistance** situé en bas de la fenêtre principale de l'interface graphique de l'application.

La fenêtre **Assistance** affiche les informations suivantes :

- Version de l'application.

- **Clé de licence** : clé de licence de base active ajoutée à l'application, ou informations sur l'absence de clé. En utilisant le lien dans ce champ, vous pouvez ouvrir la fenêtre **Licences** qui affiche des informations détaillées sur la licence.

- **État de la clé** : informations sur l'état de la clé de licence de base active ou informations sur l'absence de clé.

- **Date de publication de la base de données** : état et date de publication des bases de données de l'application.

- **Système d'exploitation** : informations sur le système d'exploitation de l'appareil ;

- **Administration de l'application** : informations indiquant si l'appareil est sous gestion d'une stratégie.

Si le paramètre **L'application peut recevoir des données étendues de la stratégie sur le l'appareil** est activé dans la stratégie de l'Agent d'administration, la fenêtre affiche également les informations suivantes sur la stratégie appliquée sur l'appareil sur lequel l'application est installée.

- **Nom de la stratégie** : nom de la stratégie sous laquelle fonctionne l'appareil avec l'application installée.
- **Date d'application de la stratégie** : date et heure de la dernière application ou mise à jour de la stratégie sur l'appareil sur lequel l'application est installée.
- **Groupe d'administration** : nom du groupe d'administration qui inclut l'appareil sur lequel l'application est installée et exécutée sous la gestion des stratégies.
- **Profils actifs de la stratégie** : liste des profils actifs de la stratégie appliqués sur l'appareil (le cas échéant).

Les liens suivants apparaissent au bas de la fenêtre **Assistance** :

- **Licences** qui ouvre la fenêtre **Licences**, affichant des informations détaillées sur la licence.
- **Base de connaissances**, qui ouvre la page Base de connaissances.
- **Assistance**, qui ouvre la page Kaspersky CompanyAccount.
- Le **traçage** qui ouvre la fenêtre **Traçage**. Cette fenêtre vous permet de créer des fichiers de traçage de l'application et configurer le niveau de détail des fichiers de traçage.

  Pour suivre le lien **Traçage**, vous devez disposer des droits d'utilisateur avec le rôle Administrateur (admin).

Création d'un fichier de traçage

Vous pouvez créer des fichiers de traçage de l'application et configurer le niveau de détail des fichiers de traçage à l'aide d'une interface graphique.

La création et la configuration du niveau de détail du fichier de traçage nécessitent des privilèges d'utilisateur avec le rôle Administrateur (admin).

Pour créer un fichier de traçage :

1. Ouvrez la fenêtre principale de l'interface graphique de l'application.
2. Dans la partie inférieure de la fenêtre principale de l'application, cliquez sur bouton **Support**.

   La fenêtre **Support** s'ouvre.
3. Cliquez sur le lien **Traçage** pour ouvrir la fenêtre **Traçage**.
4. Dans la liste déroulante **Niveau**, sélectionnez le niveau de détail du fichier de traçage.

   Il est conseillé de préciser le niveau de détail requis auprès des experts du Support Technique de Kaspersky. La valeur par défaut est **Diagnostic (300)**.
5. Cliquez sur le bouton **Activer** pour démarrer le processus de traçage.

6. Reproduisez la situation dans laquelle vous rencontrez un problème.

7. Cliquez sur le bouton **Désactiver** pour arrêter le processus de traçage.

Les fichiers de traçage créés sont stockés dans le répertoire /var/log/kaspersky/kesl/.

Vérification de l'intégrité des modules d'application

L'application Kaspersky Endpoint Security contient une multitude de modules binaires variés sous forme de bibliothèques de liens dynamiques, de fichiers exécutables, de fichiers de configuration et de fichiers d'interface. Un pirate informatique peut remplacer un ou plusieurs modules ou fichiers exécutables de l'application par d'autres fichiers contenant du code malveillant. Pour empêcher ce remplacement des modules et des fichiers, Kaspersky Endpoint Security peut vérifier l'intégrité des modules de l'application. L'application recherche la présence de modifications non autorisées ou de dommages dans les modules et les fichiers. Si la somme de contrôle du module ou du fichier de l'application est incorrecte, celui-ci est considéré comme endommagé.

Un contrôle d'intégrité est effectué sur les modules d'application suivants, s'ils sont installés sur l'appareil :

- paquet de l'application ;
- paquet de l'interface utilisateur graphique ;
- paquet de l'Agent d'administration de Kaspersky Security Center
- le plug-in Internet d'administration de Kaspersky Endpoint Security
- le plug-in MMC d'administration de Kaspersky Endpoint Security

C'est à l'utilitaire de vérification de l'intégrité qu'il convient de vérifier l'intégrité des modules de l'application. L'utilitaire vérifie l'intégrité des fichiers repris dans des listes spéciales appelées *fichiers de manifeste*. Chaque module de l'application possède son propre fichier de manifeste. Celui reprend la liste des fichiers de l'application dont l'intégrité est importante au fonctionnement correct de ce module. Le nom du fichier de manifeste de chaque module est le même. Le contenu, quant à lui, diffère. Les fichiers de manifeste possèdent une signature numérique. Leur intégrité est vérifiée également.

Pour exécuter l'utilitaire de vérification de l'intégrité sur les appareils exécutant les systèmes d'exploitation Linux, un compte avec les droits root est requis. Un compte administrateur est requis pour exécuter l'utilitaire de vérification de l'intégrité sur les appareils exécutant les systèmes d'exploitation Windows.

L'utilitaire de vérification de l'intégrité est installé avec l'application et se trouve à l'emplacement suivant :

- Dans le cadre du paquet de l'application (integrity_checker) : /opt/kaspersky/kesl/bin/integrity_checker.
- Le plug-in MMC d'administration de Kaspersky Endpoint Security (integrity_checker.exe) comprend :
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<numéro de version>.plg\integrity_checker.exe : pour les systèmes d'exploitation 32 bits ;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<numéro de version>.plg\integrity_checker.exe : pour les systèmes d'exploitation 64 bits.

Les fichiers de manifeste se trouvent dans les emplacements suivants :

- Pour vérifier l'intégrité du paquet de l'application : /opt/kaspersky/kesl/bin/integrity_check.xml.
- Pour vérifier l'intégrité du paquet de l'interface utilisateur graphique : /opt/kaspersky/kesl/bin/gui_integrity_check.xml.
- Pour vérifier l'Agent d'administration :
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml : pour les systèmes d'exploitation 32 bits ;
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml : pour les systèmes d'exploitation 64 bits ;
- Pour vérifier le plug-in MMC d'administration de Kaspersky Endpoint Security :
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_check.xml : pour les systèmes d'exploitation 32 bits ;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_check.xml : pour les systèmes d'exploitation 64 bits.
- Pour vérifier le répertoire du plug-in Internet d'administration de Kaspersky Endpoint Security :
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kesl_<numéro de version>\integrity_check.xml : sur les appareils dotés de systèmes d'exploitation Windows ;
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kesl_<numéro de version>/integrity_check.xml : sur les appareils dotés de systèmes d'exploitation Linux.

Pour vérifier l'intégrité du module de la solution, vous devez exécuter l'utilitaire à partir du dossier d'emplacement de l'utilitaire pour ce module.

Pour exécuter l'utilitaire de vérification de l'intégrité, exécutez l'une des commandes suivantes :

- Pour effectuer la vérification de l'intégrité du paquet de l'application :

  ```
  integrity_checker [<chemin d'accès au fichier de manifeste>] --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- Pour vérifier l'intégrité du paquet de l'interface utilisateur graphique :

  ```
  integrity_checker <chemin d'accès au fichier de manifeste> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- pour vérifier l'intégrité du plug-in MMC d'administration de Kaspersky Endpoint Security :

  ```
  integrity_checker.exe [<chemin d'accès au fichier de manifeste>]
  ```

- Pour vérifier l'intégrité de l'Agent d'administration :

  ```
  integrity_checker <chemin d'accès au fichier de manifeste>
  ```

- Pour vérifier l'intégrité du répertoire du plug-in Internet d'administration de Kaspersky Endpoint Security :

  ```
  integrity_checker <chemin d'accès au fichier de manifeste> --crl
  /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds
  ```

  Par défaut, le chemin d'accès utilisé est celui du fichier de manifeste situé dans le répertoire où se trouve l'utilitaire de vérification de l'intégrité.

Vous pouvez démarrer l'utilitaire avec les paramètres facultatifs suivants :

- `--crl <répertoire>` est le chemin d'accès au répertoire contenant la liste de révocation des certificats.
- `--verbose` : affichage détaillé des actions effectuées et des résultats. Si vous ne spécifiez pas ce paramètre, seules les erreurs, les objets qui n'ont pas réussi la vérification et les statistiques de l'analyse récapitulative seront fournis.
- `--trace <nom de fichier>`, où `<nom de fichier>` est le nom du fichier dans lequel les événements qui se produisent pendant les analyses seront consignés au niveau de détail DEBUG.
- `--signature-type kds` correspond au type de signature à vérifier (ce paramètre est requis pour analyser le répertoire du plug-in Internet d'administration de Kaspersky Endpoint Security).
- `--signature-type kds-with-filename` : type de signature à vérifier (ce paramètre est indispensable pour vérifier le paquet de l'application, le paquet d'interface utilisateur graphique).
- `--single-file <fichier>` vérifie uniquement le fichier spécifié dans le manifeste et ignore tous les autres objets du manifeste.
- `--version` : afficher la version de l'utilitaire sans effectuer de vérification de l'intégrité.

Vous pouvez consulter la description de tous les paramètres disponibles pour l'utilitaire de vérification de l'intégrité en exécutant la commande `integrity_checker --help`.

Le résultat de la vérification du fichier de manifeste s'affiche de la manière suivante :

- `SUCCEEDED` : l'intégrité des fichiers est confirmée (code retour 0).
- `FAILED` : l'intégrité des fichiers n'est pas confirmée (le code retour n'est pas 0).

En cas de violation de l'intégrité de l'application ou de l'Agent d'administration lors du lancement de l'application, l'application Kaspersky Endpoint Security génère l'événement à ce sujet dans le journal des événements et dans Kaspersky Security Center.

Contacter le Support technique

Si la solution à votre problème ne figure pas dans la documentation de l'application ou dans une des sources d'informations consacrées à l'application, nous vous conseillons de contacter le Support technique de Kaspersky. Les experts du Support technique répondront à toutes vos questions sur l'installation et l'utilisation de Kaspersky Endpoint Security.

Kaspersky offre une assistance pour Kaspersky Endpoint Security tout au long de son cycle de vie (cf. la page consacrée au cycle de vie des applications). 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 :

- visiter le site Internet du Support technique ;
- envoyer une demande au Support technique de Kaspersky via le portail Kaspersky CompanyAccount.

Support technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail à disposition des entreprises qui utilisent les applications de Kaspersky. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les experts de Kaspersky via des requêtes électroniques. Le portail Kaspersky CompanyAccount vous permet de suivre l'état du traitement des requêtes électroniques par les experts de Kaspersky et de stocker l'historique des requêtes électroniques.

Vous pouvez inscrire tous les employés de votre entreprise sous un seul compte dans Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de gérer de manière centralisée les demandes électroniques envoyées à Kaspersky par les employés enregistrés et de gérer les autorisations de ces employés via Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Pour en savoir plus sur Kaspersky CompanyAccount, veuillez consulter le site Internet du Support technique.

Obtention d'informations pour le Support technique

Après que vous avez informé les spécialistes du Support technique de Kaspersky du problème, ceux-ci peuvent vous demander d'envoyer *un fichier de traçage* ou *un fichier de vidage*.

En outre, les spécialistes du Support technique peuvent avoir besoin d'informations supplémentaires sur le système d'exploitation, les processus en cours d'exécution sur l'appareil et des rapports détaillés sur le fonctionnement des modules de l'application.

Lors des diagnostics, les spécialistes du Support technique peuvent vous demander de modifier les paramètres de l'application :

- activer la fonctionnalité d'obtention d'informations de diagnostic étendues ;
- affiner le fonctionnement des modules individuels de l'application, ce qui n'est pas disponible via les outils d'interface utilisateur standard ;
- modifier les paramètres de stockage des informations de diagnostic obtenues ;
- configurer l'interception du trafic réseau et l'enregistrement dans un fichier.

Toutes les informations nécessaires à l'exécution des actions ci-dessus (une description de la séquence des étapes, les paramètres modifiables, les fichiers de configuration, les scripts, les options de ligne de commande supplémentaires, les modules de débogage, les utilitaires spécialisés, etc.), ainsi que la composition des données obtenues à des fins de débogage, vous seront communiquées par les spécialistes du Support technique. Les informations de diagnostic étendues obtenues sont stockées sur l'appareil de l'utilisateur. Les données obtenues ne sont pas automatiquement envoyées à Kaspersky.

Il est conseillé de réaliser les opérations citées ci-dessus en suivant les instructions des spécialistes du Support technique. Si vous décidez de modifier vous-même les fichiers de l'application d'une manière non décrite dans la documentation de l'application ou dans les recommandations des spécialistes du Support technique, ces modifications pourraient entraîner des ralentissements et des pannes dans le fonctionnement de l'application et du système d'exploitation, une diminution du niveau de protection de votre appareil, ainsi qu'une violation de la disponibilité et de l'intégrité des informations traitées.

À propos des fichiers de traçage de l'application

Le *fichier de traçage* de l'application Kaspersky Endpoint Security vous permet de suivre l'exécution étape par étape des commandes de l'application et de détecter à quelle étape de l'application une erreur se produit.

Par défaut, les fichiers de traçage de l'application ne sont pas générés. Vous pouvez activer ou désactiver la création des fichiers de traçage de l'application et configurer le niveau de détails des fichiers de traçage dans la ligne de commande à l'aide des paramètres généraux de l'application ainsi qu'à l'aide de l'interface utilisateur graphique.

Si vous avez activé la création des fichiers de traçage de l'application, les fichiers de traçage sont conservés par défaut dans le répertoire /var/log/kaspersky/kesl/. Les privilèges root sont requis pour accéder à ce répertoire.

Le stockage des fichiers de traçage de l'application nécessite un espace disque supplémentaire au-delà de celui spécifié dans la configuration matérielle minimale requise.

Les fichiers de traçage sont stockés sur l'appareil aussi longtemps que l'application est en cours d'utilisation et sont supprimés définitivement lorsque l'application est supprimée. Les fichiers de traçage ne sont pas automatiquement envoyés à Kaspersky.

Les fichiers de traçage sont stockés sous une forme lisible. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Contenu des fichiers de traçage de l'application

Les fichiers de traçage contiennent les informations générales suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.
- 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.

Les fichiers de traçage peuvent stocker les informations suivantes en plus des données générales :

- États des modules de l'application et de leurs données d'exploitation.
- Données sur les actions des utilisateurs dans l'application.
- Données sur le matériel installé sur l'appareil.
- Données sur tout objet et événement du système d'exploitation, mais également des informations sur l'activité des utilisateurs.
- Données contenues dans les objets du système d'exploitation (par exemple, le contenu des fichiers qui peuvent contenir des données personnelles de l'utilisateur).
- données de trafic réseau (pour exemple, le contenu des champs de saisie sur un site internet, comme des informations de carte bancaire ou toutes autres données confidentielles) ;
- Données reçues des serveurs de Kaspersky (telles que la version des bases de l'application).
- données reçues des serveurs KATA, des serveurs OSMP, des serveurs NDR et des serveurs qui assurent l'interaction avec Sandbox ;

- données sur les ressources CPU consommées ;
- données sur les ressources RAM consommées ;
- données sur les opérations de lecture et d'écriture de fichiers par les applications ;
- données sur la quantité d'informations mises en cache nécessaires au fonctionnement de l'application.

Configuration des paramètres de trace de l'application

Si vous gérez l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez configurer les paramètres de traçage de l'application dans les paramètres de la stratégie de Kaspersky Endpoint Security à l'aide de Web Console ou de la Console d'administration.

Si vous gérez votre application via la ligne de commande, vous pouvez configurer les paramètres de traçage de l'application dans les paramètres généraux de l'application.

Configuration des paramètres de traçage dans Web Console

Dans Web Console, vous pouvez gérer les paramètres de traçage de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Assistance technique**).

Vous devez redémarrer l'application pour appliquer les paramètres de traçage.

Configuration des paramètres de traçage dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de traçage de l'application dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Paramètres de l'application**).

Dans le groupe **Paramètres de traçage et d'enregistrement des vidages**, cliquer sur le lien **Configurer** pour ouvrir la fenêtre dans laquelle vous pouvez configurer les paramètres de traçage (cf. le tableau ci-dessous).

Paramètres de traçage de l'application

Paramètre	Description
Chemin d'accès au répertoire contenant les fichiers de traçage	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de traçage sont stockés. Valeur par défaut : /var/log/kaspersky/kesl. Si vous indiquez un autre répertoire, assurez-vous que l'utilisateur qui exécute Kaspersky Endpoint Security dispose des autorisations de lecture et d'écriture pour ce répertoire. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root.
Taille maximale du fichier de traçage (Mo)	Dans ce champ, vous pouvez saisir la taille maximale d'un fichier de traçage d'application (en mégaoctets). Valeur par défaut : 500.
Nombre maximum de fichiers de traçage	Dans ce champ, vous pouvez saisir le nombre maximal de fichiers de traçage d'application. Valeur par défaut : 10.

Vous devez redémarrer l'application pour appliquer les paramètres de traçage.

Configuration des paramètres de traçage dans la ligne de commande

Dans la ligne de commande, vous pouvez configurer les paramètres de traçage de l'application à l'aide des paramètres `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` et `TraceMaxFileSize` dans les paramètres généraux de l'application.

Le paramètre `TraceLevel` permet d'activer ou de désactiver la génération des fichiers de traçage de l'application et de préciser le niveau de détail dans les fichiers de traçage. Le paramètre peut prendre les valeurs suivantes :

- `Detailed` : crée un fichier de traçage détaillé.
- `MediumDetailed` : crée un fichier de traçage contenant des messages d'information et d'erreur.
- `NotDetailed` : crée un fichier de traçage contenant des notifications relatives aux erreurs.
- `None` (valeur par défaut) : ne crée pas de fichier de traçage.

Le paramètre `TraceFolder` permet de spécifier le répertoire dans lequel sont stockés les fichiers de trace de l'application. Valeur par défaut : /var/log/kaspersky/kesl. Si vous indiquez un autre répertoire, assurez-vous qu'il est autorisé à être lu et écrit uniquement par le compte sous lequel Kaspersky Endpoint Security s'exécute (droits rwx------- 700). L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root.

Le paramètre `TraceMaxFileCount` permet de spécifier le nombre maximum de fichiers de traçage de l'application. Le paramètre peut prendre des valeurs de 1 à 10000. Valeur par défaut : 10.

Le paramètre `TraceMaxFileSize` permet de spécifier la taille maximale du fichier de traçage de l'application (en mégaoctets). Le paramètre peut prendre des valeurs de 1 à 1000. Valeur par défaut : 500.

Vous pouvez modifier la valeur des paramètres à l'aide de commutateurs de ligne de commande ou à l'aide d'un fichier de configuration contenant tous les paramètres généraux de l'application.

Après avoir modifié les valeurs des paramètres `TraceFolder`, `TraceMaxFileCount`, `TraceMaxFileSize`, vous devez redémarrer l'application.

À propos des fichiers de traçage du plug-in d'administration des applications

Les fichiers de trace du plug-in d'administration ne sont pas automatiquement envoyés à Kaspersky.

Les fichiers de traçage sont stockés sous une forme lisible. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Fichiers de trace du plug-in mmc d'administration

Si vous utilisez la Console d'administration pour administrer l'application Kaspersky Endpoint Security, les informations sur les événements survenus lors de l'exécution du plug-in d'administration MMC peuvent être enregistrées dans le fichier de trace du plug-in MMC de Kaspersky Endpoint Security sur l'appareil sur lequel se trouve le Serveur d'administration. Le nom du fichier contient le numéro de version de l'application, la date et l'heure de création du fichier ainsi que l'ID du processus (PID). Ce fichier enregistre des informations sur les événements qui se produisent lors du fonctionnement du plug-in MMC, en particulier sur le fonctionnement des stratégies et des tâches.

Par défaut, les fichiers de trace du plug-in MMC ne sont pas créés. Vous pouvez créer un fichier de trace du plug-in MMC à l'aide de clés de registre. Pour des informations détaillées sur la création de fichiers de traçage, vous pouvez contacter le Support technique.

Tous les fichiers de trace du plug-in MMC générés se trouvent dans le dossier spécifié par l'utilisateur lors de la définition des clés de registre.

Fichiers de traçage du plug-in Internet d'administration

Si vous utilisez Web Console pour administrer l'application Kaspersky Endpoint Security, les informations sur les événements qui se produisent lors du fonctionnement du plug-in d'administration Web peuvent être enregistrées dans les fichiers de traçage du plug-in Web.

Les fichiers de traçage du plug-in Internet sont créés automatiquement si la connexion au journal d'activité de Web Console est activée dans l'Assistant d'installation de Web Console (pour plus de détails, consultez l'aide de Kaspersky Security Center).

Les fichiers de traçage du plug-in Internet sont enregistrés dans le dossier d'installation de Web Console, dans le sous-dossier des journaux.

Contenu des fichiers de trace du plug-in d'administration

Les fichiers de traçage contiennent les informations générales suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.
- 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.

En plus des données générales, les fichiers de traçage peuvent contenir les informations suivantes :

- les données personnelles, notamment nom, prénom et patronyme, si ces données font partie du chemin d'accès aux fichiers ;
- le nom du compte de connexion au système d'exploitation, si le nom du compte fait partie du nom du fichier.

À propos des fichiers de vidage

Un *fichier de vidage* contient toutes les informations sur la mémoire de travail des processus de l'application Kaspersky Endpoint Security au moment de la création du fichier de vidage.

Les fichiers de vidage peuvent contenir des données personnelles. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Par défaut, aucun fichier de vidage n'est créé. Vous pouvez activer ou désactiver l'enregistrement des vidages lorsqu'une application plante.

Si vous avez activé l'enregistrement des vidages mémoire, les fichiers de vidage sont stockés par défaut dans les répertoires suivants :

- /var/opt/kaspersky/kesl/common/dumps (fichiers de vidage du processus kesl) ;
- /var/opt/kaspersky/kesl/common/dumps-user (fichiers de vidage du processus utilisateur).

L'accès au répertoire de stockage des fichiers de vidage défini par défaut requiert les autorisations root. Vous pouvez spécifier un répertoire différent pour stocker les fichiers de vidage du processus kesl. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).

Le stockage des fichiers de vidage nécessite un espace disque supplémentaire au-delà de celui spécifié dans la configuration matérielle minimale requise.

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 ne sont pas automatiquement envoyés à Kaspersky.

Configuration des paramètres d'enregistrement des vidages

Si vous gérez l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez configurer les paramètres d'enregistrement des vidages dans les paramètres de la stratégie de Kaspersky Endpoint Security à l'aide de Web Console ou de la Console d'administration.

Si vous exécutez votre application via la ligne de commande, vous pouvez activer ou désactiver l'enregistrement du dump à l'aide du fichier de configuration kesl.ini.

Le nombre de fichiers de vidage maximal est limité.

En fonction des paramètres de votre système d'exploitation, les fichiers de vidage personnalisés peuvent ne pas être créés. Assurez-vous que la valeur du paramètre sysctl est `sysctl kernel.yama.ptrace_scope=0`.

Configuration des paramètres d'enregistrement des vidages dans Web Console

Dans Web Console, vous pouvez gérer les paramètres du fichier de vidage de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Assistance technique**).

Les paramètres d'enregistrement des vidages dans les propriétés de la stratégie de Web Console sont décrits dans l'Annexe 5.

Vous devez redémarrer l'application pour appliquer les paramètres d'enregistrement des vidages.

Configuration des paramètres d'enregistrement des vidages dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer les paramètres de vidage de l'application dans les propriétés de la stratégie (Gestion des stratégies dans la Console d'administration, Création d'une stratégie à l'aide de la Console d'administration) (**Contrôles de sécurité** → **Paramètres de l'application**).

Sous **Paramètres de traçage et d'enregistrement des vidages**, cliquez sur **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez modifier les paramètres d'enregistrement des vidages (voir le tableau ci-dessous).

Paramètres d'enregistrement de vidage

Paramètre	Description
Créer un fichier des vidages en cas de plantage de l'application	La case active ou désactive la création d'un fichier de vidage lorsque l'application plante. La case est décochée par défaut.
Chemin d'accès au répertoire contenant les fichiers de vidage	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de vidage sont stockés. La taille du champ de saisie est limitée à 128 caractères. Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps.

Vous devez redémarrer l'application pour appliquer les paramètres d'enregistrement des vidages.

Configuration de l'enregistrement des vidages dans la ligne de commande

Pour configurer l'enregistrement des vidages à l'aide du fichier de configuration kesl.ini :

1. Démarrez Kaspersky Endpoint Security.
2. Ouvrez le fichier /var/opt/kaspersky/kesl/common/kesl.ini pour le modifier.

3. Dans la section **[General]**, définissez la valeur du paramètre :

   - `CoreDumps=yes` : activer l'enregistrement des vidages lorsque l'application plante.
   - `CoreDumps=no` : désactiver l'enregistrement des vidages.

4. Si vous souhaitez modifier le répertoire par défaut dans lequel les fichiers de vidage sont enregistrés, spécifiez le chemin d'accès au répertoire dans le paramètre `CoreDumpsPath`.

5. Lancez Kaspersky Endpoint Security.

Diagnostic à distance de l'appareil à l'aide de Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez effectuer des diagnostics à distance des appareils clients. La procédure de diagnostic à distance permet d'effectuer les opérations suivantes à distance :

- activer et désactiver le traçage ;
- modifier le niveau de traçage ;
- télécharger des fichiers de traçage ;
- télécharger le journal d'installation à distance de l'application ;
- télécharger les journaux d'événements système (syslog) ;
- démarrer, arrêter et redémarrer les applications.

Diagnostics à distance à l'aide de Web Console

Si vous gérez l'application Kaspersky Endpoint Security via Web Console, les diagnostics à distance de l'appareil client sont effectués dans la fenêtre des diagnostics à distance.

Pour ouvrir la fenêtre de diagnostic à distance de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Sélectionnez l'appareil pour lequel vous souhaitez effectuer des diagnostics à distance et cliquez sur le lien <nom de l'appareil>.

   La fenêtre des propriétés de l'appareil s'ouvrira.

3. Sous l'onglet **Avancés**, sélectionnez la section **Diagnostics à distance**.

Dans la fenêtre de diagnostic à distance de l'appareil, vous pouvez consulter le journal d'installation à distance de l'application.

Pour afficher le journal d'installation d'applications à distance sur un appareil :

1. Ouvrez la fenêtre de diagnostic à distance de l'appareil.
2. Sous l'onglet **Journaux d'événements**, dans le groupe **Fichiers de traçage**, cliquez sur le lien **Journaux d'installation à distance**.

   La fenêtre **Journaux d'événements de traçage de l'appareil** s'ouvre.

Pour plus d'informations sur le diagnostic à distance, consultez l'aide de Kaspersky Security Center.

Diagnostics à distance à l'aide de la Console d'administration

Si vous gérez l'application Kaspersky Endpoint Security via la Console d'administration, les diagnostics à distance sont effectués à l'aide de l'utilitaire spécial de diagnostic à distance de Kaspersky Security Center, qui est automatiquement installé sur l'appareil avec la Console d'administration.

Pour ouvrir la fenêtre principale de l'utilitaire de diagnostic des appareils distants :

1. Dans l'arborescence de la Console d'administration, dans le dossier **Appareils administrés**, sélectionnez le groupe d'administration qui inclut l'appareil dont vous avez besoin.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Dans la liste des appareils administrés, sélectionnez l'appareil auquel vous souhaitez connecter l'utilitaire de diagnostic à distance, et dans le menu contextuel de l'appareil, sélectionnez **Outils externes → Diagnostics à distance**.

   La fenêtre principale de l'**utilitaire de diagnostic à distance Kaspersky Security Center** s'ouvrira.

À l'aide de l'utilitaire des diagnostics à distance de l'appareil, vous pouvez afficher le journal de l'installation à distance de l'application.

Pour afficher le journal d'installation d'applications à distance sur un appareil :

1. Ouvrez la fenêtre principale de l'utilitaire de diagnostic à distance de l'appareil.
2. Si nécessaire, configurez les paramètres de connexion de l'utilitaire à l'appareil. Dans la fenêtre principale de l'utilitaire de diagnostic à distance, cliquez sur le bouton **Connexion**.
3. Dans la fenêtre qui s'ouvre, dans l'arborescence des objets, sélectionnez le dossier **Journaux d'installation à distance**.

Pour en savoir plus sur l'utilitaire de diagnostic à distance, consultez l'aide de Kaspersky Security Center.

Annexes

Cette section contient des renseignements qui viennent compléter le contenu principal de l'aide.

Annexe 1. Commandes de gestion de Kaspersky Endpoint Security

L'application Kaspersky Endpoint Security est gérée à partir de la ligne de commande à l'aide des commandes de gestion de Kaspersky Endpoint Security.

Vous pouvez afficher l'aide sur les commandes de gestion à l'aide de la commande :

```
kesl-control --help <préfixe du groupe de commandes>
```

où <préfixe du groupe de commandes> peut prendre les valeurs suivantes :

- -A : commandes de gestion par le contrôle des applications.
- -B – commandes de gestion de la sauvegarde.
- -C : commandes de gestion des paramètres généraux de l'Analyse du conteneur (Analyse du conteneur, Surveillance des conteneurs)
- -D : commandes de gestion par le contrôle des appareils.
- -E : commandes de gestion des événements de l'application (Affichage des événements en ligne de commande, Consultation des événements dans Kaspersky Security Center)
- -F : commandes de gestion du pare-feu.
- -H : commandes de gestion pour les appareils bloqués.
- -J : commandes de gestion de la collecte des métriques sur l'état du système d'exploitation.
- -L – commandes de gestion des clés de licence.
- -M : commandes de gestion des paramètres d'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Unified Monitoring and Analysis Platform.
- -N : commandes de gestion des paramètres d'analyse du trafic réseau.
- -Q : commandes de gestion de la quarantaine.
- -R : commandes de gestion permettant de gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) et Kaspersky Endpoint Detection and Response Optimum.
- -S : commandes des statistiques.

- -T : commandes pour gérer les tâches et les paramètres de l'application.
- -U : commandes pour gérer les utilisateurs et les rôles des utilisateurs.
- -V : commandes d'application en mode Light Agent pour protéger les environnements virtuels.
- -W : commandes de sortie des événements (Affichage des événements en ligne de commande, Consultation des événements dans Kaspersky Security Center)
- -X : commandes de gestion des paramètres d'intégration de l'application Kaspersky Endpoint Security avec Sandbox.

Commandes de gestion des paramètres et des tâches de l'application

Le préfixe -T indique que la commande appartient au groupe de commandes de gestion des paramètres et des tâches de l'application.

Le préfixe -C indique que la commande appartient au groupe de commandes de gestion des paramètres d'analyse du conteneur (Analyse du conteneur, Surveillance des conteneurs).

Le préfixe -N indique que la commande appartient au groupe des commandes de gestion des paramètres d'analyse du trafic réseau.

Commande kesl-control --export-settings

Cette commande affiche tous les paramètres de l'application dans la console ou les exporte vers un fichier de configuration. Cela comprend les paramètres généraux de l'analyse du conteneur, les paramètres d'analyse des connexions chiffrées, les paramètres généraux de l'application et les paramètres des tâches.

Syntaxe de la commande

```
kesl-control [-T] --export-settings [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration dans lequel les paramètres de l'application seront enregistrés.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --import-settings

La commande vous permet d'importer tous les paramètres de l'application à partir du fichier de configuration (y compris les paramètres généraux de l'analyse du conteneur, les paramètres de l'analyse des connexions sécurisées, les paramètres généraux de l'application et les paramètres des tâches).

Syntaxe de la commande

```
kesl-control [-T] --import-settings --file <chemin d'accès au fichier de configuration>
[--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés dans l'application.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --update-application

La commande vous permet d'installer la mise à jour du module de l'application téléchargée.

> La commande ne peut pas être exécutée si l'application est utilisée en mode Light Agent.

Syntaxe de la commande

```
kesl-control [-T] --update-application
```

Commandes de gestion des paramètres généraux de l'application

Commande kesl-control --get-app-settings

La commande vous permet d'afficher les valeurs actuelles des paramètres généraux de l'application sur la console ou le fichier de configuration.

Syntaxe de la commande

```
kesl-control [-T] --get-app-settings [--file <chemin d'accès au fichier de
configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'application seront écrits. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --set-app-settings

La commande vous permet de définir les valeurs des paramètres généraux de l'application à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

Syntaxe de la commande

Définir les paramètres à l'aide des clés de commande :

```
kesl-control [-T] --set-app-settings <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

Définir les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-T] --set-app-settings --file <chemin d'accès au fichier de configuration> [--json]
```

Arguments et clés

`<nom du paramètre>=<valeur du paramètre>` correspond au nom et à la valeur de l'un des paramètres généraux de l'application.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés dans l'application.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des paramètres des tâches

Commande kesl-control --get-settings

La commande vous permet d'afficher les valeurs actuelles des paramètres de la tâche spécifiée sur la console ou le fichier de configuration.

Syntaxe de la commande

`kesl-control [-T] --get-settings <ID/nom de la tâche> [--file <chemin d'accès au fichier de configuration>] [--json]`

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres de la tâche seront écrits. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --set-settings

La commande vous permet de définir les valeurs des paramètres de la tâche spécifiée à l'aide des touches de commande ou en important des paramètres à partir d'un fichier de configuration spécifié.

Syntaxe de la commande

Définir les paramètres à l'aide des clés de commande :

`kesl-control [-T] --set-settings <ID/nom de la tâche> <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>] [--add-path <chemin d'accès>] [--del-path <chemin d'accès>] [--add-exclusion <chemin d'accès>] [--del-exclusion <chemin d'accès>]`

Définir les paramètres à l'aide d'un fichier de configuration :

`kesl-control [-T] --set-settings <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]`

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur de l'un des paramètres de la tâche.

`--add-path <chemin d'accès>` ajoute un chemin d'accès à un répertoire contenant les objets à analyser.

`--del-path <chemin d'accès>` supprime un chemin d'accès à un répertoire contenant les objets à analyser.

`--add-exclusion <chemin d'accès>` ajoute un chemin d'accès à un répertoire contenant les objets à exclure de l'analyse.

`--del-exclusion <chemin d'accès>` supprime un chemin d'accès à un répertoire contenant les objets à exclure de l'analyse.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration depuis lequel les paramètres de la tâche seront importés.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --set-to-default

La commande vous permet de restaurer les valeurs par défaut des paramètres de la tâche spécifiée.

Syntaxe de la commande

```
kesl-control [-T] --set-settings <ID/nom de la tâche> --set-to-default
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

Commande kesl-control --get-schedule

La commande permet d'afficher le planification de lancement actuel de la tâche spécifiée dans la console ou dans un fichier de configuration.

Syntaxe de la commande

```
kesl-control [-T] --get-schedule <ID/nom de la tâche> [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres de planification de la tâche seront écrits. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --set-schedule

La commande vous permet de définir la planification d'une tâche spécifiée à l'aide des touches de commande ou en important des paramètres à partir d'un fichier de configuration spécifié.

Syntaxe de la commande

Définir les paramètres à l'aide des clés de commande :

```
kesl-control [-T] --set-schedule <ID/nom de la tâche> <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

Définir les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-T] --set-schedule <ID/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur de l'un des paramètres de planification de la tâche.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres de planification de la tâche seront importés.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des tâches

Commande kesl-control --get-task-list

La commande permet d'afficher une liste des tâches existantes de l'application.

Syntaxe de la commande

```
kesl-control [-T] --get-task-list [--json]
```

Arguments et clés

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --get-task-state

La commande vous permet d'afficher l'état de la tâche spécifiée.

Syntaxe de la commande

```
kesl-control [-T] --get-task-state <ID/nom de la tâche> [--json]
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --create-task

La commande vous permet de créer une tâche de type spécifié avec des paramètres par défaut ou avec des paramètres spécifiés dans le fichier de configuration.

Syntaxe de la commande

Créez une tâche avec les paramètres par défaut :

```
kesl-control [-T] --create-task <nom de la tâche> --type <type de tâche>
```

Créez une tâche avec les paramètres du fichier de configuration :

```
kesl-control [-T] --create-task <nom de la tâche> --type <type de tâche> [--file
<chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`<nom de la tâche>` est le nom que vous attribuez à la nouvelle tâche.

`<type de tâche>` est la désignation du type de tâche que vous créez.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration contenant les paramètres qui seront utilisés pour créer la tâche.

`--json` indique que les paramètres doivent être importés depuis le fichier de configuration au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --delete-task

La commande permet de supprimer la tâche.

Syntaxe de la commande

```
kesl-control [-T] --delete-task <ID/nom de la tâche>
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

Commande kesl-control --start-task

La commande vous permet de lancer la tâche.

Syntaxe de la commande

```
kesl-control [-T] --start-task <ID/nom de la tâche> [-W] [--progress]
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`[-W]` – activer l'affichage des événements en cours.

`[--progress]` : afficher la progression de la tâche.

Commande kesl-control --stop-task

La commande permet d'arrêter la tâche.

Syntaxe de la commande

```
kesl-control [-T] --stop-task <ID/nom de la tâche> [-W]
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

`[-W]` – activer l'affichage des événements en cours.

Commande kesl-control --suspend-task

La commande vous permet de suspendre la tâche.

Syntaxe de la commande

```
kesl-control [-T] --suspend-task <ID/nom de la tâche>
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

Commande kesl-control --resume-task

La commande permet de reprendre l'exécution d'une tâche.

Syntaxe de la commande

```
kesl-control [-T] --resume-task <ID/nom de la tâche>
```

Arguments et clés

`<ID/nom de la tâche>` est l'ID attribué à la tâche lors de sa création, ou le nom de la tâche sur la ligne de commande.

Commande kesl-control --scan-file

La commande vous permet de créer et d'exécuter une tâche d'analyse personnalisée.

Syntaxe de la commande

```
kesl-control [-T] --scan-file <chemin d'accès> [--action <action>]
```

Arguments et clés

`<chemin>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

`--action <action>` est l'action que l'application doit exécuter sur les objets infectés. Si vous ne spécifiez pas la clé `--action` , l'application effectuera l'action recommandée.

Commande kesl-control --scan-container my_container

La commande vous permet de créer et d'exécuter une tâche d'analyse personnalisée du conteneur ou de l'image.

Syntaxe de la commande

```
kesl-control [-T] --scan-container <ID/nom[:tag]>
```

Arguments et clés

< ID/nom [: tag]> désigne le nom ou l'ID du conteneur ou de l'image. Vous pouvez utiliser des **masques** pour analyser plusieurs objets.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque de nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère / dans le nom du fichier ou du répertoire. Par exemple, /dir/*/file ou /dir/*/*/file.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, /dir/**/file*/ ou /dir/file**/.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/file est un masque incorrect.

Vous pouvez utiliser le symbole ? au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Commandes pour contrôler la prévention du lancement des objets

Commande kesl-control --get-prevention-state

La commande permet d'afficher sur la console les règles de prévention du lancement des objets reçus du module spécifié.

Syntaxe de la commande

```
kesl-control [-T] --get-prevention-state [--kata|--edro]
```

Arguments et clés

--kata : règles de la prévention du lancement des objets du module EDR Expert (on-premises).

--edro : règles de prévention du lancement des objets du module EDR Optimum.

Commandes de gestion des paramètres généraux d'analyse du conteneur

Commande kesl-control --get-container-settings

La commande permet d'afficher les valeurs actuelles des paramètres généraux de l'analyse du conteneur dans la console ou dans un fichier de configuration.

Syntaxe de la commande

```
kesl-control [-C] --get-container-settings [--file < chemin d'accès au fichier de
configuration >] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'Analyse du conteneur seront enregistrés. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --set-container-settings

La commande vous permet de définir les valeurs des paramètres généraux de l'analyse du conteneur à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

Syntaxe de la commande

Définir les paramètres à l'aide des clés de commande :

```
kesl-control [-C] --set-container-settings <nom du paramètre>=<valeur du paramètre>
[<nom du paramètre>=<valeur du paramètre>]
```

Définir les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-C] --set-container-settings --file <chemin d'accès au fichier de
configuration> [--json]
```

Arguments et clés

`<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur d'un des paramètres généraux de l'Analyse du conteneur.

`--file <chemin d'accès au fichier de configuration>` est le chemin complet vers le fichier de configuration à partir duquel les paramètres généraux de l'Analyse du conteneur seront importés dans l'application.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commandes de gestion des paramètres d'analyse du trafic réseau

Le préfixe -N indique que la commande appartient au groupe des commandes de gestion des paramètres d'analyse du trafic réseau.

Commande kesl-control -N --query

La commande permet d'afficher des listes d'exclusions à l'analyse des connexions chiffrées :

- liste des exclusions ajoutées par l'utilisateur ;
- liste des exclusions ajoutées par l'application ;
- une liste des exclusions reçues des bases de données de l'application.

Syntaxe de la commande

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

Commande kesl-control --clear-web-auto-excluded

La commande vous permet d'effacer la liste des domaines que l'application a automatiquement exclus de l'analyse.

Syntaxe de la commande

```
kesl-control -N --clear-web-auto-excluded
```

Commande kesl-control --get-net-settings

La commande permet d'afficher les valeurs actuelles des paramètres d'analyse du trafic réseau à la console ou à un fichier de configuration.

Syntaxe de la commande

```
kesl-control [-N] --get-net-settings [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration dans lequel les paramètres d'analyse du trafic réseau seront enregistrés. Si vous ne spécifiez pas la clé `--file`, les paramètres seront affichés dans la console.

Si vous spécifiez un nom de fichier sans chemin, le fichier sera créé dans le répertoire courant. Si le fichier existe dans le chemin spécifié, il sera écrasé. Si le répertoire spécifié n'existe pas, le fichier de configuration ne sera pas créé.

`--json` : afficher les paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

Commande kesl-control --set-net-settings

La commande vous permet de définir les valeurs des paramètres d'analyse du trafic réseau à l'aide des touches de commande ou en important des paramètres à partir du fichier de configuration spécifié.

Syntaxe de la commande

Définir les paramètres à l'aide des clés de commande :

```
kesl-control [-N] --set-net-settings <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

Définir les paramètres à l'aide d'un fichier de configuration :

```
kesl-control [-N] --set-net-settings --file <chemin d'accès au fichier de configuration> [--json]
```

Arguments et clés

`<nom du paramètre>=<valeur du paramètre>` correspondent au nom et à la valeur d'un des paramètres d'analyse du trafic réseau.

`--file <chemin d'accès au fichier de configuration>` est le chemin complet vers le fichier de configuration à partir duquel les paramètres d'analyse du trafic réseau seront importés.

`--json` : importer les paramètres du fichier de configuration dans l'application au format JSON. Si vous ne spécifiez pas la clé `--json`, l'application tente de réaliser l'importation depuis un fichier au format INI. Si l'importation échoue, une erreur s'affiche.

Commande kesl-control --list-certificates

La commande permet d'afficher une liste des certificats racines de confiance.

Syntaxe de la commande

```
kesl-control [-N] --list-certificates
```

Commande kesl-control --add-certificate

La commande vous permet d'ajouter un certificat à la liste des certificats racines de confiance.

Syntaxe de la commande

```
kesl-control [-N] --add-certificate <chemin d'accès au certificat>
```

Arguments et clés

< chemin d'accès au certificat > est le chemin d'accès au fichier de certificat que vous voulez ajouter (au format PEM ou DER).

Commande kesl-control --remove-certificate

La commande permet de supprimer un certificat de la liste des certificats racines de confiance.

Syntaxe de la commande

```
kesl-control [-N] --remove-certificate < objet du certificat >
```

Commande kesl-control --add-bypass-endpoints

La commande vous permet d'ajouter une exclusion à l'interception du trafic.

Syntaxe de la commande

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip < adresse IP distante > --dst-port < port de destination >
```

Arguments et clés

<in|out> est la direction du trafic dans la connexion exclue, sortant ou entrant.

< adresse IP distante > est l'adresse IPv4 ou IPv6 de l'appareil distant. Lors de l'exclusion du trafic entrant de l'interception, le trafic provenant de l'adresse IP spécifiée sera exclu. Lors de l'exclusion du trafic sortant de l'interception, le trafic vers l'adresse IP spécifiée sera exclu.

< port de destination > est un port de l'appareil protégé (exclusion pour le trafic entrant) ou un port de l'appareil distant (exclusion pour le trafic sortant). Le trafic vers ce port est exclu de l'interception.

Commande kesl-control --list-bypass-endpoints

La commande vous permet de consulter la liste des exclusions configurées à partir de l'interception du trafic.

Syntaxe de la commande

```
kesl-control [-N] --list-bypass-endpoints
```

Commande kesl-control --remove-bypass-endpoints

La commande vous permet de supprimer une exclusion à l'interception du trafic.

Syntaxe de la commande

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <adresse IP distante> --dst-port <port de destination>
```

Arguments et clés

`<in|out>` est la direction du trafic dans la connexion exclue, sortant ou entrant.

`<adresse IP distante>` est l'adresse IPv4 ou IPv6 de l'appareil distant dont le trafic est exclu de l'interception (selon le sens du trafic).

`<port de destination>` est un port de l'appareil protégé (exclusion pour le trafic entrant) ou un port de l'appareil distant (exclusion pour le trafic sortant).

Commandes de statistiques

Le préfixe -S indique que la commande appartient au groupe de commandes de statistiques.

Commande kesl-control --app-info

La commande permet d'afficher des informations sur l'application.

Syntaxe de la commande

```
kesl-control [-S] --app-info [--json]
```

Arguments et clés

`--json` : afficher les paramètres au format JSON.

Commande kesl-control --supported-tech-info

La commande permet d'afficher une liste des fonctions de l'application, des informations sur leur état (utilisé ou non utilisé) et les technologies Linux avec lesquelles ces fonctions de l'application sont implémentées.

Syntaxe de la commande

```
kesl-control [-S] --supported-tech-info [--json]
```

Arguments et clés

`--json` : afficher les fonctions au format JSON.

Commande kesl-control --get-statistic

La commande vous permet d'afficher des statistiques sur le fonctionnement de l'application et une liste des points de montage détectés sur l'appareil.

Syntaxe de la commande

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Arguments et clés

`[--files]` : statistiques sur les fichiers que le module Protection contre les fichiers malicieux analyse le plus souvent et le nombre de fois où le module accède à ces fichiers ;

`[--processes]` : statistiques sur les processus dont Kaspersky Endpoint Security détecte le plus fréquemment les lancements, et le nombre de ces lancements ;

> L'exclusion de processus de l'analyse par le module Détection comportementale ne les supprime pas des statistiques, mais améliore les performances de Kaspersky Endpoint Security.

`[--mountpoints]` : liste des points de montage. Dans le résultat, les chemins d'accès aux points de montage sont triés comme suit :

- points de montage statiques, système, de service et autres
- paquets snap montés et points de montage dans leurs espaces de noms
- Points de montage créés par le système de gestion des conteneurs Docker

Vous pouvez spécifier une ou plusieurs clés dans n'importe quelle combinaison, ou vous pouvez ne spécifier aucune clé du tout. Si vous ne spécifiez pas de clés, l'application affichera trois listes : des statistiques sur les fichiers les plus fréquemment analysés, des statistiques sur les processus les plus fréquemment lancés et une liste des points de montage détectés sur l'appareil.

Commande kesl-control --omsinfo

La commande vous permet de créer un fichier JSON pour l'intégration avec Microsoft Operations Management Suite.

Syntaxe de la commande

```
kesl-control [-S] --omsinfo --file <chemin d'accès au fichier>
```

Commandes d'affichage des événements

Commande kesl-control -W

La commande permet l'affichage des événements en cours de l'application. La commande reprend le nom de l'événement et les informations supplémentaires sur l'événement. Vous pouvez utiliser la commande pour afficher tous les événements de l'application en cours ou uniquement les événements associés à une tâche en cours d'exécution.

Syntaxe de la commande

```
kesl-control -W [--query "<conditions de filtrage>"]
```

Arguments et clés

`<conditions de filtrage>` spécifie une ou plusieurs expressions logiques au format `<champ> <opération de comparaison> '<valeur>'` combinées à l'aide de l'opérateur logique `and` pour afficher certains événements actuels.

Commandes de gestion des événements de l'application

Le préfixe -E indique que la commande fait partie des commandes de gestion des événements de l'application (Affichage des événements sur la ligne de commande, Affichage des événements dans Kaspersky Security Center).

Commande kesl-control -E

La commande vous permet d'afficher des informations sur tous les événements du journal des événements de l'application. Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés.

Syntaxe de la commande

```
kesl-control -E
```

Commande kesl-control -E --query

La commande vous permet d'afficher des informations sur les événements du journal des événements de l'application. Vous pouvez utiliser l'utilitaire `less` pour parcourir la liste des événements affichés. Vous pouvez utiliser un filtre pour afficher des événements spécifiques et également générer une liste d'événements dans un fichier spécifié.

Syntaxe de la commande

```
kesl-control -E --query "<conditions de filtrage>" [--db <fichier de base de données>]
[-n <nombre>] [--file <chemin d'accès au fichier>] [--json] [--reverse]
```

Arguments et clés

`<fichier de base de données>` est le chemin d'accès complet au fichier de base de données du journal des événements à partir duquel afficher les événements. Par défaut, l'application enregistre les informations relatives aux événements dans la base de données /var/opt/kaspersky/kesl/private/storage/events.db. L'emplacement de la base de données est déterminé par le paramètre général de l'application `EventsStoragePath`.

`<conditions de filtrage>` spécifient une ou plusieurs expressions logiques au format `<champ> <opération de comparaison> '<valeur>'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête.

`<nombre>` est le nombre d'événements les plus récents de la sélection (enregistrements comptés à partir de la fin de la sélection) à afficher.

`--file <chemin d'accès au fichier>` est le chemin complet du fichier dans lequel enregistrer les événements. Si vous spécifiez le nom du fichier sans avoir spécifié le chemin d'accès à celui-ci, le fichier sera créé dans le répertoire en cours. Si le fichier avec le nom spécifié existe déjà dans le répertoire indiqué, il sera réenregistré. Si le répertoire indiqué n'existe pas sur le disque, le fichier ne sera pas créé.

Si vous ne spécifiez pas la clé `--file` , la liste des événements sera affichée dans la console.

`--json` – afficher les événements au format JSON.

`--reverse` : afficher les événements dans l'ordre inverse (de l'événement le plus récent en haut au plus ancien en bas).

Commandes de gestion des clés de licence

Le préfixe -L indique que la commande appartient au groupe des commandes utilisées pour gérer les clés de licence.

> Les commandes d'ajout et de suppression de clés de licence ne peuvent être exécutées que si l'application est utilisée en mode standard ou en mode Endpoint Detection and Response Agent. Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, les commandes de gestion des clés de licence échouent avec une erreur. Vous activez l'application dans le cadre de la solution Kaspersky Security for Virtualization Light Agent ; vous n'avez pas besoin d'activer l'application séparément.

Commande kesl-control --add-active-key

La commande vous permet d'ajouter une clé de licence active à l'application à l'aide d'un fichier de clé ou d'un code d'activation.

Avec cette commande, vous pouvez ajouter à la fois des clés de licence de base de l'application et des clés de licence pour des fonctionnalités supplémentaires. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

Syntaxe de la commande

```
kesl-control [-L] --add-active-key <chemin d'accès au fichier clé>

kesl-control [-L] --add-active-key <code d'activation>
```

Arguments et clés

`<chemin d'accès au fichier clé>` est le chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.

`<code d'activation>` est le code d'activation.

Exemple :
Ajouter une clé en utilisant le fichier /home/test/00000001.key comme clé active :

```
kesl-control --add-active-key /home/test/00000001.key
```

Commande kesl-control --add-reserve-key

La commande vous permet d'ajouter une clé de licence de réserve à l'application à l'aide d'un fichier clé ou d'un code d'activation.

Avec cette commande, vous pouvez ajouter à la fois des clés de licence de base de l'application et des clés de licence pour des fonctionnalités supplémentaires. Vous n'avez pas besoin de spécifier le type de clé dans la commande.

Si la clé active n'a pas encore été ajoutée à l'application sur l'appareil, la commande échoue.

Syntaxe de la commande

```
kesl-control [-L] --add-reserve-key <chemin d'accès au fichier clé>

kesl-control [-L] --add-reserve-key <code d'activation>
```

Arguments et clés

`<chemin d'accès au fichier clé>` est le chemin d'accès au fichier clé. Si le fichier clé se trouve dans le répertoire actif, il suffit de saisir uniquement le nom du fichier.

`<code d'activation>` est le code d'activation.

Exemple :
Ajouter la clé de réserve à l'aide du fichier /home/test/00000002.key :

```
kesl-control --add-reserve-key /home/test/00000002.key
```

Commande kesl-control --remove-active-key

La commande permet de supprimer une clé de licence active.

Syntaxe de la commande

```
kesl-control [-L] --remove-active-key [--edr-optimum]

kesl-control [-L] --remove-active-key [--kuma]

kesl-control [-L] --remove-active-key [--mdr]

kesl-control [-L] --remove-active-key [--edr-kata]
```

Arguments et clés

`--edr-optimum` : supprimer la clé de licence active EDR Optimum.

`--kuma –` : supprimer la clé de licence KUMA active.

`--mdr –` : supprimer la clé de licence MDR active.

`--edr-kata` kata : supprimer la clé de licence active EDR Expert (on-premises).

Si vous ne spécifiez pas l'option `--edr-optimum`, `--kuma`, `--mdr` ou `--edr-kata` sur la ligne de commande, la commande supprime la clé active primaire de l'application.

Commande kesl-control --remove-reserve-key

La commande vous permet de supprimer la clé de licence de réserve.

Syntaxe de la commande

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]

kesl-control [-L] --remove-reserve-key [--kuma]

kesl-control [-L] --remove-reserve-key [--mdr]

kesl-control [-L] --remove-reserve-key [--edr-kata]
```

Arguments et clés

`--edr-optimum` : supprimer la clé de licence de réserve EDR Optimum.

`--kuma` : supprimer la clé de licence de réserve KUMA.

`--mdr` : supprimer la clé de licence de réserve MDR.

`--edr-kata` kata : supprimer la clé de licence de réserve active EDR Expert (on-premises).

Si vous ne spécifiez pas l'option `--edr-optimum`, `--kuma`, `--mdr` ou `--edr-kata` sur la ligne de commande, la commande supprime la clé de réserve primaire de l'application.

Commande kesl-control -L --query

La commande `-L --query` permet d'afficher des informations sur la licence sous laquelle l'application est activée et sur les clés de licence utilisées.

Syntaxe de la commande

```
kesl-control -L --query [--json]
```

Arguments et clés

`--json` : afficher les données au format JSON.

Commande kesl-control --load-mdr-blob

La commande `--load-mdr-blob` vous permet de télécharger un fichier BLOB sur l'appareil, qui peut être utilisé pour l'intégration avec Kaspersky Managed Detection and Response. Le fichier BLOB se trouve dans l'archive ZIP du fichier de configuration MDR.

Syntaxe de la commande

```
kesl-control [-L] --load-mdr-blob <chemin d'accès au fichier MDR BLOB>
```

Commande kesl-control --remove-mdr-blob

La commande `--remove-mdr-blob` vous permet de supprimer un fichier BLOB de l'appareil qui peut être utilisé pour l'intégration avec Kaspersky Managed Detection and Response.

Syntaxe de la commande

```
kesl-control [-L] --remove-mdr-blob
```

Commandes de gestion du pare-feu

Le préfixe -F indique que la commande fait partie des commandes de gestion du Firewall.

Commande kesl-control --add-rule

La commande vous permet d'ajouter une nouvelle règle de paquet réseau.

Syntaxe de la commande

```
kesl-control [-F] --add-rule [--name <nom de la règle>] [--action <action>] [--protocol
<protocole>] [--direction <sens>] [--remote <adresse distante>[:<plage de ports>]] [--
local <adresse locale>[:<plage de ports>]] [--at <indice>]
```

Arguments et clés

`--name <nom de la règle>` est le nom de la règle de paquet réseau.

`--action <action>` est l'action à réaliser sur les connexions définies dans la règle de paquet réseau.

`--protocol <protocole>` est le type de protocole de communication pour lequel vous souhaitez surveiller l'activité réseau.

`--direction <sens>` est le sens de l'activité réseau surveillée.

`--remote <adresse distante>[:<plage de ports>]` est l'adresse réseau de l'appareil distant.

`--local <adresse locale>[:<plage de ports>]` est l'adresse réseau de l'appareil Kaspersky Endpoint Security.

`--at <indice>` est le numéro de la règle dans la liste des règles de paquets réseau. Si le commutateur `--at` n'est pas spécifié ou si sa valeur est supérieure au nombre de règles dans la liste, la nouvelle règle est ajoutée à la fin de la liste.

Les paramètres pour lesquels vous ne spécifiez pas de valeurs dans la commande sont définis sur les valeurs par défaut.

Commande kesl-control --del-rule

La commande permet de supprimer une règle de paquet réseau avec le nom spécifié ou avec l'index spécifié dans la liste des règles.

Syntaxe de la commande

```
kesl-control [-F] --del-rule --name <nom de la règle>

kesl-control [-F] --del-rule --index <indice>
```

Arguments et clés

`--name <nom de la règle>` est le nom de la règle de paquet réseau.

`--index <indice>` est le numéro de la règle dans la liste des règles de paquets réseau.

Commande kesl-control --move-rule

La commande vous permet de modifier la priorité d'exécution d'une règle de paquet réseau.

Syntaxe de la commande

```
kesl-control [-F] --move-rule --name <nom de la règle> --at <indice>
```

```
kesl-control [-F] --move-rule --index <indice> --at <indice>
```

Arguments et clés

`--name <nom de la règle>` est le nom de la règle de paquet réseau.

`--index <indice>` est le numéro actuel de la règle dans la liste des règles de paquets réseau.

`--at <indice>` est le nouveau numéro de la règle dans la liste des règles de paquets réseau.

Commande kesl-control --add-zone

La commande permet d'ajouter une adresse à une zone réseau.

Syntaxe de la commande

```
kesl-control [-F] --add-zone --zone <zone> --address <adresse>
```

Arguments et clés

`--zone <zone>` est le nom prédéfini de la zone réseau.

`--address <adresse>` est l'adresse réseau ou le sous-réseau.

Commande kesl-control --del-zone

La commande permet de supprimer une adresse de la zone réseau.

Syntaxe de la commande

```
kesl-control [-F] --del-zone --zone <zone> --address <adresse>
```

```
kesl-control [-F] --del-zone --zone <zone> --index <indice de l'adresse>
```

Arguments et clés

`--zone <zone>` est le nom prédéfini de la zone réseau.

`--address <adresse>` est l'adresse réseau ou le sous-réseau.

`--index <indice de l'adresse>` est le numéro de l'adresse dans la zone réseau.

Commande kesl-control -F --query

La commande vous permet d'afficher les règles de pare-feu créées à l'aide de l'application Kaspersky Endpoint Security.

Syntaxe de la commande

```
kesl-control -F --query
```

Commandes de contrôle pour les appareils bloqués

Le préfixe -H indique que la commande appartient au groupe de commandes d'administration des appareils bloqués par la Protection contre le chiffrement et la Protection contre les menaces réseau.

Commande kesl-control --get-blocked-hosts

La commande permet d'afficher une liste des appareils bloqués sur la console.

Syntaxe de la commande

```
kesl-control [-H] --get-blocked-hosts
```

Commande kesl-control --allow-hosts

La commande vous permet de déverrouiller les appareils verrouillés.

Syntaxe de la commande

```
kesl-control [-H] --allow-hosts <adresse>
```

Arguments et clés

`<adresse>` est une adresse IP d'un appareil ou d'un sous-réseau (IPv4/IPv6, y compris les adresses au format abrégé). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

Commandes de gestion du Contrôle des appareils

Le préfixe D indique que la commande appartient au groupe de commandes permettant de gérer le Contrôle des appareils.

Commande kesl-control --get-device-list

Cette commande permet d'afficher dans la console la liste des appareils installés ou connectés à un appareil client, et d'exporter cette liste dans un fichier au format JSON.

Syntaxe de la commande

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <fichier>]
```

Arguments et clés

`--all` : afficher la liste de tous les appareils connectés.

`--json` : afficher la liste des appareils connectés au format JSON.

`--export <fichier>` exporte la liste des appareils connectés vers un fichier, au format d'une liste d'appareils de confiance. Vous devez spécifier le chemin d'accès complet au fichier au format JSON.

La commande kesl-control --trusted-devices

Cette commande permet de consulter la liste des appareils de confiance, d'y ajouter et d'en supprimer des appareils, et d'importer une liste d'appareils de confiance à partir d'un fichier.

Syntaxe de la commande

```
kesl-control [-D] --trusted-devices [--list] [--add <identifiant>] [--delete
<identifiant>] [--merge|--add|--replace --file <fichier>]
```

Arguments et clés

`--list` : afficher une liste des appareils de confiance.

`--add <ID>` ajoute un appareil à la liste des appareils de confiance à l'aide de l'identifiant de l'appareil ou d'un masque d'identifiant d'appareil.

`--delete <ID>` supprime un appareil de la liste des appareils de confiance à l'aide de l'identifiant de l'appareil ou d'un masque d'identifiant d'appareil.

`--merge` : fusionner les listes des appareils de confiance lors de l'importation. Si la liste actuelle et la liste importée contiennent des enregistrements pour un appareil ayant le même identifiant, les paramètres de l'enregistrement existant sont modifiés. Des enregistrements sont ajoutés pour les appareils qui ne figurent pas dans la liste actuelle.

`--add` : compléter la liste actuelle des appareils de confiance lors de l'importation. Seules les enregistrements pour les appareils qui ne figuraient pas auparavant dans la liste sont ajoutés.

`--replace` : remplacer la liste actuelle des appareils de confiance. La liste existante des appareils de confiance est remplacée par la liste importée.

`--file <fichier>` importe une liste d'appareils de confiance à partir du fichier spécifié. Vous devez spécifier le chemin d'accès complet au fichier au format JSON.

Commande kesl-control --request-temporary-device-access

Cette commande vous permet de créer un fichier de requête d'accès pour demander un accès temporaire à un appareil verrouillé.

Syntaxe de la commande

```
kesl-control [-D] --request-temporary-device-access --device-id <identifiant de l'appareil> --access-duration <durée d'accès> --path <chemin d'accès au fichier de demande d'accès>
```

Arguments et clés

`--device-id <identifiant de l'appareil>` spécifie l'identifiant de l'appareil bloqué auquel vous souhaitez accéder.

`--access-duration <durée d'accès>` spécifie la période pendant laquelle vous souhaitez pouvoir accéder à l'appareil (en heures). Valeurs possibles : 1 à 100.

`--path <chemin d'accès au fichier de demande d'accès>` spécifie le chemin d'accès au répertoire dans lequel vous souhaitez enregistrer le fichier de demande d'accès avec l'extension .akey.

Commande kesl-control --upload-temporary-device-access-key

Cette commande permet de charger une clé d'accès pour obtenir un accès temporaire à un appareil verrouillé.

Syntaxe de la commande

```
kesl-control [-D] --upload-temporary-device-access-key --path <chemin d'accès au fichier contenant la clé d'accès>
```

Arguments et clés

`--path <chemin d'accès au fichier contenant la clé d'accès>` est le chemin d'accès au fichier contenant la clé d'accès à l'appareil (fichier avec l'extension .acode).

Commandes de gestion du Contrôle des applications

Le préfixe -A indique que la commande appartient au groupe de commandes de gestion du Contrôle des applications.

Commande kesl-control --get-app-list

La commande permet d'afficher une liste des applications détectées sur l'appareil client lors de la tâche Inventaire.

Syntaxe de la commande

```
kesl-control [-A] --get-app-list [--json]
```

Arguments et clés

`--json` : afficher les données au format JSON.

Commande kesl-control --get-categories

La commande permet d'afficher une liste des catégories créées de contrôle des applications.

Syntaxe de la commande

```
kesl-control [-A] --get-categories [--names <nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>] [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`<nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>` désignent les noms des catégories pour lesquelles vous souhaitez consulter les informations. Si vous souhaitez consulter des informations sur plusieurs catégories, saisissez les noms des catégories séparés par un espace.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration JSON dans lequel les paramètres seront écrits.

`--json` : afficher les données au format JSON.

Commande kesl-control --set-categories

La commande vous permet de créer ou de modifier la liste des catégories créées du contrôle des applications.

Syntaxe de la commande

```
kesl-control [-A] --set-categories [--names <nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>] --file <chemin d'accès au fichier de configuration>
```

Arguments et clés

`<nom de la catégorie 1> <nom de la catégorie 2> ... <nom de la catégorie N>` désignent les noms des catégories dont vous souhaitez modifier les informations. Si vous souhaitez modifier les informations sur plusieurs catégories, spécifiez les noms de catégories séparés par un espace. Si vous ne fournissez pas de nom de catégorie, elle sera supprimée de la liste.

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès au fichier de configuration contenant les paramètres de la catégorie.

Commande kesl-control --get-settings 21

La commande permet d'afficher une liste des règles créées du contrôle des applications.

Syntaxe de la commande

```
kesl-control --get-settings 21 [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration dans lequel les paramètres seront écrits.

`--json` : afficher les données au format JSON.

Commande kesl-control --set-settings 21

La commande vous permet de modifier la liste des catégories créées des applications et des règles du Contrôle des applications.

Syntaxe de la commande

```
kesl-control --set-settings 21 [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés.

`--json` : importer les données d'un fichier au format JSON.

Commande kesl-control --set-to-default 21

La commande vous permet de supprimer une liste des catégories des applications et des règles du Contrôle des applications.

Syntaxe de la commande

```
kesl-control --set-settings 21 --set-to-default
```

Commandes de gestion du Contrôle Internet

Commande kesl-control --get-settings 26

La commande permet d'afficher une liste des paramètres configurés du Contrôle Internet.

Syntaxe de la commande

```
kesl-control --get-settings 26 [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration dans lequel les paramètres seront écrits.

`--json` : afficher les données au format JSON.

Commande kesl-control --set-settings 26

La commande permet de modifier la liste des paramètres configurés du Contrôle Internet.

Syntaxe de la commande

```
kesl-control --set-settings 26 [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` est le chemin d'accès complet au fichier de configuration à partir duquel les paramètres seront importés.

`--json` : importer les données d'un fichier au format JSON.

Commande kesl-control --set-to-default 26

La commande vous permet de supprimer les paramètres configurés et de restaurer les valeurs des paramètres du Contrôle Internet à règle par défaut.

Syntaxe de la commande

```
kesl-control --set-settings 26 --set-to-default
```

Commandes de gestion de la sauvegarde

Le préfixe -B indique que la commande appartient au groupe des commandes utilisées pour gérer le stockage de sauvegarde.

Commande kesl-control -B --mass-remove

La commande vous permet de supprimer tous ou uniquement les objets spécifiés de la sauvegarde.

Syntaxe de la commande

Supprimer tous les objets :

```
kesl-control -B --mass-remove
```

Supprimer les objets qui correspondent aux conditions du filtre :

```
kesl-control -B --mass-remove --query "< conditions de filtrage >"
```

Arguments et clés

`< conditions de filtrage >` spécifient une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête.

Commande kesl-control -B --query

La commande vous permet d'afficher des informations sur les objets de la sauvegarde.

Syntaxe de la commande

Afficher des informations sur tous les objets de la sauvegarde :

```
kesl-control -B --query [-n < nombre >] [--json] [--reverse]
```

Affichez des informations sur les objets de la sauvegarde qui correspondent aux conditions de filtre :

```
kesl-control -B --query ["< conditions de filtrage >"] [-n < nombre >] [--json] [--reverse]
```

Arguments et clés

`< conditions de filtrage >` spécifient une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtre, l'application affichera des informations sur tous les objets de la sauvegarde.

< nombre > est le nombre d'objets les plus récents à afficher. Si vous ne spécifiez pas la clé -n, les 30 derniers objets seront affichés. Pour afficher tous les objets, saisissez la valeur 0.

--json : afficher les données au format JSON.

--reverse : afficher les objets dans l'ordre inverse (de l'objet le plus récent en haut au plus ancien en bas).

Commande kesl-control -B --restore

La commande vous permet de restaurer un objet à partir de la sauvegarde.

Syntaxe de la commande

```
kesl-control -B --restore < identifiant de l'objet > [--file < chemin d'accès au fichier >]
```

Arguments et clés

< identifiant de l'objet > est l'identifiant de l'objet dans la sauvegarde.

--file < chemin d'accès au fichier > est le nouveau nom du fichier ainsi que le chemin d'accès au répertoire dans lequel l'enregistrer. Si vous ne spécifiez pas la clé --file, l'objet sera restauré avec son nom d'origine à son emplacement d'origine.

Commandes de gestion de la quarantaine

Le préfixe -Q indique que la commande appartient au groupe des commandes utilisées pour gérer la quarantaine.

Commande kesl-control -Q --mass-remove

La commande vous permet de supprimer tous les fichiers spécifiés ou uniquement ceux spécifiés de la quarantaine.

Syntaxe de la commande

Supprimer tous les fichiers :

```
kesl-control -Q --mass-remove
```

Supprimer les fichiers qui correspondent aux conditions du filtre :

```
kesl-control -Q --mass-remove --query "< conditions de filtrage >"
```

Arguments et clés

< conditions de filtrage > spécifient une ou plusieurs expressions logiques au format < champ > < opération de comparaison > '< valeur >' combinées à l'aide de l'opérateur logique and pour limiter les résultats de la requête.

Commande kesl-control --put

La commande est disponible uniquement lorsque Kaspersky Endpoint Security est intégré à Kaspersky Endpoint Detection and Response Optimum ou Kaspersky Managed Detection and Response.

La commande vous permet de mettre un fichier dans la quarantaine.

Syntaxe de la commande

```
kesl-control [-Q] --put <chemin d'accès au fichier> [--md5] [--sha256] [--save-original-file]
```

Arguments et clés

`<chemin d'accès au fichier>` est le chemin d'accès au fichier que vous souhaitez mettre en quarantaine.

`--md5` : somme de hachage MD5 du fichier que vous souhaitez mettre en quarantaine ;

`--sha256` : somme de hachage SHA256 du fichier que vous souhaitez mettre en quarantaine ;

`--save-original-file` : ne pas supprimer le fichier d'origine. Si vous ne spécifiez pas cette clé, le fichier d'origine sera supprimé.

Commande kesl-control -Q --query

La commande vous permet d'afficher des informations sur les fichiers mis en quarantaine.

Syntaxe de la commande

Afficher des informations sur tous les fichiers mis en quarantaine :

```
kesl-control -Q --query [-n <nombre>] [--json]
```

Afficher des informations sur les fichiers mis en quarantaine qui correspondent aux conditions du filtre :

```
kesl-control -Q --query ["<conditions de filtrage>"] [-n <nombre>]
```

Arguments et clés

`<conditions de filtrage>` spécifient une ou plusieurs expressions logiques au format `<champ> <opération de comparaison> '<valeur>'` combinées à l'aide de l'opérateur logique `and` pour limiter les résultats de la requête. Si vous ne spécifiez pas de conditions de filtrage, l'application affichera des informations sur tous les fichiers mis en quarantaine.

`<nombre>` est le nombre de fichiers les plus récemment mis en quarantaine que vous souhaitez afficher. Si vous ne spécifiez pas la clé `-n`, les 30 derniers fichiers seront affichés. Pour afficher tous les fichiers, saisissez la valeur 0.

`--json` : afficher les données au format JSON.

Commande kesl-control -Q --restore

La commande vous permet de restaurer un fichier de la quarantaine.

Syntaxe de la commande

```
kesl-control -Q --restore <identifiant du fichier> [--file <chemin d'accès au fichier>]
```

Arguments et clés

`<identifiant du fichier>` : l'identifiant du fichier mis en quarantaine.

`--file <chemin d'accès au fichier>` est le nouveau nom du fichier ainsi que le chemin d'accès au répertoire dans lequel l'enregistrer. Si vous ne spécifiez pas la clé `--file`, le fichier sera restauré avec son nom d'origine à son emplacement d'origine. Si le répertoire est supprimé ou si l'utilisateur n'a pas de droits d'accès à ce répertoire, l'application place le fichier dans le répertoire /var/opt/kaspersky/kesl/common/restored/. Vous pouvez déplacer manuellement le fichier de ce répertoire vers le répertoire souhaité.

Commandes de gestion des utilisateurs et des rôles

-U : préfixe qui indique que la commande appartient au groupe de commandes pour l'administration des utilisateurs et des rôles.

Commande kesl-control --get-user-list

La commande permet d'afficher une liste d'utilisateurs et de rôles.

Syntaxe de la commande

```
kesl-control [-U] --get-user-list
```

Commande kesl-control --grant-role

La commande vous permet d'attribuer un rôle à un utilisateur spécifique.

Syntaxe de la commande

```
kesl-control [-U] --grant-role <rôle> <utilisateur>
```

Commande kesl-control --revoke-role

La commande vous permet de révoquer un rôle d'un utilisateur spécifique.

Syntaxe de la commande

```
kesl-control [-U] --revoke-role <rôle> <utilisateur>
```

Commandes d'administration du module Expert EDR (on-premise)

-R – un préfixe indiquant que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) et Kaspersky Endpoint Detection and Response Optimum.

Commande kesl-control --add-kataedr-server-certificate

Cette commande vous permet d'ajouter ou de remplacer un certificat précédemment ajouté pour le serveur KATA, le serveur d'actions de réponse OSMP ou le serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --add-kataedr-server-certificate <fichier> [--server-type
<response|telemetry>]
```

Arguments et clés

`<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez ajouter ou remplacer un certificat en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous ajoutez ou remplacez un certificat de serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --remove-kataedr-server-certificate

La commande vous permet de supprimer le certificat pour le serveur KATA, le serveur d'actions de réponse OSMP ou le serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type
<response|telemetry>]
```

Arguments et clés

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez supprimer un certificat en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous supprimez le certificat du serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --query-kataedr-server-certificate

La commande vous permet d'afficher les informations sur le certificat du serveur KATA, du serveur d'actions OSMP ou du serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Arguments et clés

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez afficher les informations du certificat en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous souhaitez afficher des informations sur le certificat du serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control --add-kataedr-client-certificate

Cette commande permet d'ajouter ou de remplacer un certificat client précédemment ajouté, utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --add-kataedr-client-certificate <fichier> [--server-type
<response|telemetry>]
```

Arguments et clés

`<fichier>` est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

`--server-type <response|telemetry>` permet de sélectionner le type de serveur auquel vous souhaitez ajouter un certificat client en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous ajoutez ou remplacez un certificat client pour la connexion au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control [-R] --remove-kataedr-client-certificate

Cette commande permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions de réponse OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type
<response|telemetry>]
```

Arguments et clés

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez supprimer un certificat client en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous supprimez un certificat client utilisé pour la connexion au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commande kesl-control [-R] --query-kataedr-client-certificate

Cette commande affiche des informations sur le certificat client utilisé pour sécuriser la connexion au serveur KATA, au serveur d'actions de réponse OSMP ou au serveur de collecte de télémétrie OSMP (selon le mode d'intégration).

Syntaxe de la commande

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Arguments et clés

`--server-type <response|telemetry>` permet de sélectionner le type de serveur pour lequel vous souhaitez afficher les informations sur un certificat client en mode d'intégration EDR Expert (OSMP) :

- `response` : serveur d'actions de réponse OSMP ;
- `telemetry` : serveur de collecte de télémétrie OSMP.

Si vous souhaitez afficher des informations sur le certificat client utilisé pour se connecter au serveur KATA, ne spécifiez pas la clé `--server-type`.

Commandes d'administration des modules NDR (KATA)

-R – un préfixe indiquant que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) et Kaspersky Endpoint Detection and Response Optimum.

Commande kesl-control --add-katandr-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat du serveur NDR précédemment ajouté.

Syntaxe de la commande

```
kesl-control [-R] --add-katandr-server-certificate <fichier>
```

Arguments et clés

`<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

Commande kesl-control --remove-katandr-server-certificate

Cette commande supprime un certificat de serveur NDR.

Syntaxe de la commande

```
kesl-control [-R] --remove-katandr-server-certificate
```

Commande kesl-control --query-katandr-server-certificate

La commande vous permet d'afficher des informations sur le certificat du serveur NDR.

Syntaxe de la commande

```
kesl-control [-R] --query-katandr-server-certificate
```

Commande kesl-control --add-katandr-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour sécuriser la connexion au serveur NDR.

Syntaxe de la commande

```
kesl-control [-R] --add-katandr-client-certificate <fichier>
```

Arguments et clés

< `fichier` > est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

Commande kesl-control --remove-katandr-client-certificate

La commande vous permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur NDR.

Syntaxe de la commande

```
kesl-control [-R] --remove-katandr-client-certificate
```

Commande kesl-control --query-katandr-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

Syntaxe de la commande

```
kesl-control [-R] --query-katandr-client-certificate
```

Commandes de contrôle d'isolation réseau des appareils

-R – un préfixe indiquant que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (on-premise) et Kaspersky Endpoint Detection and Response Optimum. L'isolement réseau des appareils est appliquée comme mesure de réponse à la détection des menaces lorsqu'elle est intégrée aux solutions Detection and Response spécifiées.

Commande kesl-control --isolation-stat

La commande permet d'afficher l'état actuel de l'isolation réseau sur la console : activée ou désactivée.

Syntaxe de la commande

```
kesl-control [-R] --isolation-stat
```

Commande kesl-control --isolation-off

La commande vous permet de désactiver temporairement l'isolation réseau d'un appareil.

Syntaxe de la commande

```
kesl-control [-R] --isolation-off
```

Commandes de gestion des paramètres d'intégration avec KUMA

Le préfixe -M indique que la commande appartient au groupe de commandes permettant de gérer les paramètres de Kaspersky Unified Monitoring and Analysis Platform.

Commande kesl-control --add-kuma-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat du serveur KUMA précédemment ajouté.

Syntaxe de la commande

```
kesl-control [-M] --add-kuma-server-certificate <chemin d'accès au fichier>
```

Arguments et clés

`<chemin d'accès au fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

Commande kesl-control --remove-kuma-server-certificate

La commande permet de supprimer le certificat du serveur KUMA.

Syntaxe de la commande

```
kesl-control [-M] --remove-kuma-server-certificate
```

Commande kesl-control --query-kuma-server-certificate

La commande vous permet d'afficher des informations sur le certificat du serveur KUMA.

Syntaxe de la commande

```
kesl-control [-M] --query-kuma-server-certificate
```

Commande kesl-control --add-kuma-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour sécuriser la connexion au serveur KUMA.

Syntaxe de la commande

```
kesl-control [-M] --add-kuma-client-certificate <chemin d'accès au fichier>
```

Arguments et clés

`<chemin d'accès au fichier>` est le chemin d'accès au conteneur crypto (archive au format PFX) contenant le certificat client et la clé privée.

Commande kesl-control --remove-kuma-client-certificate

La commande vous permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur KATA.

Syntaxe de la commande

```
kesl-control [-M] --remove-kuma-client-certificate
```

Commande kesl-control --query-kuma-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

Syntaxe de la commande

```
kesl-control [-M] --query-kuma-client-certificate
```

Commandes de gestion des paramètres d'intégration avec Sandbox

Le préfixe -X indique que la commande appartient au groupe de commandes de gestion des paramètres d'intégration avec Sandbox.

Commande kesl-control --add-sandbox-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat précédemment ajouté du serveur qui assure l'interaction avec Sandbox.

Syntaxe de la commande

```
kesl-control [-X] --add-sandbox-server-certificate <fichier>
```

Arguments et clés

`<fichier>` est le chemin d'accès au fichier contenant le certificat du serveur.

kesl-control --remove-sandbox-server-certificate

La commande vous permet de supprimer le certificat du serveur qui assure la communication avec Sandbox.

Syntaxe de la commande

```
kesl-control [-X] --remove-sandbox-server-certificate
```

Commande kesl-control --query-sandbox-server-certificate

La commande affiche des informations sur le certificat du serveur qui permet l'interaction avec Sandbox.

Syntaxe de la commande

```
kesl-control [-X] --query-sandbox-server-certificate
```

Commande kesl-control --add-sandbox-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour protéger la connexion au serveur qui assure l'interaction avec Sandbox.

Syntaxe de la commande

```
kesl-control [-X] --add-sandbox-client-certificate <fichier>
```

Arguments et clés

`<fichier>` est le chemin d'accès au conteneur crypto (archive PFX) contenant le certificat client et la clé privée.

Commande kesl-control --remove-sandbox-client-certificate

La commande vous permet de supprimer un certificat client utilisé pour protéger la connexion au serveur qui assure l'interaction avec Sandbox.

Syntaxe de la commande

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Commande kesl-control --query-sandbox-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

Syntaxe de la commande

```
kesl-control [-X] --query-sandbox-client-certificate
```

Commande kesl-control --sandbox

La commande vous permet d'envoyer des fichiers à Sandbox pour analyse.

Syntaxe de la commande

```
kesl-control [-X] --sandbox <chemin 1> <chemin 2>
```

Arguments et clés

`<chemin>` est le chemin d'accès au fichier ou au répertoire que vous souhaitez analyser. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

Commandes de gestion de l'analyse IOC

Le préfixe -T indique que la commande appartient au groupe de commandes de gestion des paramètres et des tâches de l'application.

Commande kesl-control --scan-ioc

La commande exécute une recherche d'indicateurs de compromission sur l'appareil (IOC).

Syntaxe de la commande

```
kesl-control [-T] --scan-ioc --path <chemin d'accès au répertoire ou au fichier> [--process on|off] [--hint <expression régulière>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <liste des exclusions>] [--scope <liste des répertoires>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Arguments et clés

`--path <chemin d'accès au répertoire ou au fichier>` est le chemin d'accès au fichier IOC ou au répertoire contenant des fichiers IOC portant l'extension .IOC ou .XML, à utiliser pour effectuer l'analyse.

> Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces. Vous pouvez également spécifier les deux types de chemins (fichier et répertoire).

`--process` : activation de l'analyse des processus en cours d'exécution sur l'appareil.

Arguments possibles :

- `on` : activer l'analyse des processus en cours d'exécution sur l'appareil (valeur par défaut).
- `off` : désactiver l'analyse des processus en cours d'exécution sur l'appareil.

Si vous n'indiquez pas la clé `--process`, l'application effectue une analyse de processus uniquement si le fichier IOC utilisé contient les données de processus (`ProcessItem`).

`--hint <expression régulière>` est l'expression régulière qui correspond au chemin complet du fichier (`FileItem`) ou du fichier exécutable du processus (`ProcessItem`) à analyser.

Vous pouvez utiliser les éléments d'expressions régulières suivants :

- métacaractères : `. ^ $ |`
- classes de caractères : chiffre, alpha, inférieur, supérieur, cntrl
- quantificateurs : `* + ? {n} {n,} {n, m}`
- négation : `[^a-c]`
- caractères d'échappement : `\a \e \f`, `\n \r \t \v \b`

`--arpentry` : activation de l'analyse des enregistrements dans la tableau ARP (`ArpEntryItem`).

Arguments possibles :

- `on` : activer l'analyse des enregistrements dans le tableau ARP (valeur par défaut).
- `off` : désactiver l'analyse des enregistrements dans le tableau ARP.

Si vous n'indiquez pas la clé `--arpentry`, l'application analyse la tableau ARP uniquement si le fichier IOC utilisé contient les données de la table (`ArpEntryItem`).

`--ports` : activation de l'analyse des ports ouverts pour la connexion.

Arguments possibles :

- `on` : activer l'analyse des ports ouverts pour les connexions et vérifier les connexions actives sur l'appareil (valeur par défaut).
- `off` : désactiver l'analyse des ports ouverts pour les connexions et ne pas vérifier les connexions actives sur l'appareil.

Si vous n'indiquez pas la clé `--ports`, l'application effectue une analyse de ports uniquement si le fichier IOC utilisé contient les données de ports (`PortItem`).

`--system` : activation de l'analyse de l'environnement système.

Arguments possibles :

- `on` : activation de l'analyse de l'environnement système (valeur par défaut).
- `off` : désactivation de l'analyse de l'environnement système.

Si vous n'indiquez pas la clé `--system`, l'application effectue une analyse de l'environnement système uniquement si les informations sur l'environnement système (`SystemInfoItem`) sont spécifiées dans le fichier IOC utilisé.

`--files` : activation de l'analyse des fichiers.

Arguments possibles :

- `on` : activation de l'analyse des fichiers (valeur par défaut).
- `off` : désactivation de l'analyse des fichiers.

Si vous n'indiquez pas la clé `--files`, l'application effectue une analyse de fichiers uniquement si le fichier IOC utilisé contient les données de fichiers (`FileItem`).

`--drives` : zones à analyser.

Arguments possibles :

- `all` : analyser toutes les zones de fichiers disponibles.
- `system` : analyser tous les fichiers du système de fichiers racine.
- `critical` : analyser les fichiers dans les répertoires utilisateur et système (valeur par défaut).
- `custom` : analyser uniquement les fichiers dans les zones que vous spécifiez.

Si vous ne spécifiez pas la clé `--drives`, l'application analyse les fichiers dans les répertoires utilisateur et système.

`--excludes <liste des exclusions>` est la liste des chemins exclus des analyses.

Les exclusions spécifiées par cette clé sont globales et s'appliquent quel que soit le type de zone ou de liste de répertoires. Ces exclusions ont la priorité sur les autres options de ligne de commande, notamment `--hint` et `--scope`.

> Les exclusions sont spécifiées sous forme de chemins, mais ne peuvent pas contenir des éléments récursifs ni de caractères de masque (par exemple, `*`).

Si vous ne spécifiez pas la clé `--excludes`, l'analyse est effectuée sans exclusion.

Vous pouvez spécifier plusieurs exclusions, séparées par des espaces.

`--scope <liste des répertoires>` est la liste des répertoires supplémentaires à analyser.

Cette option est obligatoire si vous avez spécifié l'argument `--drives` pour l'option `custom`.

`--action` : action effectuée lorsque des indicateurs de compromission sont détectés.

Arguments possibles :

- `Skip` : l'application n'effectuera aucune action avec l'objet détecté, mais les informations le concernant seront enregistrées dans les résultats de la tâche (valeur par défaut).
- `QuarantineFile` : l'application mettra en quarantaine l'objet détecté.
- `IsolateHost` : l'application isole du réseau l'appareil sur lequel l'objet est détecté.
- `ScanCriticalAreas` : l'application analysera les **zones critiques**.
  - /lib/systemd
  - /lib/udev
  - /lib/dbus-1.0
  - /usr/local/lib/systemd/user
  - /usr/share/dbus-1
  - /usr/share/gdm/autostart
  - /usr/share/gnome/autostart
  - /var/spool/at
  - /var/spool/at/spool
  - /var/spool/anacron
  - /var/spool/cron
  - /boot
  - /bin
  - /sbin
  - /lib
  - /lib32
  - /lib64
  - /libx32
  - /usr/lib

- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

Vous pouvez spécifier plusieurs actions séparées par des espaces.

Si vous avez spécifié l'argument `Skip`, vous n'avez pas besoin d'ajouter d'autres arguments. L'argument `Skip` ne peut être utilisé que de manière indépendante.

Commandes applicatives en mode Light Agent pour la protection des environnements virtuels

Le préfixe -V indique que la commande appartient au groupe des commandes de Kaspersky Endpoint Security utilisées en mode Light Agent pour la protection des environnements virtuels (dans le cadre de Kaspersky Security for Virtualization Light Agent).

Les commandes ne peuvent être exécutées que si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

Commande kesl-control --ksvla-info

La commande permet d'afficher les informations sur l'utilisation des l'application en mode Light Agent pour protéger les environnements virtuels.

Syntaxe de la commande

```
kesl-control --ksvla-info
```

Commande kesl-control --viis-info

La commande permet d'afficher des informations sur la connexion du Light Agent (application Kaspersky Endpoint Security utilisée comme Light Agent dans le cadre de la solution Kaspersky Security for Virtualization Light Agent) au Serveur d'intégration.

Syntaxe de la commande

```
kesl-control --viis-info
```

Commande kesl-control --svm-info

La commande permet d'afficher des informations sur la connexion du Light Agent (application Kaspersky Endpoint Security utilisée comme Light Agent dans le cadre de la solution Kaspersky Security for Virtualization Light Agent) à la SVM.

Syntaxe de la commande

```
kesl-control --svm-info
```

Commandes pour gérer la collecte de métriques d'état du système

Commande kesl-control --export-metrics

La commande vous permet de configurer la collecte des métriques sur l'état du système d'exploitation.

Syntaxe de la commande

```
kesl-control [-J] --export-metrics [--period <intervalle entre les exportations en secondes>|--interactive]
```

Arguments et clés

`--period` : affichage périodique des résultats sur la ligne de commande ;

`<intervalle entre les exportations en secondes>` (en secondes) définit la période de sortie.

`--interactive` : affichage interactif (en appuyant sur la touche **Enter**).

Annexe 2. Fichiers de configuration et paramètres de l'application par défaut

Les fichiers de configuration suivants sont utilisés pour contrôler le fonctionnement de l'application Kaspersky Endpoint Security :

- Fichiers de configuration contenant les paramètres de configuration initiale de l'application :
  - fichier de configuration autoinstall.ini utilisé lors de l'installation de l'application à l'aide de Kaspersky Security Center ;
  - fichier de configuration utilisé lors de l'installation de l'application à l'aide de la ligne de commande.
- Fichiers de configuration prédéfinis créés automatiquement lors de la configuration initiale de l'application et contiennent les valeurs de paramètres spécifiées lors de la configuration initiale. Ces paramètres sont appliqués pendant l'exécution de l'application.
- Fichiers de configuration que vous pouvez créer à l'aide des commandes de gestion de l'application Kaspersky Endpoint Security. Ces fichiers de configuration peuvent contenir des paramètres de tâches et d'autres paramètres de l'application. Vous pouvez modifier ces fichiers et les importer dans l'application pour modifier les paramètres correspondants.

Règles d'édition des fichiers de configuration des tâches de l'application

Lors de la modification d'un fichier de configuration, veuillez respecter les règles suivantes :

- Attribuez une valeur à tous les paramètres obligatoires du fichier de configuration. Pour définir des paramètres distincts d'une tâche, vous pouvez opter pour la ligne de commande qui permet de réaliser l'opération sans fichier.
- Si le paramètre appartient à une section quelconque, ne le placez que dans cette section. Au sein d'une section, vous pouvez indiquer les paramètres dans n'importe quel ordre.
- Mettez les noms des sections entre crochets [ ].
- Spécifiez les valeurs des paramètres au format < `nom du paramètre` >=< `valeur du paramètre` > (les espaces entre le nom du paramètre et sa valeur ne sont pas traités).

  Exemple :

  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Les caractères "espace" et "tabulation" sont ignorés avant le premier guillemet et après le dernier guillemet d'une valeur de ligne, ainsi qu'au début et à la fin d'une valeur de ligne ne figurant pas entre guillemets.
- S'il s'avère nécessaire de définir plusieurs valeurs, répétez le paramètre autant de fois que le nombre de valeurs que vous voulez définir.

Exemple :

```
AreaMask.item_0000=*xml
AreaMask.item_0001=*doc
```

- Respectez la casse lors de la saisie des valeurs des paramètres des types suivants :
  - noms (masques) des objets analysés et des objets exclus ;
  - noms (masque) des menaces.

  Les autres valeurs de paramètres ne sont pas sensibles à la casse.
- Indiquez les valeurs des paramètres de type booléen comme suit : `Yes / No`.
- Les chaînes de valeur contenant un "espace" doivent être saisies entre guillemets (par exemple, les noms de fichiers ou les répertoires et les chemins d'accès à ceux-ci, les expressions contenant la date et l'heure au format AAAA-MM-DD HH:MM:SS).

  Les autres valeurs peuvent être saisies entre guillemets et sans guillemets.

  Exemple :

  ```
  AreaDesc=" Analyse des bases de messagerie "
  ```

  Un guillemet solitaire en début ou en fin de ligne est une erreur.

Fichiers de configuration préinstallés

Après la configuration initiale, les fichiers de configuration suivants sont créés dans l'application :

- /var/opt/kaspersky/kesl/common/objects-backup/

  Le fichier de configuration agreements.ini contient les paramètres relatifs au Contrat de licence utilisateur final, à la Politique de confidentialité et à la Déclaration de Kaspersky Security Network.
- /var/opt/kaspersky/kesl/common/kesl.ini

  Le fichier de configuration kesl.ini contient les paramètres figurant dans le tableau ci-dessous.

Si nécessaire, vous pouvez modifier les valeurs des paramètres dans ces fichiers.

Il est conseillé de modifier les valeurs par défaut dans ces fichiers uniquement en suivant les instructions des experts du Support technique.

Pour appliquer les modifications apportées au fichier de configuration, redémarrez l'application Kaspersky Endpoint Security.

Si le paramètre est absent dans le fichier ou si une valeur incorrecte du paramètre est spécifiée, l'application utilisera la valeur par défaut.

Paramètre	Description	Valeurs
La section **[Général]** contient les paramètres suivants :		
`Locale`	Paramètres régionaux utilisés pour localiser les événements transmis par l'application Kaspersky Endpoint Security à Kaspersky Security Center. La localisation spécifiée dans la variable d'environnement `LANG` est utilisée pour afficher l'interface graphique et la ligne de commande de l'application. Si l'application ne prend pas en charge la localisation spécifiée, la localisation anglaise est utilisée.	La locale au format défini par la norme RFC 3066. Si le paramètre `Locale` n'est pas spécifié, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à détecter la langue de localisation du système d'exploitation ou si cette localisation n'est pas prise en charge, l'anglais (en_US.UTF-8 au format standard RFC 3066) est utilisé pour localiser les événements.
`PackageType`	Format du progiciel installé. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. La valeur est renseignée automatiquement lors de la configuration initiale de l'application.	`rpm` : un RPM est installé. `deb` : un paquet DEB est installé.
`UseFanotify`	Utilisation de la technologie fanotify pour intercepter les opérations sur les fichiers. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application.	`true/yes` : l'application utilise la technologie fanotify pour intercepter les opérations sur les fichiers. `false/no` : la technologie fanotify n'est pas utilisée.
`KsvlaMode`	Utilisation de Kaspersky Endpoint Security est utilisé en mode Light Agent. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application.	`true/yes` : l'application est utilisée en mode Light Agent pour protéger les environnements virtuels. `false/no` : l'application est utilisée en mode standard.
`EndpointAgentMode`	Utilisation de Kaspersky Endpoint Security en mode Endpoint Detection and Response Agent.	`true/yes` : l'application est utilisée en mode Endpoint Detection and Response Agent. `false/no` : l'application est utilisée en mode standard.
`KcsMode`	Utilisation de l'application Kaspersky Endpoint Security dans le cadre de la solution Kaspersky Container Security en tant que module Protection contre les fichiers malicieux. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Ce paramètre est utilisé uniquement dans le fonctionnement de la solution Kaspersky Container Security.	`true/yes` : l'application est utilisée comme module Protection contre les fichiers malicieux dans la solution Kaspersky Container Security. `false/no` (valeur par défaut) : l'application est utilisée dans l'un des modes de l'application de Kaspersky Endpoint Security (en mode standard, en mode Light Agent pour la protection des environnements virtuels).
`StartupTraces`	Activation de la création de fichiers de traçage au lancement de l'application.	`true/yes` : crée des fichiers de traçage au lancement de l'application. `false/no` (valeur par défaut) : ne crée pas de fichiers de traçage au lancement de l'application.
`RevealSensitiveInfoInTraces`	Affichage des informations dans les fichiers de traçage qui peuvent contenir des données personnelles (par exemple, des mots de passe).	`true/yes` : afficher des informations pouvant contenir des données personnelles dans les fichiers de traçage de l'application. `false/no` (valeur par défaut) : ne pas afficher d'informations pouvant contenir des données personnelles dans les fichiers de traçage.
`AsyncTraces`	Activation du traçage asynchrone, dans lequel les informations sont écrites pour tracer les fichiers de manière asynchrone.	`true/yes` : activer le traçage asynchrone. `false/no` (par défaut) : ne pas activer le traçage asynchrone.
`CoreDumps`	Permettre la création d'un fichier de vidage lorsque l'application plante.	`true/yes` pour créer un fichier de vidage en cas de plantage de l'application. `false/no` (valeur par défaut) pour ne pas créer de fichier de vidage en cas de plantage de l'application.

Paramètre	Description	Valeurs
`CoreDumpsPath`	Chemin d'accès au répertoire où sont stockés les fichiers de vidage.	Valeur par défaut : /var/opt/kaspersky/kesl/common/dumps. L'accès au répertoire de stockage des fichiers de vidage défini par défaut requiert les autorisations root.
`MinFreeDiskSpace`	Quantité minimale de mémoire disque qui restera après l'écriture du fichier de vidage, en mégaoctets.	Valeur par défaut : 300.
`ScanMemoryLimit`	Restriction d'utilisation de la mémoire par l'application en mégaoctets.	Valeur par défaut : 8192. Il est recommandé de définir la valeur du paramètre `ScanMemoryLimit` à une valeur inférieure à celle du paramètre `MaxMemory` afin d'éviter que les tâches d'analyse et les redémarrages de l'application n'utilisent toute la mémoire disponible.
`MachineId`	ID unique de l'appareil de l'utilisateur.	La valeur du paramètre est renseignée automatiquement lors de l'installation de l'application.
`SocketPath`	Chemin d'accès au socket pour la connexion à distance, par exemple, de l'interface graphique et de l'utilitaire kesl-control.	Valeur par défaut : /var/run/bl4control.
`MaxInotifyWatches`	Limitation du nombre d'abonnements aux modifications de fichiers et de répertoires (user watches) indiqué dans /proc/sys/fs/inotify/max_user_watches. Si la valeur du paramètre du système d'exploitation est inférieure à la valeur du paramètre `MaxInotifyWatches`, l'application remplace la valeur du paramètre du système d'exploitation par la valeur du paramètre `MaxInotifyWatches`.	Valeur par défaut : 299987.
`MaxInotifyInstances`	Limitation du nombre d'abonnements aux modifications des fichiers et des répertoires par utilisateur, spécifiée dans le fichier /proc/sys/fs/inotify/max_user_instances. Si la valeur du paramètre du système d'exploitation est inférieure à la valeur du paramètre `MaxInotifyInstances`, l'application remplace la valeur du paramètre du système d'exploitation par la valeur du paramètre `MaxInotifyInstances`.	Valeur par défaut : 2047.
`ExecEnvMax`	Nombre de variables d'environnement que l'application capturera à partir de l'appel de la commande.	Valeur par défaut : 50.
`ExecArgMax`	Nombre d'arguments que l'application récupérera à partir de l'appel exec.	Valeur par défaut : 20.

Paramètre	Description	Valeurs
`AdditionalDNSLookup`	Utilisation du DNS public. Si l'accès aux serveurs via le DNS système échoue, l'application utilisera le DNS public. Ceci est nécessaire pour la mise à jour des bases de l'application et maintenir le niveau de sécurité de l'appareil. L'application utilisera les DNS publics suivants par ordre d'apparition : 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).	`true/yes` : utiliser le DNS public pour accéder aux serveurs de Kaspersky. `false/no` (valeur par défaut) : ne pas utiliser le DNS public pour accéder aux serveurs de Kaspersky. Les demandes de l'application peuvent contenir des adresses de domaine et l'adresse IP externe de l'utilisateur, car l'application établit une connexion TCP/UDP avec le serveur DNS. Ces données sont nécessaires, par exemple, pour l'analyse du certificat d'une ressource Internet lors de l'accès via HTTPS. Si l'application utilise un serveur DNS public, les règles de traitement des données sont régies par la Politique de confidentialité de ce service.
`PanicThreshold`	Nombre maximal d'arrêts anormaux de l'application lors de l'utilisation d'un module de noyau mis à jour. Lorsque la valeur spécifiée est atteinte, l'application passe en mode « sécurisé », dans lequel le module du noyau mis à jour n'est pas lancé.	Valeur par défaut : 3.
`SafeMode`	Activation du mode « sécurisé » de fonctionnement de l'application lors de l'utilisation d'un module de noyau mis à jour. Dans ce mode, l'application n'exécute pas le module de noyau mis à jour. Le mode « sécurisé » est activé automatiquement si l'application atteint le nombre maximal d'arrêts anormaux spécifié dans le paramètre `PanicThreshold`.	`true/yes` : le mode de fonctionnement « sécurisé » de l'application est activé. `false/no` (valeur par défaut) : le mode « sécurisé » de l'application est désactivé, l'application fonctionne en mode normal.
`GetContainerName`	Transmission des informations suivantes relatives aux conteneurs dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response : • indicateur précisant que l'événement s'est produit dans un conteneur ; • identifiant de l'espace de noms du conteneur ; • nom du conteneur. Le nom du conteneur n'est transmis que si vous disposez d'une licence pour utiliser la tâche Analyse du conteneur et si le conteneur a une durée de vie suffisante.	`true/yes` (valeur par défaut) : transmettre des informations étendues sur le conteneur dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response. `false/no` : ne pas transmettre les informations étendues du conteneur dans les données de télémétrie lors de l'intégration avec Kaspersky Managed Detection and Response.
La section **[Network]** contient les paramètres suivants :		
`WtpFwMark`	Étiquette dans les règles de l'utilitaire iptables pour rediriger le trafic vers une application en vue de son traitement par le module Protection contre les menaces Internet. Vous devrez peut-être modifier cette étiquette si un autre logiciel s'exécute sur le même appareil que l'application installée, que ce logiciel utilise le neuvième bit du masque de paquet TCP et qu'un conflit se produit.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x100. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x1000 ou 0x10000 (la marque est limitée à un entier de 32 bits).

Paramètre	Description	Valeurs
`NtpFwMark`	Étiquette dans les règles de l'utilitaire iptables pour rediriger le trafic vers une application en vue de son traitement par le module Protection contre les menaces réseau. Vous devrez peut-être modifier cette étiquette si un autre logiciel s'exécute sur le même appareil que l'application installée, que ce logiciel utilise le neuvième bit du masque de paquet TCP et qu'un conflit se produit.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x200. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x2000 ou 0x20000 (la marque est limitée à un entier de 32 bits).
`BypassFwMark`	Étiquette qui marque les paquets créés ou analysés par l'application afin qu'ils ne tombent pas à nouveau dans le programme pour analyse.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x400. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x4000 ou 0x40000 (la marque est limitée à un entier de 32 bits).
`BypassNFlogMark`	Une étiquette utilisée pour marquer les paquets créés ou examinés par une application afin qu'ils ne soient pas enregistrés par l'utilitaire iptable.	La valeur est indiquée sous forme de nombre décimal ou hexadécimal avec le préfixe 0x. Valeur par défaut : 0x800. Pour éviter l'analyse cyclique du trafic lorsque l'application s'exécute sur des nœuds utilisés dans le cadre de systèmes distribués, tels que Kubernetes, vous devez modifier les valeurs des marques de paquets réseau à l'aide des bits de poids fort. Par exemple : 0x8000 ou 0x80000 (la marque est limitée à un entier de 32 bits).
`ProxyRouteTable`	Numéro de table de routage.	Valeur par défaut : 101.
La section **[ScannerImpactStats]** contient les paramètres suivants :		
`CollectFileScanStatistics`	Permet à l'application de comptabiliser les statistiques de vérification des fichiers et des processus.	`true/yes` (valeur par défaut) : active le calcul des statistiques de l'analyse des fichiers et des processus. `false/no` : ne pas activer le calcul des statistiques de l'analyse des fichiers et des processus.
`StatCollectionPeriod`	Intervalle de temps pendant lequel l'application comptabilise les statistiques des fichiers vérifiés et des processus détectés avant de les enregistrer dans le fichier de traçage et dans les rapports.	Valeur par défaut : 10 minutes.
`StatCollectionCount`	Nombre de fichiers vérifiés et de processus détectés qui ont été comptés par l'application pendant l'intervalle de temps spécifié par le paramètre `StatCollectionPeriod` et qui seront inclus dans le rapport et dans les fichiers de traçage.	Valeur par défaut : 10.
`ReportStatAmount`	Nombre d'enregistrements qui seront affichés dans les rapports sur les fichiers et les processus les plus fréquemment analysés par jour.	Valeur par défaut : 20.
La section **[Virtualization]** contient les paramètres suivants :		

Paramètre	Description	Valeurs
`ServerMode`	Rôle d'une machine virtuelle protégée sur laquelle l'application Kaspersky Endpoint Security est utilisée en mode Light Agent pour protéger les environnements virtuels : serveur ou poste de travail. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application.	`true/yes` : la machine virtuelle est utilisée comme serveur. `false/no` : la machine virtuelle est utilisée comme poste de travail.
`VdiMode`	Activation du mode de protection de l'infrastructure VDI lors de l'utilisation de l'application en mode Light Agent pour protéger les environnements virtuels. Il n'est pas recommandé de modifier la valeur de ce paramètre manuellement. Le paramètre est configuré lors de la configuration initiale de l'application.	`true/yes` : le mode de protection de l'infrastructure VDI est activé. `false/no` : le mode de protection de l'infrastructure VDI est désactivé.
La section **[Watchdog]** contient les paramètres suivants :		
`TimeoutAfterHeadshot`	Temps d'attente maximal pour que le processus kesl se termine à partir du moment où le signal HEADSHOT est envoyé par le serveur Watchdog au processus kesl.	Valeur par défaut : 2 minutes.
`StartupTimeout`	Le temps d'attente maximum pour démarrer l'application (en minutes), après quoi le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 3 minutes.
`TimeoutAfterKill`	Temps d'attente maximal pour que le processus kesl géré termine son exécution à partir du moment où le serveur Watchdog envoie le signal SIGKILL au processus kesl. Si le processus kesl n'a pas terminé son exécution après ce délai, l'action spécifiée par le paramètre --failed-kill est exécutée.	Valeur par défaut : 2 jours.
`PingInterval`	Fréquence à laquelle l'application tente d'envoyer un message PONG au serveur Watchdog en réponse à un message PING reçu.	Valeur par défaut : 2000 millisecondes.
`MaxRestartCount`	Nombre maximum de tentatives consécutives infructueuses pour lancer l'application.	Valeur par défaut : 5.
`ActivityTimeout`	Intervalle de temps maximum pendant lequel l'application doit envoyer un message au serveur Watchdog. S'il n'y a pas de message de l'application pendant cet intervalle de temps, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 2 minutes.
`ConnectTimeout`	Le temps maximum d'attente pour qu'une application se connecte au serveur Watchdog à partir du moment où le processus kesl démarre. Si l'application n'a pas le temps de créer une connexion dans cet intervalle de temps, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 3 minutes.
`RegisterTimeout`	Intervalle de temps maximum à partir du moment où l'application se connecte au serveur Watchdog jusqu'à ce que le serveur reçoive le message REGISTER.	Valeur par défaut : 500 millisecondes.
`TimeoutAfterShutdown`	Temps d'attente maximal pour que le processus kesl se termine à partir du moment où le signal SHUTDOWN est envoyé par le serveur Watchdog au processus kesl.	Valeur par défaut : 2 minutes.

Paramètre	Description	Valeurs
MaxMemory	Limite d'utilisation de la mémoire résidente du processus kesl. Si la mémoire résidente du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	off : l'utilisation de la mémoire résidente n'est pas limitée. < valeur >% – valeur comprise entre 1 et 100 % de la mémoire RAM. < valeur >MB – valeur en mégaoctets. lowest/< valeur >%/< valeur >MB – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. highest/< valeur >%/< valeur >MB – la plus grande des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. auto : jusqu'à 50 % de la mémoire disponible, mais pas moins de 2 Go et pas plus de 16 Go. Valeur par défaut : auto.
MaxVirtualMemory	Limite d'utilisation de la mémoire virtuelle du processus kesl. Si la mémoire virtuelle du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	off (valeur par défaut) : l'utilisation de la mémoire virtuelle n'est pas limitée. < valeur >MB – valeur en mégaoctets.
MaxSwapMemory	Limite de taille du fichier swap du processus kesl. Si le fichier swap du processus géré dépasse cette limite, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	off (valeur par défaut) – La taille du fichier swap n'est pas limitée. < valeur >% – valeur comprise entre 0 et 100 % de la mémoire RAM. < valeur >MB – valeur en mégaoctets. lowest/< valeur >%/< valeur >MB – la plus petite des deux : la valeur en pourcentage et la valeur absolue en mégaoctets. highest/< valeur >%/< valeur >MB – la valeur la plus élevée entre la valeur en pourcentage et la valeur absolue en mégaoctets.
TrackProductCrashes	Activation d'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center lorsque l'application est instable.	true/yes : activer l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center. false/no (valeur par défaut) : désactiver l'envoi de l'état de l'appareil depuis l'application Kaspersky Endpoint Security vers Kaspersky Security Center.
ProductHealthLogFile	Chemin d'accès au fichier utilisé pour surveiller la stabilité de l'application.	Valeur par défaut : /var/opt/kaspersky/kesl/private/kesl_health.log.
WarnThreshold	L'intervalle de temps (en secondes) pendant lequel l'application doit compter le nombre d'arrêts anormaux avant d'afficher une notification instable.	Valeur par défaut : 3600 secondes.
WarnAfter_#_crash	Le nombre maximum d'arrêts anormaux de l'application, une fois atteint, une notification concernant le fonctionnement instable de l'application s'affiche.	Valeur par défaut : 10. Si la valeur est 0, la notification d'instabilité de l'application ne s'affiche pas.
WarnRemovingThreshold	Intervalle de temps (en secondes) après lequel l'état instable de l'application sera effacé.	Valeur par défaut : 86400 secondes.
SyscallHangProbePeriod	Fréquence à laquelle le serveur Watchdog appelle les fonctions système open et execve et augmente les compteurs pour les appels réussis de ces fonctions.	Valeur par défaut : 3 secondes.
SyscallHangCheckPeriod	Fréquence à laquelle le serveur Watchdog vérifie les compteurs pour les appels réussis des fonctions open et execve. Si passé ce délai la valeur des compteurs n'a pas changé, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeur par défaut : 32 secondes.

Paramètre	Description	Valeurs
`DumpSuspendPeriod`	Temps maximum d'attente pour la création du fichier de vidage de l'application avant que le serveur Watchdog ne suspende la vérification de l'activité de l'application. Si passé ce délai; la création du fichier de vidage n'est pas terminée, le serveur Watchdog lance la procédure de redémarrage du processus kesl.	Valeurs possibles : 1 – 30 minutes. Valeur par défaut : 2 minutes.
`TimeoutAfterCoredump`	Durée maximale pendant laquelle le serveur Watchdog suspendra l'envoi d'autres signaux au processus kesl après l'envoi d'un signal SIGTRAP, lequel est envoyé lors de la procédure d'arrêt anormal du processus.	Valeur par défaut : 2 minutes. Il est recommandé de spécifier une valeur du paramètre `TimeoutAfterCoredump` supérieure ou égale à la valeur du paramètre `DumpSuspendPeriod`. Vous pouvez spécifier la valeur du paramètre dans les unités suivantes : • pendant `<n> day|days|d` jours • pendant `<n> hour|hours|hr|h` heures • pendant `<n> minute|minutes|min|m` minutes • pendant `<n> second|seconds|sec|s` secondes • pendant `<n> [msec|ms]` millisecondes Si aucune unité n'est spécifiée, l'application utilisera par défaut les millisecondes.
La section **[Environment]** n'est pas présente dans le fichier de configuration par défaut.		
`ExperimentalContainerdSupport`	Activation de la prise en charge de l'environnement containerd lorsque le module Surveillance des conteneurs est en cours d'exécution (ContainerScan, Surveillance des conteneurs). Ce paramètre n'est pas présent dans le fichier de configuration par défaut. Si vous souhaitez utiliser l'environnement containerd lors de l'exécution du module Surveillance du conteneur, vous devez ajouter manuellement la section `[Environment]` au fichier de configuration et y ajouter le paramètre `ExperimentalContainerdSupport`.	`true/yes` : activer la prise en charge de l'environnement containerd lors du fonctionnement du module Surveillance du conteneur. `false/no` : ne pas activer la prise en charge de l'environnement containerd lors du fonctionnement du module Surveillance du conteneur.
`ReduceSWMemoryConsumption`	Limitation de la consommation de mémoire par le module Détection comportementale pour le traitement de la file d'attente des événements. La définition d'une limite de mémoire a un impact négatif sur la détection des menaces, notamment sur la qualité de la télémétrie transmise dans le cadre de l'intégration avec des solutions Detection and Response. Nous recommandons de définir une limite uniquement sur les systèmes fortement sollicités et après avoir contacté le Support technique afin d'obtenir des instructions spécifiques, s'il n'existe aucune autre option pour résoudre le problème de consommation élevée de mémoire.	1 – limite l'utilisation de la mémoire par le module Détection comportementale pour le traitement de la file d'attente des événements. 0 (par défaut) – ne limite pas l'utilisation de la mémoire. Le relancement de l'application est nécessaire après la modification de ce paramètre.

Paramètres des tâches de ligne de commande par défaut

Cette section contient les paramètres par défaut de toutes les tâches prédéfinies fournies pour gérer l'application Kaspersky Endpoint Security à l'aide de la ligne de commande.

Les tâches `Rollback` et `License` n'ont aucun paramètre.

Paramètres par défaut de la tâche File_Threat_Protection (ID:1)

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects
```

```
UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Scan_My_Computer (ID:2)

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]
```

```
AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Scan_File (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**
```

```
[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Critical_Areas_Scan (ID:4)

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes
```

```
DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Paramètres par défaut pour la tâche Update (ID:6)

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

Paramètres par défaut de la tâche System_Integrity_Monitoring (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Firewall_Management (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]
```

```
[NetworkZonesLocal]

[NetworkZonesPublic]
```

Paramètres par défaut de la tâche Anti_Cryptor (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche Web_Threat_Protection (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Paramètres par défaut de la tâche Device_Control (ID:15)

```
OperationMode=Block

AllowToRequestTemporaryAccess=No

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus
```

```
Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default
```

```
Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Paramètres par défaut de la tâche Removable_Drives_Scan (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Paramètres par défaut de la tâche Network_Threat_Protection (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes
```

```
BlockDurationMinutes=60

UseExcludeIPs=No
```

Paramètres par défaut pour les tâches Container_Scan (ID:18) et Custom_Container_Scan (ID:19)

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip
```

```
UseGlobalExclusions=Yes
```

Vous pouvez également utiliser les paramètres de ce fichier de configuration pour la tâche Analyse personnalisée du conteneur.

Paramètres par défaut de la tâche Behavior_Detection (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Paramètres par défaut de la tâche Application_Control (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Paramètres par défaut de la tâche Inventory_Scan (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche KATAEDR (ID:24)

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes
```

```
MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Paramètres par défaut pour la tâche Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Paramètres par défaut de la tâche Standalone_Sandbox (ID:29)

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes

ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

Paramètres par défaut de la tâche KATANDR (ID:31)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5
```

```
ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

Paramètres par défaut de la tâche KUMA (ID:33)

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

Paramètres par défaut de la tâche Protection contre les menaces par emails (ID : 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt

[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi
```

```
[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

Paramètres par défaut de la tâche Protection BadUSB (ID:37)

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No
```

Paramètres généraux de l'application

Les paramètres généraux de l'application déterminent le fonctionnement de l'application dans son ensemble et le fonctionnement des fonctions individuelles.

Paramètre	Description	Valeurs
`SambaConfigPath`	Répertoire dans lequel se trouve le fichier de configuration Samba. Le fichier de configuration Samba est nécessaire pour garantir l'application des valeurs `AllShared` ou `Shared:SMB` du paramètre `Path`. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Le répertoire standard du fichier de configuration SAMBA est indiqué par défaut. Valeur par défaut : /etc/samba/smb.conf.
`NfsExportPath`	Répertoire dans lequel se trouve le fichier de configuration NFS. Le fichier de configuration NFS est nécessaire pour garantir l'application des valeurs `AllShared` ou `Shared:NFS` du paramètre `Path`. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Le répertoire standard du fichier de configuration NFS est indiqué par défaut. Valeur par défaut : /etc/exports.
`TraceLevel`	Activer le traçage des applications et le niveau de détails des fichiers de traçage.	`Detailed` : crée un fichier de traçage détaillé. `MediumDetailed` : crée un fichier de traçage contenant des messages d'information et d'erreur. `NotDetailed` : crée un fichier de traçage contenant des notifications relatives aux erreurs. `None` (valeur par défaut) : ne crée pas de fichier de traçage.
`TraceFolder`	Répertoire dans lequel se trouvent les fichiers de traçage de l'application. Le relancement de l'application est nécessaire après la modification de ce paramètre.	Valeur par défaut : /var/log/kaspersky/kesl. L'accès au répertoire des fichiers de trace par défaut requiert les privilèges root. Si vous indiquez un autre répertoire, assurez-vous que seul l'utilisateur root dispose des autorisations de lecture et d'écriture sur ce répertoire (autorisations `700` ou `rwx--------`).
`TraceMaxFileCount`	Spécifie le nombre maximal de fichiers de traçage d'application. Le relancement de l'application est nécessaire après la modification de ce paramètre.	1 à 10000 Valeur par défaut : 10.
`TraceMaxFileSize`	Définit la taille maximale d'un fichier de trace de l'application (en mégaoctets). Le relancement de l'application est nécessaire après la modification de ce paramètre.	1 à 1000 Valeur par défaut : 500.

Paramètre	Description	Valeurs
`BlockFilesGreaterMaxFileNamePath`	Blocage de l'accès aux fichiers dont la longueur du chemin d'accès complet dépasse la valeur du paramètre définie (en octets). Si la longueur du chemin complet d'accès au fichier analysé excède la valeur de ce paramètre, les tâches d'analyse ignorent ce fichier lors de l'analyse. Ce paramètre s'applique uniquement aux systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify. Après avoir modifié la valeur de ce paramètre, relancez la tâche Protection contre les fichiers malicieux.	4096 à 33 554 432 Valeur par défaut : 16384.
`DetectOtherObjects`	Activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.	`Yes` : activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données. `No` (valeur par défaut) : désactiver la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.
`NamespaceMonitoring`	Activation de l'analyse des espaces de noms et des conteneurs (Analyse du conteneur, Surveillance des conteneurs). L'application ne vérifie pas les espaces de noms et les conteneurs à moins que les modules permettant de travailler avec les conteneurs et les espaces de noms ne soient installés sur le système d'exploitation.	`Yes` (valeur par défaut) : activer la surveillance des espaces de noms et des conteneurs. `No` : désactive la surveillance des espaces de noms et des conteneurs.
`FileBlockDuringScan`	Activation du mode d'interception pour les opérations sur les fichiers avec blocage de l'accès aux fichiers pendant l'analyse. Le mode d'interception des opérations sur les fichiers affecte le fonctionnement des modules Protection contre les fichiers malicieux et Contrôle des appareils.	`Yes` (valeur par défaut) : bloquer l'accès aux fichiers pendant l'analyse. `No` : ne pas bloquer l'accès aux fichiers lors de l'analyse. L'accès à n'importe quel fichier est autorisé, la vérification est effectuée en mode asynchrone. Ce mode d'interception des opérations sur les fichiers a moins d'impact sur les performances du système pendant le fonctionnement, mais il existe un risque qu'une menace dans un fichier ne soit pas désinfectée ou supprimée si, lors de l'analyse, ce fichier peut, par exemple, changer de nom avant que l'application ne prenne une décision sur l'état de ce dossier. Dans ce cas, les modules Protection contre les fichiers malicieux, Contrôle des appareils et Prévention de l'exécution des objets fonctionnent en mode de notification, quel que soit le mode de fonctionnement configuré.
`UseKSN`	Configuration de l'utilisation de Kaspersky Security Network dans l'application.	`Basic` : activer l'utilisation de Kaspersky Security Network en mode standard. `Extended` : activer l'utilisation de Kaspersky Security Network en mode avancé. `No` (valeur par défaut) : ne pas utiliser Kaspersky Security Network.

Paramètre	Description	Valeurs
`CloudMode`	Activation du mode cloud de l'application. Le mode Cloud est disponible si l'utilisation de KSN est activée. Si vous prévoyez d'utiliser le mode cloud, assurez-vous que KSN est disponible sur votre appareil. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`Yes` : activer le mode de fonctionnement dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données des applications malveillantes. `No` (valeur par défaut) – utilisez la version complète de la base de données des logiciels malveillants. Le mode Cloud est automatiquement désactivé si l'utilisation de KSN est désactivée.
`UseMDR`	Activation du module Managed Detection and Response pour l'intégration avec Kaspersky Managed Detection and Response. Si vous activez le module MDR et que Kaspersky Security Network est désactivé ou utilisé en mode standard, un message d'erreur s'affiche et le module MDR n'est pas activé. Pour activer le module MDR, vous devez activer l'utilisation de KSN en mode avancé.	`Yes` pour activer le module Managed Detection and Response. `No` (valeur par défaut) : désactiver le module Managed Detection and Response.
`UseEdrOptimum`	Activation du module EDR Optimum pour l'intégration avec Kaspersky Endpoint Detection and Response Optimum.	`Yes` : activer le module EDR Optimum. `No` (valeur par défaut) : désactiver le module EDR Optimum.
`UseProxy`	Activation de l'utilisation d'un serveur proxy par les modules de l'application Kaspersky Endpoint Security. Le serveur proxy peut être utilisé pour accéder aux serveurs d'activation de Kaspersky, aux sources de mises à jour des bases de données et des modules de l'application, à Kaspersky Security Network et lors de la vérification des certificats de sites à l'aide du module Protection contre les menaces Internet. Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'utilisation d'un serveur proxy pour la connexion à Kaspersky Security Network, à la SVM et au Serveur d'intégration n'est pas prise en charge.	`Yes` : active l'utilisation d'un serveur proxy. `No` (valeur par défaut) : désactiver l'utilisation d'un serveur proxy.

Paramètre	Description	Valeurs
`ProxyServer`	Adresse du serveur proxy à utiliser pour la connexion à Internet. Pour se connecter via un serveur proxy selon le protocole HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le serveur proxy HTTP utilise une connexion non chiffrée et le compte utilisateur peut être compromis.	Adresse du serveur proxy dans l'un des formats suivants : • `[<connection protocol>://]<IP address of the proxy server>:<port>`, si aucune authentification n'est requise pour se connecter au serveur proxy ; • `[<connection protocol>://][<user name>:[<password>]@]<IP address of the proxy server>:<port>`, si l'authentification est requise pour se connecter au serveur proxy. La connexion à un serveur proxy via le protocole HTTPS n'est pas prise en charge.
`ProxyBypass`	Liste des adresses pour lesquelles un serveur proxy n'est pas utilisé.	L'adresse est indiquée au format `< adresse >[:< numéro de port >`. Pour spécifier des adresses, vous pouvez utiliser des masques (symboles `*`) et des commentaires (après le symbole \).
`ProxyBypassEdr`	Utiliser un serveur proxy lors de la connexion aux Serveurs d'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises).	`Yes` : ne pas utiliser de serveur proxy lors de la connexion aux serveurs intégrant Kaspersky Endpoint Detection and Response Expert (on-premises). `No` (valeur par défaut) : utiliser un serveur proxy lors de la connexion aux serveurs permettant l'intégration de Kaspersky Endpoint Detection and Response Expert (on-premises).
`ProxyBypassNdr`	Utiliser un serveur proxy lors de la connexion aux Serveurs permettant l'intégration de Kaspersky Network Detection and Response (KATA).	`Yes` : ne pas utiliser de serveur proxy lors de la connexion aux serveurs assurant l'intégration avec Kaspersky Network Detection and Response (KATA). `No` (valeur par défaut) : utiliser un serveur proxy pour se connecter aux serveurs assurant l'intégration avec Kaspersky Network Detection and Response (KATA).
`ProxyBypassSandbox`	Utiliser d'un serveur proxy lors de la connexion aux serveurs qui permettent l'interaction avec Sandbox.	`Yes` : ne pas utiliser de serveur proxy lors de la connexion aux serveurs qui permettent l'interaction avec Sandbox. `No` (valeur par défaut) : utiliser un serveur proxy lors de la connexion aux serveurs qui permettent l'interaction avec Sandbox.
`MaxEventsNumber`	Quantité maximale d'événements qui sera enregistrée dans l'application. Quand la quantité maximale d'événements définie est atteinte, l'application supprime les événements les plus anciens.	Valeur par défaut : 500 000. Si défini sur 0, les nouveaux événements ne sont pas enregistrés et les anciens événements seront supprimés.
`LimitNumberOfScanFileTasks`	Nombre maximum de tâches d'analyse personnalisée qu'un utilisateur non privilégié peut exécuter simultanément sur un appareil. Ce paramètre ne limite pas la quantité de tâches que l'utilisateur doté des autorisations root peut démarrer.	0 à 100000 0 : un utilisateur non privilégié ne peut pas lancer des tâches d'analyse personnalisée. Valeur par défaut : 5.
`UseSyslog`	Activer la journalisation des événements de l'application dans syslog. L'accès à syslog requiert les privilèges root.	`Yes` : active l'enregistrement des événements dans syslog. `No` (valeur par défaut) : désactiver l'enregistrement des événements dans syslog.

Paramètre	Description	Valeurs
`EventsStoragePath`	Chemin vers le fichier principal de la base de données du journal des événements. L'accès à la base de données des événements par défaut requiert les privilèges root.	Valeur par défaut : /var/opt/kaspersky/kesl/private/storage/events.db.
`ExcludedMountPoint.item_#`	Point de montage que vous souhaitez exclure de la zone d'analyse. L'exclusion s'applique au fonctionnement des modules Protection contre les fichiers malicieux, Protection contre le chiffrement, Surveillance des conteneurs (Analyse du conteneur, Surveillance des conteneurs) ainsi qu'à la tâche Analyse des disques amovibles, et se configure également pour les tâches d'analyse ODS et ContainerScan. Vous pouvez indiquer plusieurs points de montage à exclure d'une analyse. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`. Le paramètre `ExcludedMountPoint.item_#` n'est pas défini par défaut.	`AllRemoteMounted` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'appareil via les protocoles SMB et NFS. `Mounted:NFS` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole NFS. `Mounted:SMB` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur l'ordinateur via le protocole SMB. `Mounted:<type de système de fichiers>` — Exclut de l'interception des opérations sur les fichiers tous les répertoires montés avec le type de système de fichiers indiqué. `/mnt` — exclut les objets du point de montage /mnt (y compris les sous-répertoires) de l'interception des opérations sur les fichiers. Ce répertoire est utilisé comme point de montage temporaire pour les disques amovibles. `<chemin qui contient le masque /mnt/user* ou /mnt/**/user_share>` — Exclut de l'interception des opérations sur les fichiers les objets des points de montage dont le nom contient le **masque** indiqué. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Pour exclure le point de montage `/dir`, vous devez indiquer exactement `/dir` (sans les astérisques). Le masque `/dir/*` exclut tous les points de montage d'un niveau inférieur à partir de `/dir`, mais pas le point de montage `/dir` lui-même. Le masque `/dir/**` exclut tous les points de montage à n'importe quel niveau d'imbrication sous `/dir`, mais pas le point de montage `/dir` lui-même. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.

Paramètre	Description	Valeurs
`MemScanExcludedProgramPath.item_#`	Exclusion de la mémoire d'un processus de l'analyse L'application n'analysera pas la mémoire du processus spécifié.	`< chemin d'accès complet au processus >` – Exclut de l'analyse le processus dans le répertoire local spécifié. Vous pouvez utiliser des **masques** pour spécifier le chemin. Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque de nom de fichier ou de répertoire. Vous pouvez saisir le caractère `*` au lieu d'un ensemble de caractères (y compris un ensemble vide) quelconque devant le caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/file` ou `/dir/*/*/file`. Vous pouvez saisir deux caractères `*` consécutifs pour remplacer n'importe quel ensemble de caractères (y compris un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/file*/` ou `/dir/file**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/file` est un masque incorrect. Vous pouvez utiliser le symbole `?` au lieu de n'importe quel caractère unique dans un nom de fichier ou de répertoire.
`UseOnDemandCPULimit`	Activation des limites d'utilisation du processeur pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan*.	`Yes` active la limitation de la consommation des ressources du processeur pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan*. `No` (valeur par défaut) : désactiver la limite de consommation des ressources CPU pour les tâches.
`OnDemandCPULimit`	La charge maximale sur tous les cœurs de processeur (en pourcentage) lors de l'exécution des tâches de type *ODS*, *ContainerScan* et *InventoryScan*.	Un entier compris entre 10 et 100. Valeur par défaut : 100.
`BackupDaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Après une durée spécifiée, l'application supprime les fichiers de sauvegarde les plus anciens. Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.	0 – 10000 0 : la durée de conservation des objets dans la sauvegarde n'est pas limitée. Valeur par défaut : 30.
`BackupSizeLimit`	Volume maximal de la sauvegarde (Mo). Quand la taille de la sauvegarde atteint la valeur maximale définie, l'application supprime les objets les plus anciens. Pour supprimer la limite sur la taille de la sauvegarde, spécifiez la valeur 0.	0 – 999999 0 : la taille de la sauvegarde est illimitée. Valeur par défaut : 0.
`QuarantineBackupFolder`	Chemin d'accès au répertoire où sont stockés les copies de sauvegarde des fichiers et les fichiers mis en quarantaine. Vous pouvez modifier le répertoire par défaut. Si le répertoire indiqué n'existe pas ou est inaccessible, l'application utilise le répertoire par défaut.	Valeur par défaut : /var/opt/kaspersky/kesl/common/objects-backup/ L'accès au répertoire par défaut requiert les privilèges root.
`QuarantineFillingNotification`	Pourcentage de plénitude de quarantaine auquel un événement de quarantaine complète est généré. Pour désactiver la génération des événements sur la quarantaine complète, spécifiez la valeur 0.	0 – 100 0 : la génération des événements concernant le remplissage de la quarantaine est désactivée. Valeur par défaut : 90.

Paramètre	Description	Valeurs
`QuarantineSizeLimit`	Volume maximal de la quarantaine (en mégaoctets). Lorsque la taille maximale de la quarantaine est atteinte, l'application supprime les fichiers les plus anciens. Pour supprimer la limite de taille de la quarantaine, saisissez la valeur 0.	0 – 999999 0 : la taille de la quarantaine est illimitée. Valeur par défaut : 200 si l'application est utilisée en mode standard, et 100 si l'application est utilisée en mode Light Agent.
`ShowPopUpNotifications`	Activation de l'affichage des notifications contextuelles dans l'interface utilisateur graphique.	`Yes` (par défaut) : afficher les notifications contextuelles dans l'interface utilisateur graphique. `No` : ne pas afficher les notifications contextuelles dans l'interface utilisateur graphique.
`PowerSaveMode`	Annulez l'exécution des tâches planifiées sur un appareil fonctionnant sur batterie.	`Yes` (valeur par défaut) : ignorer l'exécution des tâches planifiées lorsque l'appareil fonctionne sur batterie. `No` : exécuter les tâches selon un calendrier, quelle que soit la source d'alimentation à laquelle l'appareil est connecté (réseau ou batterie).
`InterceptorMode`	Le mécanisme d'interception des événements système utilisé par l'application Kaspersky Endpoint Security dans son travail. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`UseFanotify` (valeur par défaut) : utiliser la technologie fanotify pour intercepter les événements système. `UseUpdatableKernelModule` : utiliser un module de noyau mis à jour pour intercepter les événements système.
`InterceptorFallbackStrategy`	L'action qu'une application entreprend si un module de noyau mis à jour ne parvient pas à démarrer. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`FallbackToFanotify` (valeur par défaut) : passer à l'utilisation de la technologie fanotify pour intercepter les événements système. `FallbackToLimitedMode` : ne pas utiliser l'interception des événements système. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Paramètre	Description	Valeurs
`InterceptorApplyStrategy`	Si une application passe à l'utilisation d'un module du noyau mis à jour, un redémarrage de l'application est nécessaire pour démarrer le module. Ce paramètre vous permet de spécifier si l'application sera redémarrée automatiquement ou si un redémarrage manuel de l'application est requis. Le paramètre ne s'applique qu'aux appareils dont le système d'exploitation prend en charge la technologie fanotify.	`RestartServiceAutomatically` : redémarrer automatiquement l'application pour exécuter le module du noyau à actualiser. `RestartServiceManually` : exécuter le module de noyau mis à jour après le redémarrage manuel de l'application par l'utilisateur. Il est recommandé de redémarrer automatiquement l'application pour passer à l'utilisation du module de noyau mis à jour. L'exécution d'un module de noyau mis à jour après le redémarrage manuel de l'application peut provoquer des erreurs dans l'application.
`SystemEventsTransmission`	Activation de l'enregistrement des informations relatives aux événements des applications tierces dans syslog. L'accès à syslog requiert les privilèges root.	`Yes` : activer l'enregistrement des informations relatives aux événements des applications tierces dans syslog. `No` (valeur par défaut) : désactive l'enregistrement des informations relatives aux événements des applications tierces dans syslog.

Paramètres généraux d'analyse du conteneur

Les paramètres généraux de l'Analyse du conteneur sont utilisés lors de l'analyse des espaces de noms et des conteneurs en temps réel (Analyse du conteneur, Surveillance des conteneurs).

Paramètres généraux d'analyse du conteneur et des espaces de noms

Paramètre	Description	Valeurs
`OnAccessContainerScanAction`	Spécifie l'action à effectuer sur un conteneur lorsqu'un objet infecté est détecté. Cette option est disponible lors de l'utilisation de l'application sous une licence qui active cette fonctionnalité. Lors de l'analyse des objets à l'intérieur d'un conteneur, les paramètres de la tâche Protection contre les fichiers malicieux sont utilisés.	`StopContainerIfFailed` (valeur par défaut) : arrête le conteneur en cas d'échec de la désinfection ou de la suppression d'un objet infecté. Si cette valeur est sélectionnée, l'action effectuée sur le conteneur dépend également de la valeur spécifiée du paramètre `ActionOnThreat` de la tâche Protection contre les fichiers malicieux. Si le paramètre `ActionOnThreat` est défini sur `DisinfectDeleteIfNotPossible` et que l'application ne parvient pas à désinfecter ou à supprimer l'objet infecté lors de l'exécution de l'action, le conteneur sera arrêté. `StopContainer` : arrête le conteneur à la suite de la détection d'un objet infecté. `Skip` : n'effectue aucune action sur les conteneurs lorsqu'un objet infecté a été détecté.

Paramètre	Description	Valeurs
`UseDocker`	Utilisation du système d'administration par les conteneurs Docker. L'intégration avec le système d'administration par les conteneurs Docker version 28.5.2 et antérieures est prise en charge.	`Yes` (valeur par défaut) : utiliser le système d'administration par les conteneurs Docker. `No` : ne pas utiliser le système d'administration par les conteneurs Docker.
`DockerSocket`	Chemin ou URI (ID universel de ressource) du socket de Docker.	Valeur par défaut : /var/run/docker.sock.
`UseCrio`	Utilisation de l'environnement CRI-O.	`Yes` (valeur par défaut) : utilise l'environnement CRI-O. `No` : n'utilise pas l'environnement CRI-O.
`CrioConfigFilePath`	Chemin d'accès au fichier de configuration CRI-O.	Valeur par défaut : /etc/crio/crio.conf.
`UsePodman`	Utilisation de l'utilitaire Podman.	`Yes` (valeur par défaut) : utilise l'utilitaire Podman. `No` : n'utilise pas l'utilitaire Podman.
`PodmanBinaryPath`	Chemin d'accès au fichier exécutable de l'utilitaire Podman.	Valeur par défaut : /usr/bin/podman.
`PodmanRootFolder`	Chemin de la racine du stockage de conteneurs.	Valeur par défaut : /var/lib/containers/storage.
`UseRunc`	Utilisation de l'utilitaire runc.	`Yes` (valeur par défaut) : utilise l'utilitaire runc. `No` : n'utilise pas l'utilitaire runc.
`RuncBinaryPath`	Chemin d'accès au fichier exécutable de l'utilitaire runc.	Valeur par défaut : /usr/bin/runc.
`RuncRootFolder`	Chemin de la racine du Stockage des états de conteneurs.	Valeur par défaut : /run/runc.

Paramètres d'analyse du trafic réseau

Paramètres d'analyse du trafic réseau

Paramètre	Description	Valeurs
`EncryptedConnectionsScan`	Active ou désactive l'analyse des connexions chiffrées. Pour le protocole FTP, l'analyse des connexions chiffrées est désactivée par défaut.	`Yes` (valeur par défaut) : active l'analyse des connexions chiffrées. `No` : désactive l'analyse des connexions chiffrées. L'application ne déchiffre pas le trafic chiffré.
`EncryptedConnectionsScanErrorAction`	Spécifie l'action à effectuer lorsqu'une erreur d'analyse de connexion chiffrée se produit sur un site Internet.	`AddToAutoExclusions` (valeur par défaut) : ajoute le domaine qui a entraîné l'erreur à la liste des domaines avec des erreurs d'analyse. L'application ne surveillera pas le trafic réseau chiffré lors de la visite de ce domaine. `Disconnect` : bloque la connexion réseau.
`CertificateVerificationPolicy`	Spécifie la façon dont Kaspersky Endpoint Security vérifie les certificats. Si un certificat est auto-signé, l'application n'effectue pas la vérification supplémentaire.	`FullCheck` (valeur par défaut) : l'application utilise Internet pour vérifier et télécharger les chaînes manquantes qui sont nécessaires pour vérifier un certificat. `LocalCheck` : l'application n'utilise pas Internet pour vérifier un certificat.

Paramètre	Description	Valeurs
`UntrustedCertificateAction`	L'action entreprise par l'application lorsqu'elle rencontre un certificat non vérifié.	`Allow` (valeur par défaut) : autorise la connexion réseau établie lors de la visite d'un domaine avec un certificat douteux. `Block` : bloque la connexion réseau établie lors de la visite d'un domaine avec un certificat douteux.
`ManageExclusions`	Utilisation d'exclusions lors de l'analyse du trafic chiffré.	`Yes` : ne pas analyser les sites spécifiés dans la section `[Exclusions.item_#]` (cf. ci-dessous). `No` (valeur par défaut) : analyse tous les sites Internet.
`MonitorNetworkPorts`	Manière dont Kaspersky Endpoint Security surveille les ports réseau.	`Selected` (valeur par défaut) : surveille uniquement les ports réseau spécifiés dans la section [`[NetworkPorts.item_#]` (voir ci-dessous). `All` : surveille tous les ports réseau. La spécification de cette valeur peut augmenter considérablement la charge d'un système d'exploitation.
`NetInterceptorMode`	Mode d'interception du trafic par l'application Kaspersky Endpoint Security.	`UseEBPF` : utiliser la technologie eBPF pour l'interception du trafic. `UseIPTables` (valeur par défaut) : utiliser l'utilitaire iptables pour intercepter le trafic. Pour modifier le mode d'interception du trafic, vous devez redémarrer l'application. Les connexions réseau établies sont perdues lors du redémarrage.
La section **[Exclusions.item_#]** contient les domaines à exclure de l'analyse. L'application n'analyse pas les connexions établies lors de la visite de domaines spécifiés.		
`DomainName`	Spécifie le nom de domaine.	Vous pouvez utiliser des masques pour spécifier le domaine.
La section **[IncomingEndpointsExclusions.item_#]** contient des exclusions pour le trafic entrant.		
`RemoteIp`	Une adresse IP de l'appareil distant, dont le trafic est exclu de l'interception.	
`DestinationPort`	Un port de l'appareil protégé, dont le trafic provenant des appareils distants est exclu de l'interception.	
La section **[OutgoingEndpointsExclusions.item_#]** contient des exclusions pour le trafic sortant.		
`RemoteIp`	Une adresse IP de l'appareil distant vers laquelle le trafic est exclu de l'interception.	
`DestinationPort`	Un port de l'appareil protégé vers lequel le trafic provenant d'un appareil protégé est exclu de l'interception.	
La section **[NetworkPorts.item_#]** contient les ports réseau que l'application doit surveiller.		
`PortName`	Description du port réseau.	
`Port`	Numéros de port réseau à surveiller par l'application.	`1` : `65535`. La valeur par défaut n'est pas définie.

Paramètres de planification des tâches

Le tableau ci-dessous décrit les paramètres de planification des tâches que vous pouvez gérer pour toutes les tâches de l'application.

Paramètres de planification de la tâche

Paramètre	Description	Valeurs
`RuleType`	Planifier l'exécution de la tâche.	`Once` : exécuter la tâche une fois. `Monthly` : exécuter la tâche chaque mois, le jour et l'heure spécifiés. `Weekly` : exécuter la tâche chaque semaine, le jour et l'heure spécifiés. `Daily` : exécuter la tâche régulièrement, avec un intervalle spécifié en jours. `Hourly` : exécuter la tâche régulièrement, à un intervalle spécifié en heures, à partir de la date et de l'heure spécifiées. `Minutely` : exécuter la tâche régulièrement, à un intervalle spécifié en minutes, à partir de l'heure spécifiée. `Manual` : lance la tâche manuellement. `PS` : lance la tâche après le lancement de l'application. `BR` : lancement de la tâche après la mise à jour des bases de données de l'application.
`StartTime`	La date et l'heure du lancement de la tâche. Le paramètre `StartTime` est obligatoire si le paramètre `RuleType` a l'une des valeurs suivantes : Once, Monthly, Weekly, Daily, Hourly, Minutely.	`[< année >/< mois >/< jour du mois >] [ hh ]:[ mm ]:[ ss ]; [< jour du mois >| < jour de la semaine >]; [< périodicité de lancement >]`
`RandomInterval`	Intervalle de temps de 0 à la valeur spécifiée (en minutes), qui sera ajouté à l'heure de lancement de la tâche pour éviter le lancement simultané de tâches.	Valeur par défaut : 99 minutes.
`RunMissedStartRules`	Lancement d'une tâche ignorée après le lancement de l'application.	`Yes` (valeur par défaut) : démarrer la tâche ignorée après le lancement de l'application. `No` : ne pas désactiver le lancement d'une tâche ignorée après le lancement de l'application.
`UseWorkingTimeout`	Arrêt de la tâche lorsque la durée maximale d'exécution de la tâche spécifiée par le paramètre `WorkingTimeout` est atteinte. La tâche sera arrêtée même si elle n'est pas terminée. Le prochain lancement de la tâche sera effectué comme prévu.	`Yes` : arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte. `No` (valeur par défaut) : ne pas arrêter la tâche lorsque la durée maximale d'exécution de la tâche est atteinte.
`WorkingTimeout`	Le temps maximum d'exécution de la tâche (en minutes), après lequel l'application arrête l'exécution de la tâche, si la valeur du paramètre `UseWorkingTimeout=yes`.	Valeur par défaut : 120 minutes.

Annexe 3. Codes de retour de la ligne de commande

L'application Kaspersky Endpoint Security prévoit les codes de retour de la ligne de commande.

0 : réussite de l'exécution de la commande/de la tâche ;

1 : erreur générale dans la syntaxe de la commande ;

2 : erreur dans les paramètres de l'application transmis ;

64 : l'application Kaspersky Endpoint Security n'est pas lancée ;

66 – les bases de données de l'application ne sont pas chargées (ce code est utilisé uniquement par la commande `kesl-control --app-info`).

67 : échec de l'activation 2.0 suite à des problèmes de réseau ;

68 : impossible d'exécuter la commande car l'application est soumise à une stratégie ;

69 : l'application est dans l'infrastructure Amazon Paid Ami ;

70 : tentative de lancement d'une tâche déjà en cours d'exécution, de suppression d'une tâche en cours d'exécution, de modification des paramètres d'une tâche en cours d'exécution, d'arrêt d'une tâche arrêtée, de suspension d'une tâche suspendue ou de relance d'une tâche en cours d'exécution ;

71 : rejet des dispositions de la Déclaration de Kaspersky Security Network ;

72 : détection de menaces dans le cadre de l'exécution des tâches Analyse personnalisée et Analyse personnalisée du conteneur ;

73 – tentative de définition de paramètres de la tâche Contrôle des applications ayant un impact sur le fonctionnement de l'application sans les confirmer à l'aide de l'option `--accept`.

74 : la mise à jour requiert le redémarrage de l'application Kaspersky Endpoint Security ;

75 : il faut redémarrer l'appareil ;

76 : connexion interdite, car seuls les utilisateurs ayant des droits d'accès à la racine doivent avoir des droits d'écriture sur le chemin spécifié ;

77 : la clé de licence spécifiée est déjà utilisée sur l'appareil ;

78 : la commande/tâche ne peut pas être exécutée parce que l'application est utilisée en mode Light Agent ;

79 : la commande ne peut pas être exécutée parce que l'application est utilisée en mode standard ;

80 : l'opération de téléchargement de la mise à jour a échoué en raison de problèmes de réseau ;

128 : erreur inconnue ;

65 : toutes les autres erreurs.

Annexe 4. Configuration de la collaboration avec Kaspersky Antivirus for Linux Mail Server

Pour configurer la compatibilité entre l'application Kaspersky Endpoint Security et Kaspersky Anti-Virus for Linux Mail Server :

1. Enregistrez les paramètres de la tâche Protection contre les fichiers malicieux dans le fichier de configuration à l'aide de la commande suivante :

   ```
   kesl-control --get-settings 1 --file <chemin d'accès complet au fichier>
   ```

2. Ouvrez le fichier de configuration créé afin d'en modifier le contenu.

3. Ajoutez la section suivante dans le fichier créé :

   ```
   [ExcludedFromScanScope.item_<numéro d'élément>]
   Path=/var/opt/kaspersky/klms
   ```

4. Répéter la section indiquée ci-dessus pour tous les agents de messagerie intégrés à Kaspersky Anti-Virus for Linux Mail Server.

5. Pour exclure le répertoire temporaire des filtres et des services de Kaspersky Anti-Virus for Linux Mail Server de l'analyse, ajoutez la section suivante dans le fichier créé la section :

   ```
   [ExcludedFromScanScope.item_<numéro d'élément>]
   Path=/tmp/klmstmp
   ```

6. Enregistrez les modifications dans le fichier de configuration.

7. Importez les paramètres du fichier de configuration dans la tâche Protection contre les fichiers malicieux à l'aide de la commande suivante :

   ```
   kesl-control --set-settings 1 --file <chemin d'accès complet au fichier>
   ```

Annexe 5. Paramètres de l'application dans Web Console

Cette section décrit les paramètres de stratégie disponibles dans la console Web, sous l'onglet **Paramètres de l'application** .

Protection contre les menaces contre l'hôte

Protection contre les fichiers malicieux

pour Windows, macOS et Linux

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.

`Linux` Pour les appareils Linux, le module est influencé par le mode de blocage de l'accès aux fichiers pendant les analyses, que vous pouvez sélectionner dans les paramètres généraux de l'application. Par défaut, l'accès au fichier est bloqué pendant l'analyse.

Paramètres de l'Antivirus fichiers

Paramètres	SE	Description
Exclusions de l'analyse	`Windows` `macOS` `Linux`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**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 (dépend du système d'exploitation)**. `Windows` `Linux` Si cette option est sélectionnée, l'application essaie automatiquement de désinfecter le fichier infecté détecté. Si la désinfection échoue, l'application bloque ce fichier. **Bloquer ou demander une action (selon le système d'exploitation utilisé)**. `Windows` `Linux` Si cette option est sélectionnée, l'application bloque automatiquement le fichier infecté sans tenter de le désinfecter ou de le supprimer. `macOS` Kaspersky Endpoint Security affiche une fenêtre de notification qui contient les informations relatives au type d'objet malveillant à l'origine de l'infection du fichier et propose à l'utilisateur de sélectionner l'action à exécuter. Les actions disponibles varient en fonction de l'état de l'objet. Avant de désinfecter ou de supprimer un fichier infecté, l'application crée une copie de sauvegarde du fichier au cas où celui-ci devrait être restauré ultérieurement ou sa désinfection deviendrait possible.
Zone de protection	`Windows` `macOS` `Linux`	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. `Linux` Pour les appareils Linux, vous pouvez modifier ou supprimer les zones d'analyse à l'aide du module Protection contre les fichiers malicieux. Spécifiez au moins une zone de protection pour le fonctionnement du module.

Paramètres	SE	Description
File types	`macOS`	**Scan all files**. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension). **Scan applications and documents by content**. 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. **Scan applications and documents by 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.
Optimisation de l'analyse	`Windows` `macOS`	Sous **Optimisation de l'analyse**, vous pouvez configurer Kaspersky Endpoint Security de manière à améliorer les performances lors de l'analyse des fichiers. • `Windows` `macOS` **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. • `Windows` **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas de 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. • `macOS` **Ignorer l'analyse du volume du système en lecture seule**. Si la case est cochée, l'application n'analyse pas le volume système en lecture seule. La durée de l'analyse s'en trouve considérablement réduite. • `Windows` **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si cette case est cochée, l'application analyse le conteneur uniquement lors de son lancement. Si la case n'est pas cochée, l'application analyse le conteneur en permanence et en temps réel.
Analyse des fichiers composés	`Windows` `macOS` `Linux`	L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour détecter les virus et autres menaces dissimulés de cette manière, le fichier composé doit être décompressé, ce qui peut ralentir l'analyse. Vous pouvez limiter les types de fichiers composés à analyser pour accélérer l'analyse. • **Archives**. Analyse des 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 l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive). • **Paquets de distribution et archives autoextractibles**. Analyse des paquets d'installation des applications tierces et des archives autoextractibles. Les archives auto-extractibles sont des archives qui contiennent un décompresseur exécutable d'archives. Pour que les archives autoextractibles soient analysées, vous devez cocher la case **Analyser les archives**. • `Windows` `macOS` **Fichiers au format Office et objets OLE intégrés**. Analyse des fichiers Microsoft Office (par exemple, DOC, DOCX, XLS, PPT) et des objets OLE intégrés dans des fichiers (par exemple, tableaux Excel, macros, pièces jointes à des emails). • `Windows` `Linux` **Analyser les bases de messagerie**. Analyse des bases de données de messagerie de Microsoft Outlook, Outlook Express, The Bat! et d'autres clients de messagerie. • `Linux` **Analyser les fichiers au format de messagerie**. Analyse des fichiers de messages électroniques au format texte brut.
Autoriser la décompression en arrière-plan des archives dont la taille est supérieure à (Mo)	`Windows` `macOS`	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.
Ne pas analyser les archives de plus de (Mo)	`Windows` `macOS` `Linux`	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.
Ignorer un fichier si son analyse prend plus de (secondes)	`Linux`	Si la case est cochée, l'application arrête d'analyser les fichiers composés au terme de la durée définie. Si la valeur est définie sur `0`, la durée d'analyse est illimitée.

Paramètres	SE	Description
Analyse en arrière-plan	`Windows`	*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.
Analyse depuis le menu contextuel	`Windows`	Kaspersky Endpoint Security vous permet d'effectuer une analyse des fichiers individuels à la recherche de virus et autres programmes malveillants depuis le menu contextuel. 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.

Protection BadUSB

pour Windows et Linux

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 est saisi incorrectement, l'application en génère un nouveau. 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.

Le module Protection BadUSB n'est pas installé par défaut. Si vous avez besoin du module Protection BadUSB, vous pouvez l'ajouter dans les propriétés du fichier d'installation avant d'installer l'application ou modifier la sélection des modules de l'application après avoir installé l'application.

Autorisation de clavier

Paramètres du module Protection BadUSB

Paramètres	SE	Description
Nombre maximal de tentatives d'autorisation des appareils USB	`Windows` `Linux`	Bloque automatiquement un appareil USB si le code d'autorisation est saisi incorrectement un nombre de fois spécifié. 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 affichera la durée de verrouillage 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)	`Windows` `Linux`	La durée de blocage de l'appareil USB après le nombre indiqué de tentatives infructueuses de saisie du code d'autorisation. Les valeurs autorisées vont de 1 à 180 minutes.
Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB	`Windows` `Linux`	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	`Windows` `Linux`	Si le commutateur à bascule est activé, Kaspersky Endpoint Security n'affiche pas de code-barres dans la notification pour l'authentification par le lecteur de code-barres.

Analyse des disques amovibles

pour Windows, macOS et Linux

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.

Paramètres d'analyse des disques amovibles

Paramètres	SE	Description
Type d'analyse	`Windows` `Linux`	**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. **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.
Empêcher les utilisateurs d'arrêter l'analyse	`Windows`	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.
Bloquer l'accès au disque amovible pendant l'analyse	`Linux`	Si la case est cochée, Kaspersky Endpoint Security bloque l'accès aux fichiers du disque connecté pendant l'exécution de l'analyse.
Masquer la barre de progression de l'analyse	`Windows`	Si la case est cochée, Kaspersky Endpoint Security masque la barre de progression de l'analyse des disques amovibles. L'application exécute l'analyse en arrière-plan. Si la case est décochée, Kaspersky Endpoint Security affiche la progression de l'analyse des disques amovibles dans une nouvelle fenêtre et dans la section **Tâches**.
Ne pas analyser les disques amovibles dont la taille est supérieure à	`Windows`	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.

Détection comportementale

pour Windows, macOS et Linux

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.

Pour optimiser les performances du module Détection comportementale, nous vous recommandons d'activer le module Protection contre les menaces Internet.

Paramètres de la Détection comportementale

Paramètres	SE	Description
Applications de confiance	`Windows` `macOS` `Linux`	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. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.

Paramètres	SE	Description
Exclusions de l'analyse	`Windows` `macOS` `Linux`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**Supprimer un fichier ou un bloc (en fonction du système d'exploitation)**. `Windows` `macOS` Si cette option est sélectionnée, lors de la détection d'une activité malveillante, Kaspersky Endpoint Security supprime le fichier exécutable de l'application malveillante et crée une copie de sauvegarde du fichier dans Sauvegarde. `Linux` Si une activité malveillante est détectée, Kaspersky Endpoint Security bloque l'application qui effectue l'activité malveillante et enregistre les informations relatives à l'activité malveillante détectée. **Informer**. `Windows` `Linux` Si cette option est sélectionnée, 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. `macOS` En cas de détection d'une activité malveillante, Kaspersky Endpoint Security invite l'utilisateur à sélectionner l'action à effectuer en cas de détection d'une activité malveillante. Les actions disponibles varient en fonction de l'état de l'objet. **Interdire**. Si cette option est sélectionnée, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.

Protection contre le chiffrement

pour Windows, macOS et Linux

`Windows` Pour les appareils Windows, le module surveille uniquement les opérations concernant les fichiers qui se trouvent au niveau du système de fichiers NTFS et qui ne sont pas chiffrés par le système EFS.

`Linux` Pour les appareils Linux, le module analyse les fichiers dans les répertoires locaux avec accès réseau via SMB/NFS.

`macOS` Pour les appareils macOS, le module surveille les partages SMB.

Le module Protection contre le chiffrement à distance assure la protection contre le chiffrement à distance en analysant l'activité sur les partages réseau. Si l'activité correspond à un modèle de comportement dangereux caractéristique du chiffrement externe, Kaspersky Endpoint Security exécute l'action choisie.

`Linux` Avant d'activer le module sur les appareils Linux, assurez-vous de lire et de comprendre les informations relatives à la Protection contre le chiffrement.

Paramètres	SE	Description
Exclusions de l'analyse	`Windows` `Linux`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
Exclusions par nom ou par adresse IP	`Windows`	**Noms d'ordinateurs / adresses IP de confiance**. La liste des ordinateurs pour lesquels les tentatives de chiffrement des dossiers partagés ne sont pas traquées. **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. 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	`Windows` `macOS` `Linux`	**Informer**. Si cette option est sélectionnée, lors de la détection d'une tentative de modification de fichiers dans des dossiers partagés, Kaspersky Endpoint Security ajoute les informations relatives à cette tentative à la liste des menaces actives et ajoute une entrée au rapport. **Bloquer la connexion pendant (minutes)**. `Windows` 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. `macOS` `Linux` Lorsque Kaspersky Endpoint Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque le trafic réseau provenant de l'appareil impliqué dans l'activité malveillante. L'application crée un événement *Chiffrement détecté* qui contient des informations relatives à l'appareil compromis.
Zone de protection	`Windows` `macOS` `Linux`	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. `macOS` Kaspersky Endpoint Security protège tous les dossiers partagés des appareils macOS. Il n'est pas possible de modifier la zone de protection. `Windows` `Linux` Vous pouvez sélectionner la zone de protection : **Tous les dossiers réseau partagés de l'appareil protégé**. L'application surveillera l'activité des fichiers dans tous les dossiers partagés. **Uniquement les dossiers partagés indiqués**. L'application surveillera les tentatives de chiffrement uniquement dans les dossiers partagés indiqués.

Protection contre les Exploits

pour Windows, macOS et Linux

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.

Pour que le module Protection contre les Exploits fonctionne, le module Détection comportementale doit être activé. Pour optimiser les performances du module Protection contre les Exploits, nous vous recommandons également d'activer le module Protection contre les menaces Internet.

`Linux` Pour les appareils Linux, le module de noyau évolutif pour l'interception d'événements système doit également être activé.

Paramètres de protection contre les exploits

Paramètres	SE	Description
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**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. **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.
Protection de la mémoire du processus système	`Windows`	Si le commutateur est activé, Kaspersky Endpoint Security bloque les processus tiers qui tentent d'accéder à la mémoire des processus système.

Protection des connexions réseau et des moyens de communications

Protection contre les menaces par emails

pour Windows, macOS et Linux

La Protection contre les menaces par emails analyse les pièces jointes des messages entrants et sortants à la recherche de virus et d'autres pièces jointes malveillantes. 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.

`Linux` L'application pour les appareils Linux ne prend pas en charge le protocole NNTP.

Clients de messagerie pris en charge

- `Windows`, `macOS` Microsoft Office Outlook
- `Windows`, `macOS` Mozilla Thunderbird
- `Windows` Windows Mail
- `Windows`, `Linux` MyOffice Mail

- `Windows`, `Linux` R7-Office Organizer
- `macOS` Apple Mail
- `macOS` Canary Mail
- `macOS` Spark
- `macOS` Mimestream
- `macOS` Airmail
- `macOS` Post Box
- `macOS` Boxy Suite 2
- `macOS` Twobird
- `macOS` Shift
- `macOS` Clean Email
- `macOS` eM Client
- `macOS` Superhuman
- `macOS` Polymail
- `macOS` HEY
- `macOS` Mail+ for Gmail
- `macOS` Spike mail

`Windows` 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, l'Antivirus emails inclut une extension Kaspersky ASAP Outlook Plugin pour Microsoft Office Outlook. L'extension permet d'analyser les messages au niveau du client de messagerie. Le plug-in Kaspersky ASAP pour Outlook est compatible avec Outlook 2010, 2013, 2016, 2019 et 2021.

> 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	SE	Description
Exclusions de l'analyse	`Windows` `macOS` `Linux`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. Kaspersky Endpoint Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque.
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**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 reçoit alors un message avec une pièce jointe sûre. En cas d'échec de la désinfection, l'application supprime l'objet infecté. L'application ajoutera des informations sur l'action effectuée à l'objet du message, par exemple : *[Le message a été traité] <objet du message>*. `Windows` `Linux` **Désinfecter ; bloquer si la désinfection est impossible**. Lorsqu'un objet infecté est détecté dans un message entrant, l'application tente de le désinfecter. L'utilisateur reçoit alors un message avec une pièce jointe sûre. Si l'objet n'a pas pu être désinfecté, l'application ajoutera un avertissement à l'objet du message. L'utilisateur aura accès 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 ajoutera un avertissement à l'objet du message. L'utilisateur aura accès 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. `Linux` Pour les appareils Linux, le module Protection contre les menaces par emails ne tente pas de désinfecter l'objet infecté dans les messages sortants, mais bloque immédiatement la transmission du message.
Analyser le trafic POP3, SMTP, NNTP et IMAP	`Windows`	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	`Windows`	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. L'application peut analyser les messages entrants et sortants de Microsoft Outlook à différentes étapes : • **Analyser à la réception**. Si cette case est cochée, l'application utilise la Protection contre les menaces par emails lors de la réception de messages via Microsoft Outlook. • **Analyser à la lecture**. • **Analyser à l'envoi**. 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	`Windows` `Linux`	Analyse des 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 l'analyse, l'application effectue une décompression récursive. Cela permet de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (archive dans une archive).
Analyser les fichiers joints aux formats Office	`Windows` `Linux`	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 de moins de 1 Mo, quel que soit l'état de la case.
Ne pas analyser les archives de plus de (Mo)	`Windows` `macOS` `Linux`	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 dépasse celle spécifiée. Si cette case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques.
Ignorer un fichier si son analyse prend plus de (secondes)	`Windows` `macOS` `Linux`	Si la case est cochée, la durée d'analyse des archives jointes aux messages est limitée à la période spécifiée.

Paramètres	SE	Description
Filtre des pièces jointes	`Windows` `Linux`	Le filtre des pièces jointes détermine l'action que la Protection contre les menaces par emails applique aux fichiers joints aux emails. Le filtre des pièces jointes ne s'applique pas aux emails sortants. • **Ne pas modifier les pièces jointes**. Si cette option est sélectionnée, la Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques. • **Renommer les pièces jointes de types indiqués**. Lorsque cette option est sélectionnée, la Protection contre les menaces par emails remplace le dernier caractère de l'extension des fichiers joints des types spécifiés par un trait de soulignement (par exemple, attachment.doc_). L'utilisateur doit donc renommer le fichier pour l'ouvrir. • **Supprimer les pièces jointes de types indiqués**. Lorsque cette option est sélectionnée, la Protection contre les menaces par emails supprime les pièces jointes des types de fichiers spécifiés des messages électroniques. Vous pouvez spécifier les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.

Protection contre les menaces Internet

pour Windows, macOS et Linux

Le module Protection contre les menaces Internet empêche le téléchargement de fichiers malveillants via Internet. Il bloque également l'accès aux sites Internet malveillants et de phishing. Le module protège l'ordinateur à l'aide de bases antivirus, du service cloud Kaspersky Security Network et d'une analyse heuristique.

Le module Protection contre les menaces Internet analyse le trafic HTTP, HTTPS et FTP entrant, les sites Internet ainsi que les adresses Internet.

La Protection contre les menaces Internet sous `Linux` est désactivée par défaut. L'activation de l'Antivirus Internet peut réduire les performances des applications tierces installées et du système d'exploitation. Pour plus d'informations sur la configuration de l'application afin d'activer l'Antivirus Internet sur les appareils Linux, consultez la Base de connaissances du Support technique.

Paramètres de l'Antivirus Internet

Paramètres	SE	Description
URL de confiance	`Windows` `macOS` `Linux`	Liste des adresses Internet que la Protection contre les menaces Internet considère comme fiables. Le module n'analyse pas le trafic entrant et sortant de ces adresses à la recherche de menaces. La liste des adresses de confiance peut être utilisée, par exemple, si le module Protection contre les menaces Internet empêche le téléchargement d'un fichier à partir d'un site Internet connu. 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. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
Exclusions de l'analyse	`Windows`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.

Paramètres	SE	Description
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**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)**. `Windows` 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. `macOS` Kaspersky Endpoint Security affiche une notification contenant des informations sur le type de programme malveillant qui a infecté l'objet de trafic Internet et invite l'utilisateur à choisir l'action que Kaspersky Endpoint Security va prendre sur cet objet. Les actions disponibles varient en fonction de l'état de l'objet. `Linux` Kaspersky Endpoint Security informe l'utilisateur de la détection d'un objet infecté dans le trafic Internet. La Protection contre les menaces Internet autorise le téléchargement de cet objet sur l'appareil. À ce stade, l'application enregistre les informations relatives à l'objet infecté et ajoute celui-ci à la liste des menaces actives.

Protection contre les menaces réseau

pour Windows, macOS et Linux

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.

`Linux` La Protection contre les menaces Internet est désactivée par défaut. L'activation de la Protection contre les menaces réseau peut réduire les performances des applications tierces installées et du système d'exploitation. Pour plus d'informations sur la configuration de l'application afin d'activer la Protection contre les menaces réseau sur les appareils Linux, consultez la Base de connaissances de l'Assistance technique.

Paramètres de la Protection contre les menaces réseau

Paramètres	SE	Description
Adresses IP de confiance	`Windows` `Linux`	Liste des adresses IP des appareils de confiance. Le module Protection contre les menaces réseau ne bloque pas l'activité du réseau à partir de ces adresses. `Windows` Vous pouvez ajouter une adresse IP avec un port ou des plages de ports et un protocole spécifiés. `Linux` Vous pouvez ajouter uniquement une adresse IP à la liste des exclusions. L'application n'ajoute pas non plus au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions.
Action en cas de détection d'une menace	`Windows` `macOS` `Linux`	**Interdire**. Lorsqu'une menace est détectée, la Protection contre les menaces réseau bloque l'attaque. **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. 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.

Paramètres	SE	Description
Traiter l'analyse des ports et l'inondation des réseaux comme des attaques	`Windows`	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. 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. 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.
Protection contre le MAC Spoofing	`Windows`	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

pour Windows, macOS et Linux

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.

`Linux` Pour les appareils Linux, l'application utilise le module Gestion du pare-feu. Le module gère les paramètres et les règles du pare-feu du système d'exploitation.

Paramètres du pare-feu

Paramètres	SE	Description
Règles pour les paquets réseau	`Windows` `macOS` `Linux`	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 Kaspersky pour une protection optimale du trafic réseau des ordinateurs sous l'administration des systèmes d'exploitation Microsoft Windows et Linux. 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.

Paramètres	SE	Description
Réseaux disponibles	`Windows` `macOS` `Linux`	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 le type **Réseau public**. Vous ne pouvez pas modifier le type de réseau Internet. 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). Lorsque l'utilisateur utilise un ordinateur connecté à un tel réseau, le pare-feu bloque l'accès 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 toute activité réseau au sein des réseaux ayant cet état.
Toujours ajouter les règles d'autorisation pour les ports de l'Agent d'administration	`macOS` `Linux`	Cette case active ou désactive l'ajout automatique de règles d'autorisation pour les ports de l'Agent d'administration.
Privilèges des applications et des ressources protégées	`Windows`	**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.

Contrôles de sécurité

Contrôle des appareils

pour Windows, macOS et Linux

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.

Le Contrôle des appareils permet ou bloque l'accès aux appareils aux niveaux suivants :

- **Type d'appareil** Par exemple, imprimantes, disques amovibles, lecteurs CD/DVD.
- **Bus de connexion**. Un *bus de connexion* est une interface qui permet de connecter des appareils à l'appareil (USB, FireWire, etc.). Si le mode **Dépend du bus** est sélectionné pour le type d'appareil, l'application contrôle l'accès à l'appareil conformément au mode du bus auquel l'appareil se connecte (par exemple, USB).
- **Appareils de confiance** Les *appareils de confiance* sont des appareils auxquels des utilisateurs ou des groupes d'utilisateurs donnés ont un accès total à tout moment.

Vous pouvez ajouter des appareils de confiance en fonction des données suivantes :

- `Windows` `macOS` **Modèle**. Chaque appareil possède un identifiant de fabricant (en anglais, Vendor ID - VID) et un identifiant de produit (en anglais, Product ID - PID). Vous pouvez consulter les identificateurs dans les propriétés de l'appareil à l'aide des outils du système d'exploitation. Modèle de saisie du VID et du PID : `VID_1234&PID_5678`. L'ajout d'appareil par modèle est pratique si vous utilisez des appareils d'un certain modèle dans votre organisation. Ainsi, vous pouvez ajouter tous les appareils de ce modèle.

- **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.

- `Windows` `macOS` **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. Le caractère `?` remplace n'importe quel caractère unique. Par exemple, `VID_05AC&PID_*`.

- **Appareils par masque d'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. Le caractère `?` remplace n'importe quel caractère unique. Par exemple, `WDC_C*`.

`Linux` Pour les appareils Linux, l'action exécutée par le module dépend du mode d'interception des opérations sur les fichiers sélectionné dans la section Paramètres généraux, sous-section Paramètres de détection.

Paramètres du contrôle des appareils

Paramètres	SE	Description
Appareils de confiance	`Windows` `macOS` `Linux`	Liste des appareils de confiance et des utilisateurs autorisés à accéder à ceux-ci. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque.
Modèles de messages	`Windows` `Linux`	**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.
Autoriser les demandes d'accès temporaire	`Windows` `Linux`	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.
Mode de fonctionnement	`Linux`	Kaspersky Endpoint Security exécute l'action sélectionnée en cas de tentative d'accès à l'appareil dont l'accès est bloqué conformément aux paramètres du Contrôle des appareils. • **Informer**. Si vous sélectionnez cette option, Kaspersky Endpoint Security teste le mode d'accès sélectionné et génère un événement relatif à la tentative détectée d'accès à un appareil. • **Bloquer**. Si vous sélectionnez cette option, Kaspersky Endpoint Security applique le mode d'accès défini pour l'appareil ou le bus.
Appareils et réseaux Wi-Fi	`Windows` `macOS` `Linux`	Liste de tous les types d'appareils disponibles selon la classification du module Contrôle des appareils, y compris leurs états d'accès respectifs.
Bus de connexion	`Windows` `Linux`	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.

Paramètres	SE	Description
Anti-Bridging	`Windows`	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.

Contrôle Internet

pour Windows, macOS et Linux

Le Contrôle Internet contrôle l'accès des utilisateurs aux ressources Internet. Cela vous permet de réduire la consommation de trafic et de réduire l'utilisation inappropriée du temps de travail. Lorsqu'un utilisateur tente d'ouvrir un site dont l'accès est restreint par le Contrôle Internet, l'application Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement.

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 l'accès aux sites Internet pour les zones d'analyse suivantes :

- **Catégorie du site.** 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). Vous pouvez limiter l'accès des utilisateurs à certaines catégories, par exemple, la catégorie *Réseaux sociaux* ou d'autres catégories.
- `Windows` **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 Office* uniquement pour la catégorie de sites *Emails en ligne*.

Le Contrôle Internet permet également de configurer les paramètres avancés des règles d'accès aux sites Internet suivants :

- **Utilisateur ou groupe d'utilisateurs auxquels la règle du Contrôle des applications s'applique**.

  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'accès des appareils**.

  Par exemple, vous pouvez limiter l'accès à Internet via un navigateur uniquement pendant les heures ouvrables.

Paramètres du Contrôle Internet

Paramètres	SE	Description
Modèles de messages	`Windows` `Linux`	**Avertissement**. Le champ de saisie contient un modèle de message qui apparaît lorsqu'une règle est déclenchée, avertissant d'une tentative d'accès à une ressource Web non recommandée. **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**. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise. Utilisé si l'utilisateur pense que l'accès à la ressource Internet a été bloqué par erreur. 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.
Liste des règles	`Windows` `macOS` `Linux`	Liste des règles d'accès aux sites Internet. Chaque règle est prioritaire. Plus une règle figure en haut de la liste, plus sa priorité est élevée. Si un site Internet est ajouté à plusieurs règles, Contrôle Internet utilise la règle dont la priorité est la plus élevée.
Action par défaut	`Windows` `macOS` `Linux`	Règle d'accès aux ressources Internet qui ne figurent dans aucune des règles. Les options suivantes existent : • **Autoriser tout ce qui ne figure pas dans la liste des règles**. • **Bloquer tout ce qui ne figure pas dans la liste des règles**.
Mettre fin aux sessions de navigation des utilisateurs actifs une fois la règle appliquée	`Windows`	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.
Surveillance des sessions Internet	`Windows`	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 des événements Windows et dans un rapport. 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 applications

pour Windows et Linux

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.

Le module Contrôle des applications utilise des règles pour contrôler le lancement des applications sur les appareils protégés. Une règle contient des conditions et des actions que le module Contrôle des applications exécute lorsqu'une règle se déclenche. Par exemple, la catégorie à laquelle appartient une application. Une *catégorie d'applications* est un groupe d'applications qui ont quelque chose en commun. Par exemple, une catégorie qui comprend les fichiers exécutables des applications installées ou une catégorie qui comprend l'ensemble standard des applications utilisées dans l'organisation. Vous ne pouvez utiliser une catégorie dans une seule règle.

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.

Paramètres du Contrôle des applications

Paramètres	SE	Description
Modèles de messages	`Windows`	**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 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.
Mode de fonctionnement	`Windows` `Linux`	Vous avez le choix entre les options suivantes : • **Autoriser tout ce qui ne figure pas dans la liste des règles**. Si cette option est sélectionnée, le Contrôle des applications permet à tous les utilisateurs de lancer n'importe quelle application, à l'exception des applications interdites par les règles de blocage du Contrôle des applications. • **Bloquer tout ce qui ne figure pas dans la liste des règles**. Si cette option est sélectionnée, le Contrôle des applications empêche tous les utilisateurs de lancer une application, à l'exception des applications autorisées par les règles d'autorisation du Contrôle des applications.
Action lors du démarrage des applications	`Windows` `Linux`	• **Appliquer les règles**. Kaspersky Endpoint Security gère le démarrage des applications selon le mode sélectionné. • **Informer**. Kaspersky Endpoint Security informe de la tentative d'exécution d'une application.
Ajouter des règles depuis la stratégie aux règles locales	`Linux`	Si vous choisissez cette option, l'application applique les règles configurées dans la stratégie en même temps que les règles locales configurées sur l'appareil protégé.
Utiliser une vérification stricte de la signature numérique	`Windows`	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.
Surveiller le chargement des modules DLL	`Windows`	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.

Paramètres	SE	Description
Règles	`Windows` `Linux`	Règle du Contrôle des applications que Kaspersky Endpoint Security utilise pour contrôler le lancement des applications sur les appareils protégés. Pour chaque mode du Contrôle des applications, vous pouvez ajouter cinq règles maximum.
Programmes de mise à jour de confiance	`Windows`	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 permet de créer et d'exécuter de nouveaux fichiers exécutables pour de telles applications.

Contrôle de l'intégrité du système

pour Windows et Linux

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.

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.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre de la liste des zones. Si nécessaire, placez le sous-répertoire à un niveau plus élevé dans la liste que le répertoire parent afin de configurer pour un sous-répertoire des paramètres de sécurité différents de ceux du répertoire parent.

`Linux` Les limitations techniques du système d'exploitation Linux empêchent l'application d'identifier l'utilisateur ou le processus qui a apporté les modifications au fichier.

Paramètres du Contrôle de l'intégrité du système

Paramètres	SE	Description
Contrôle de l'intégrité du système en temps réel	`Windows`	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.
Action en cas de détection de modifications au sein du système	`Windows`	**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.
Surveiller les fichiers et le registre	`Windows`	Le Contrôle de l'intégrité du système surveille les modifications apportées aux fichiers, aux dossiers et au registre.
Surveiller les appareils	`Windows`	Le Contrôle de l'intégrité du système surveille la connexion et la déconnexion des appareils externes.
Vérification de l'intégrité du système	`Windows`	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	SE	Description
Zones de contrôle	`Linux`	Le tableau contient les zones de contrôle pour le module Contrôle de l'intégrité du système. L'application contrôle les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau contient la zone de contrôle des **Objets internes de Kaspersky**.
Zones d'exclusions	`Linux`	Le tableau contient les zones d'exclusion de l'analyse. L'application n'analysera les fichiers et les répertoires situés dans les chemins spécifiés dans le tableau. Par défaut, le tableau est vide.
Exclusions selon un masque	`Linux`	Vous pouvez configurer des exclusions d'analyse pour des objets par masque de nom. L'application n'analysera pas les fichiers dont les noms contiennent les masques définis. Par défaut, la liste des masques est vide.

Exclusions de l'analyse pour l'application

pour Windows, macOS et Linux

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.

Kaspersky Endpoint Security prend en charge la spécification des noms de fichiers ou de dossiers à l'aide de masques. Vous pouvez utiliser les caractères génériques suivants dans 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.

- 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.

Paramètres des zones de confiance

Paramètres	SE	Description
Adresses Internet	`Windows` `macOS` `Linux`	Liste des adresses Internet que la Protection contre les menaces Internet considère comme fiables. Le module n'analyse pas le trafic entrant et sortant de ces adresses à la recherche de menaces. La liste des adresses de confiance peut être utilisée, par exemple, si le module Protection contre les menaces Internet empêche le téléchargement d'un fichier à partir d'un site Internet connu. 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.
Adresses IP	`Windows` `Linux`	Liste des adresses IP des appareils de confiance. Le module Protection contre les menaces réseau ne bloque pas l'activité du réseau à partir de ces adresses. `Windows` Vous pouvez ajouter une adresse IP avec un port ou des plages de ports et un protocole spécifiés. `Linux` Vous pouvez ajouter uniquement une adresse IP à la liste des exclusions. L'application n'ajoute pas non plus au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions.
Ports réseau	`Windows` `macOS` `Linux`	Liste des ports connus et enregistrés sur lesquels les modules Contrôle Internet, Protection contre les fichiers malicieux, Protection contre les menaces Internet, Protection contre les menaces par emails, Protection contre les Exploits et Détection comportementale contrôlent les flux de données. Si ce commutateur est activé, le port est considéré comme fiable et les données passant par un tel port sur les appareils de confiance ne sont pas surveillées.
Certificats de confiance	`Windows` `macOS` `Linux`	Liste des certificats racines que Kaspersky Endpoint Security considère comme étant de confiance. La liste des certificats racine de confiance est utilisée lors de l'analyse des connexions chiffrées.

Paramètres	SE	Description
Noms d'ordinateurs / adresses IP de confiance	`Windows`	Liste des noms d'hôtes et des adresses IP que le module Détection comportementale considère comme étant fiables. Kaspersky Endpoint Security n'analyse pas les appareils indiqués à la recherche de virus et d'autres applications menaçantes.
Domaines	`Windows` `Linux`	Liste des domaines de confiance. Les modules Protection contre les menaces Internet, Contrôle Internet et Cloud Discovery (uniquement pour appareil Windows) ne contrôlent pas les connexions chiffrées avec ces domaines. Les connexions aux domaines figurant dans cette liste seront bloquées sur les appareils Windows si elles sont établies via le protocole SSL/TLS et si l'option "Bloquer les connexions SSL/TLS" est activée.
Points de montage fiables	`Linux`	Liste des points de montage fiables. Ils sont exclus des analyses effectuées par les modules Protection contre les fichiers malicieux, Protection contre le chiffrement, Contrôle des applications et Détection comportementale. Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.
Exclusions de l'interception du trafic	`Linux`	Liste des connexions réseau que Kaspersky Endpoint Security exclut de l'interception du trafic. Les exclusions relatives à l'interception du trafic concernent les modules Protection contre les menaces Internet, Protection contre les menaces réseau et Contrôle Internet. Une connexion exclue est définie par les paramètres suivants : • Direction du trafic, entrant ou sortant. • Adresse IP de l'appareil distant, c'est-à-dire l'adresse IP dont le trafic entrant et sortant est exclu de l'interception (en fonction de la direction du trafic). • Port de destination, c'est-à-dire un port sur l'appareil protégé (dans une exclusion d'interception du trafic entrant) ou un port sur l'appareil distant (dans une exclusion d'interception du trafic sortant). Les exclusions relatives à l'interception du trafic ne s'appliquent qu'aux connexions TCP et n'ont aucune incidence sur les règles pour les paquets réseau.
Réseaux Wi-Fi	`macOS`	Liste des réseaux Wi-Fi de confiance. Vous pouvez définir les paramètres suivants : • Nom du réseau Wi-Fi. • Type de chiffrement. • Type d'authentification.
Applications	`Windows` `macOS` `Linux`	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.
Exclusions de l'analyse des logiciels malveillants	`Windows` `macOS` `Linux`	*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 d'analyse vous permettent de travailler avec des applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky.
Appareils	`Windows` `Linux`	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.

Paramètres généraux

Paramètres de détection

pour Windows, macOS et Linux

Cette section décrit comment configurer les paramètres de détection en fonction de vos besoins. L'efficacité de la détection et de la prévention des menaces dépend de la configuration adéquate des paramètres.

Paramètres de détection

Paramètres	SE	Description
Détection d'autres types d'objets	`Windows` `macOS` `Linux`	Quelle que soit la configuration des paramètres de Kaspersky Endpoint Security, l'application détecte et bloque toujours les virus, les vers, les chevaux de Troie et les outils malveillants. Ces programmes peuvent provoquer des dégâts considérables à votre ordinateur. Vous pouvez en outre activer la détection des types d'objets suivants : • **Programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles**. Ces applications ne possèdent pas nécessairement de fonctionnalités malveillantes, mais elles peuvent être exploitées par des pirates informatiques. Pour obtenir des informations détaillées sur les applications légitimes que les intrus peuvent utiliser pour endommager l'ordinateur ou les données utilisateur, consultez le site Internet de l'Encyclopédie Kaspersky. • `Windows` **Logiciels publicitaires**. Elles affichent des bannières publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. • `Windows` **Numéroteurs automatiques**. Les numéroteurs automatiques peuvent établir discrètement des connexions téléphoniques à l'aide d'un modem. Ces applications sont également des logiciels légitimes qui peuvent être utilisés par des pirates informatiques pour compromettre l'appareil ou les données de l'utilisateur. • `Windows` **Compresseurs**. Pour dissimuler les programmes malveillants afin qu'ils ne soient pas détectés par un antivirus, les pirates informatiques les emballent à l'aide de compacteurs spéciaux. Les experts de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.
Technologie de désinfection avancée	`Windows`	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*.
Bloquer l'accès aux fichiers pendant l'analyse	`Linux`	Si cette case est cochée, l'application bloque l'accès aux fichiers pendant qu'ils sont analysés par les modules Protection contre les fichiers malicieux et Contrôle des appareils, l'action Prévention de l'exécution et la tâche Analyse des disques amovibles. Si la case est décochée, l'accès à n'importe quel fichier est autorisé pendant la durée de l'analyse, et l'analyse s'exécute en mode asynchrone.
Paramètres de journalisation des objets	`Linux`	**Journaliser les objets non infectés**. Si cette case est cochée, l'application enregistre les événements *ObjectProcessed* dans le journal pour tout objet analysé. **Journaliser les objets non traités**. Si cette case est cochée, l'application enregistre un événement *ObjectNotProcessed* dans le journal. **Journaliser les objets compactés**. Si cette case est cochée, l'application enregistre un événement *PackedObjectDetected* dans le journal.

Kaspersky Security Network

pour Windows, macOS et Linux

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 une infrastructure de service cloud qui permet d'accéder à la base de connaissances de Kaspersky sur la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network permet à Kaspersky Endpoint Security de réagir plus rapidement aux nouvelles menaces, améliore les performances de certains modules de protection et réduit la probabilité de faux positifs. 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 plus de détails sur la configuration de 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 décider de participer au KSN ou d'interrompre votre participation à tout moment.

Pour en savoir plus sur la soumission des statistiques obtenues pendant la participation à KSN, sur le stockage et la destruction de ces informations, consultez la Déclaration de Kaspersky Security Network et le site 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 les bases 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 légale ou restriction de la sécurité de l'entreprise d'envoyer des données en dehors du pays ou du réseau local de l'entreprise.

Paramètres de Kaspersky Security Network

Paramètres	SE	Description
Utiliser le mode étendu de KSN	`Windows` `macOS` `Linux`	Le *mode étendu de 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. `Linux` Pour les appareils Linux, cette option est masquée lors de l'utilisation de la solution *Kaspersky Private Security NetworK (KPSN).*
Utiliser le mode cloud	`Windows` `macOS` `Linux`	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 la case est cochée, 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 la case est décochée, 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	`Windows`	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	`Windows` `macOS` `Linux`	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	`Windows` `macOS` `Linux`	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).

Interaction avec l'utilisateur

pour Windows, macOS et Linux

Cette section décrit comment configurer les paramètres d'interface de l'application et les paramètres d'interaction utilisateur.

Paramètres d'interface de l'application

Paramètres	SE	Description
Lancer Kaspersky Endpoint Security au démarrage de l'ordinateur (recommandé)	`Windows` `macOS`	Si cette fonctionnalité est activée, Kaspersky Endpoint Security est lancé après le chargement du système d'exploitation pour protéger l'ordinateur pendant toute la durée de la session. Si cette fonctionnalité est désactivée, 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.
Afficher l'icône de l'application	`Windows` `macOS`	L'ordinateur client dispose d'une icône d'application dans la zone de notification. 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 présenter l'interface de l'application aux utilisateurs	`Windows` `macOS`	Si cette case est sélectionnée, Kaspersky Endpoint Security ne permet pas à l'utilisateur d'ouvrir la fenêtre principale de l'application et masque l'interface de l'application sur un ordinateur distant. Si cette case est sélectionnée, l'utilisateur peut ouvrir la fenêtre principale de Kaspersky Endpoint Security et utiliser l'interface de l'application sur un ordinateur distant.

Paramètres	SE	Description
Masquer la section Surveillance des applications	`Windows`	Si cette case est cochée, le bouton **Surveillance des applications** n'est pas disponible dans la fenêtre principale de Kaspersky Endpoint Security sur l'ordinateur client. 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.
Gérer les mises à jour localement	`macOS`	Si cette case est cochée, l'utilisateur peut gérer localement les mises à jour de Kaspersky Endpoint Security sur un ordinateur distant. Si cette case est décochée, vous pouvez administrer les mises à jour de Kaspersky Endpoint Security sur un ordinateur distant uniquement à l'aide du plug-in Kaspersky Endpoint Security de Kaspersky Security Center.
Gérer les clés localement	`macOS`	Si cette case est cochée, l'utilisateur peut administrer localement les clés de Kaspersky Endpoint Security sur un ordinateur distant. Si cette case est décochée, vous pouvez administrer les clés de Kaspersky Endpoint Security sur un ordinateur distant uniquement à l'aide du plug-in Kaspersky Endpoint Security de Kaspersky Security Center.
Quitter l'application	`macOS`	Si cette case est cochée, la commande **Quitter** est présente dans le menu contextuel de l'icône de l'application. L'utilisateur d'un ordinateur distant peut arrêter Kaspersky Endpoint Security sur l'ordinateur distant. Si cette case est décochée, la commande **Quitter** n'est pas présente dans le menu contextuel de l'icône de l'application. L'utilisateur d'un ordinateur distant ne peut pas arrêter Kaspersky Endpoint Security sur l'ordinateur distant.
Accéder aux tâches locales	`Windows` `Linux`	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 la case est décochée, l'utilisation des tâches locales est interrompue. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. Les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de Kaspersky Endpoint Security ou via la ligne de commande. 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	`Windows`	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	`Windows` `Linux`	Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans la console de Kaspersky Endpoint Security. 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 Endpoint Security.
État de l'ordinateur	`Windows`	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*.
Notifications de l'état de l'application	`Windows`	Paramètres des notifications d'événements de l'application dans la barre d'état système. Sélectionnez les cases en regard des catégories d'événements pour lesquels vous souhaitez voir des notifications dans la zone de notification. • **Présence de menaces actives**. • **Redémarrage de l'ordinateur requis**. • **Problèmes de bases anti-malware**. • **Problèmes de niveau de protection**. • **Problèmes de licence**. • **Mises à jour disponibles**. 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.
Notifications sur l'état des bases anti-malware locales	`Windows`	Paramètres de notification sur le caractère dépassé des bases antivirus que l'application utilise. Vous pouvez définir le nombre de jours au bout desquels Kaspersky Endpoint Security envoie les messages "Les bases sont dépassées" et "Les bases sont fortement dépassées" à l'utilisateur.
Paramètres de démarrage de l'application	`Linux`	Paramètres de lancement de l'application : • **Nombre maximum de tentatives consécutives infructueuses pour démarrer une application**. • **Durée maximale d'attente pour le démarrage de l'application (min)**. À l'expiration du délai d'attente spécifié, le processus kesl est relancé.

Paramètres	SE	Description
Installer les mises à jour de l'application sans redémarrer l'ordinateur	`Windows`	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 niveau sur la machine virtuelle sans redémarrage. Pour mettre à niveau l'application sur une machine virtuelle, vous devez redémarrer la machine virtuelle. Une fois que vous aurez mis à niveau 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. 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 niveau de l'application sans redémarrage est désactivée. Si l'application est installée sur un serveur, l'option de mise à niveau de l'application sans redémarrage est activée.
Compatibilité avec les logiciels d'administration à distance	`Windows`	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. Le mode de compatibilité RAT peut réduire le niveau de sécurité de l'ordinateur. Nous vous déconseillons d'activer le mode de compatibilité si Kaspersky Endpoint Security ne pose pas de problèmes avec votre RAT. Cette fonction est désactivée par défaut. 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.

Performances

pour Windows, macOS et Linux

Dans Kaspersky Endpoint Security, le concept de performance fait référence à la consommation d'énergie et à l'utilisation des ressources de l'ordinateur.

Paramètres	SE	Description
Attribution des ressources aux autres applications	`Windows`	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. Le mode de transfert des ressources vers d'autres applications est activé par défaut.
Reporter ou ignorer les tâches planifiées en cas d'alimentation par batterie	`Windows` `macOS` `Linux`	Si cette fonctionnalité est activée, Kaspersky Endpoint Security passe en mode d'économie d'énergie. `Windows` Kaspersky Endpoint Security *reporte* les tâches planifiées. Vous pouvez démarrer manuellement une analyse ou les tâches de mise à jour, si nécessaire. `macOS` `Linux` Kaspersky Endpoint Security *annule* 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 des logiciels malveillants* • *Mise à jour des bases données d'applications malveillantes* • *Vérification de l'intégrité de l'application* • *Analyse IOC*.
Limitation de l'utilisation du processeur pour les tâches d'analyse	`Windows` `macOS` `Linux`	Pour optimiser les performances de Kaspersky Endpoint Security, vous pouvez limiter l'utilisation du processeur par les tâches d'analyse. Selon le système d'exploitation utilisé, les tâches pour lesquelles l'utilisation du processeur est limitée peuvent varier : • `Windows` `Linux` Analyse des logiciels malveillants • `macOS` `Linux` Critical Areas Scan • `Linux` Inventory • `Linux` Analyse du conteneur Si cette fonctionnalité est activée, la charge moyenne générée par la tâche d'analyse sur tous les cœurs du processeur se rapproche de la valeur indiquée.
Limite d'utilisation de la mémoire pour les tâches d'analyse (Mo)	`Linux`	Vous pouvez configurer la limite d'utilisation de la mémoire pour les tâches d'analyse (*Analyse des logiciels malveillants*, *Analyse des zones critiques*, *Inventaire* et *Analyse des conteneurs*).
Configurer l'exclusion de l'analyse de la mémoire du processus	`Linux`	Vous pouvez configurer des exclusions d'analyse pour la mémoire des processus. L'application n'analysera pas la mémoire des processus spécifiés. Spécifiez le chemin d'accès aux processus que l'application exclura de l'analyse de la mémoire des processus. Vous pouvez utiliser des masques pour spécifier le chemin. Par défaut, la liste est vide.
Limiter l'utilisation de la mémoire par l'application	`Linux`	Vous pouvez configurer la limite d'utilisation de la mémoire résidente pour l'application. Le réglage par défaut est automatique. **Méthode de calcul des limites** : • **Illimité**. Si cette option est sélectionnée, l'utilisation de la mémoire résidente n'est pas limitée. • **Définir une valeur exacte (%)**. • **Définir une valeur exacte (Mo)**. • **Utiliser la plus petite des deux valeurs (% ou Mo)**. • **Utiliser la plus élevée des deux valeurs (% ou Mo)**. • **Limitée automatiquement (recommandé)**. Si cette option est sélectionnée, l'utilisation de la mémoire résidente est limitée automatiquement.
Activer la surveillance de la stabilité de l'application	`Linux`	Vous pouvez activer ou désactiver la surveillance de la stabilité des applications de Kaspersky Endpoint Security, qui suit le nombre d'arrêts anormaux des applications et notifie l'administrateur des performances instables des applications. Si la case est cochée, l'application surveille le fonctionnement de Kaspersky Endpoint Security. Pour appliquer le paramètre, redémarrez l'application. Si l'application est instable, le message suivant s'affiche dans les propriétés de l'appareil avec l'application installée : *<Number> arrêts anormaux de l'application depuis<date and time>*.

Paramètres du réseau

pour Windows, macOS et Linux

Vous pouvez configurer le serveur proxy utilisé pour la connexion Internet, sélectionner le mode de surveillance des ports réseau et mettre en place l'analyse des connexions chiffrées.

Paramètres du réseau

Paramètres	SE	Description
Certificats racine de confiance	`Windows` `macOS` `Linux`	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.
Serveur proxy	`Windows` `macOS` `Linux`	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.
Utiliser l'authentification sur le serveur proxy	`Windows` `macOS` `Linux`	Si cette case est cochée, l'application utilise l'authentification avec un nom d'utilisateur et un mot de passe lors de la connexion au serveur proxy. `Windows` Pour les appareils Windows, il faut sélectionner un type d'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. • **Authentification Kerberos avec nom d'utilisateur et mot de passe**. Authentification Kerberos avec des identifiants spécifiés manuellement.
Ne pas utiliser de serveur proxy pour les adresses locales	`Windows` `macOS`	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.
Ne pas utiliser le serveur proxy pour les modules	`Linux`	Cochez les cases en regard des modules d'application pour lesquels vous ne souhaitez pas utiliser le serveur proxy : • **Endpoint Detection and Response Expert (on-premise)** – ne pas utiliser de serveur proxy lors de la connexion aux serveurs KATA. • **KATA Sandbox** – ne pas utiliser de serveur proxy lors de la connexion aux serveurs Central Node responsables de l'interaction avec KATA Sandbox. • **Network Detection and Response (KATA)** – ne pas utiliser de serveur proxy lors de la connexion aux serveurs Network Detection and Response.
Ne pas utiliser de serveur proxy pour les adresses IP et les noms DNS spécifiés	`Linux`	Le tableau contient une liste d'adresses IP et de noms DNS pour lesquels le serveur proxy ne doit pas être utilisé. Pour spécifier l'adresse, vous pouvez utiliser des masques (symboles `*` et `?`). Vous pouvez ajouter, modifier ou supprimer des adresses dans le tableau.
Analyse des connexions chiffrées	`Windows` `macOS` `Linux`	Cette fonctionnalité permet aux modules Protection contre les menaces Internet, Protection contre les menaces par emails, Contrôle Internet et Cloud Discovery de surveiller et de gérer les connexions chiffrées (HTTPS). `Linux` Pour les appareils Linux, la **Stratégie de vérification du certificat** est disponible, ce qui détermine la façon dont l'application valide les certificats : • **Vérification locale** signifie que l'application n'utilise pas Internet pour valider les certificats. • **Vérification complète** (par défaut) signifie que l'application utilise Internet pour valider et télécharger les chaînes manquantes nécessaires pour valider un certificat.
Domaines de confiance	`Windows` `Linux`	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.

Paramètres	SE	Description
Restreindre le trafic sur les connexions limitées	`Windows`	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	`Windows`	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. 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.
Vérifier les connexions chiffrées avec un site à l'aide d'un certificat EV	`Windows`	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 ce commutateur est activé, l'application déchiffre et surveille les connexions chiffrées avec les sites Internet qui utilisent un certificat EV. Si le commutateur est désactivé, 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.
Bloquer les connexions SSL 2.0	`Windows`	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 TLS 1.0	`Windows`	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.
Bloquer les connexions SSL 3.0	`Windows`	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.
Ports contrôlés	`Windows` `macOS` `Linux`	**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. Pour les appareils Mac, seuls les ports sélectionnés peuvent être surveillés.
Applications surveillées	`Windows`	Liste des applications pour lesquelles tout le trafic sur tous les ports est surveillé, quels que soient les paramètres d'analyse des ports.

Paramètres	SE	Description
Sélectionnez la liste de certificats à utiliser par Firefox	`macOS`	**Trousseau des racines du système (recommandé)**. Si cette option est sélectionnée, Kaspersky Endpoint Security analyse le trafic HTTPS chiffré dans le navigateur Mozilla Firefox à l'aide d'un certificat racine issu du trousseau des racines du système. Cette option est sélectionnée par défaut. **Liste de certificats dans les paramètres du navigateur Mozilla Firefox**. Si cette option est sélectionnée, Kaspersky Endpoint Security utilise le certificat provenant de la liste de certificats du navigateur. Dans ce cas, vous devez ajouter manuellement le certificat Kaspersky Endpoint Security au stockage des certificats de Mozilla Firefox. Pour en savoir plus, consultez l'article Comment ajouter le certificat Kaspersky au stockage des certificats de Mozilla Firefox ?.
Mode d'interception du trafic	`Linux`	**iptables**. Kaspersky Endpoint Security utilise l'utilitaire iptables pour intercepter le trafic. **eBPF**. L'application utilise la technologie eBPF pour intercepter le trafic.

Analyser les conteneurs.

pour Linux

L'application vérifie les conteneurs et les espaces de noms en cours d'exécution en temps réel. L'application prend en charge l'intégration avec le système de gestion de conteneurs Docker, l'environnement CRI-O ainsi que les utilitaires Podman et runc.

L'analyse des conteneurs requiert l'activation du module Protection contre les fichiers malicieux. Les paramètres du module Protection contre les fichiers malicieux sont appliqués lors de l'analyse des conteneurs et des espaces de noms.

L'application ne vérifie pas les espaces de noms et les conteneurs à moins que les modules permettant de travailler avec les conteneurs et les espaces de noms ne soient installés sur le système d'exploitation.

Paramètres d'analyse de conteneur

Paramètres	SE	Description
Action en cas de détection d'une menace	`Linux`	**Ignorer le conteneur**. En cas de détection d'un objet infecté, l'application n'exécute aucune action sur le conteneur. **Arrêter le conteneur**. En cas de détection d'un objet infecté, l'application arrête le conteneur. **Arrêter le conteneur en cas d'échec de la désinfection**. Si un objet infecté n'a pas pu être désinfecté, l'application arrête le conteneur.
Utiliser Docker	`Linux`	Utilisation de l'environnement Docker. Pour utiliser l'environnement, saisissez un chemin d'accès ou un URI (identifiant universel de ressource) du socket Docker.
Utiliser CRI-O	`Linux`	Utilisation de l'environnement CRI-O. Pour pouvoir utiliser cet environnement, saisissez le chemin d'accès au fichier de configuration CRI-O.
Utiliser Podman	`Linux`	Utilisation de l'utilitaire Podman. Pour utiliser cet utilitaire, saisissez le chemin d'accès au fichier exécutable de l'utilitaire et le chemin d'accès au répertoire racine du stockage du conteneur.
Utiliser runc	`Linux`	Utilisation de l'utilitaire runc. Pour utiliser cet utilitaire, saisissez le chemin d'accès au fichier exécutable de l'utilitaire et le chemin d'accès au répertoire racine du stockage d'état du conteneur.

Support technique

pour Windows et Linux

Afin d'éliminer les éventuels dysfonctionnements de Kaspersky Endpoint Security sur les ordinateurs, le personnel de l'Assistance technique peut avoir besoin d'informations sur le système et sur les événements survenus pendant le fonctionnement de l'application. Ces informations sont reprises dans les fichiers de vidage et les fichiers de traçage.

Le *fichier de vidage* contient toutes les informations relatives à la mémoire de travail des processus de Kaspersky Endpoint Security au moment de la création de ce fichier de vidage.

Le *fichier de traçage* permet de retracer l'exécution des commandes de l'application étape par étape et de déterminer à quel stade de l'exécution l'erreur a eu lieu.

Les fichiers de vidage et les fichiers de traçage peuvent contenir des données sensibles. Pour contrôler l'accès aux données, vous devez garantir vous-même la protection de ces fichiers.

Les fichiers de vidage et 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.

Une fois qu'un profil de sécurité a été attribué aux ordinateurs, l'application commence à écrire les fichiers de vidage. Après un dysfonctionnement, au prochain lancement de l'application, une fenêtre de chargement des informations pour le Support Technique s'ouvre. Cette fenêtre permet de vérifier les informations relatives aux fichiers de vidage créés et d'approuver leur envoi à Kaspersky.

Paramètres de l'Assistance technique

Paramètres	SE	Description
Enregistrement des fichiers dump ACTIVÉ	`Windows` `Linux`	Si l'écriture de fichiers de vidage est activée, Kaspersky Endpoint Security en crée en cas de plantage de l'application. `Linux` Les fichiers de vidage occupent un espace disque considérable. Si l'espace libre sur le disque est inférieur à 4 Go, l'activation du vidage peut entraîner un manque d'espace disque.
Protection des fichiers de vidage et de traçage ACTIVÉE	`Windows`	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.
Chemin d'accès au vidage du code	`Windows` `Linux`	Les fichiers de vidage sont conservés dans les dossiers suivants : • `Windows` : `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` Vous ne pouvez pas définir un dossier différent pour les fichiers de vidage. • `Linux` : `var/opt/kaspersky/kesl/common/dumps` et `var/opt/kaspersky/kesl/common/dumps-user` Si vous indiquez un autre répertoire, assurez-vous que l'utilisateur qui exécute Kaspersky Endpoint Security dispose des autorisations de lecture et d'écriture pour ce répertoire. L'accès au répertoire du fichier de vidage requiert des autorisations racine.
Chemin d'accès au dossier de traçage	`Windows` `Linux`	Les fichiers de traçage sont conservés dans les dossiers suivants : • `Windows` : `%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces` Vous ne pouvez pas définir un dossier différent pour les fichiers de traçage. • `Linux` : `var/log/kaspersky/kesl` Si vous indiquez un autre répertoire, assurez-vous que l'utilisateur qui exécute Kaspersky Endpoint Security dispose des autorisations de lecture et d'écriture pour ce répertoire. L'accès au répertoire du fichier de traçage requiert des autorisations racine.
Taille maximale du fichier de traçage (Mo)	`Linux`	Dans ce champ, vous pouvez saisir la taille maximale d'un fichier de traçage d'application (en mégaoctets).
Nombre maximum de fichiers de traçage	`Linux`	Dans ce champ, vous pouvez saisir le nombre maximal de fichiers de traçage d'application.
Ressources Internet du Support technique personnalisé	`Windows`	Tableau contenant les informations de contact que les utilisateurs peuvent utiliser pour contacter l'Assistance technique en cas de dysfonctionnement de Kaspersky Endpoint Security. Vous pouvez également configurer des modèles de messages pour les utilisateurs avec des instructions sur la façon d'obtenir de l'aide. Par défaut, l'application affiche les liens vers le site Internet de Kaspersky.

Rapports et stockage

pour Windows, macOS et Linux

Cette section permet de gérer les paramètres de création et de conservation des rapports sur les événements rencontrés par Kaspersky Endpoint Security, ainsi que de configurer le stockage des objets dans la Sauvegarde et la Quarantaine.

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*.

`Windows` Les rapports se trouvent dans le dossier `C:\ProgramData\Kaspersky Lab\KES.12.4.0\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 :

- `Windows` : `C:\ProgramData\Kaspersky Lab\KES.12.4.0\QB`
- `Linux` : `/var/opt/kaspersky/kesl/common/objects-backup/`

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.

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 chiffrés et ne menacent pas la sécurité de l'appareil.

Paramètres des rapports et du stockage

Paramètres	SE	Description
Supprimer les rapports après (jours)	`Windows` `macOS`	Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle renseigné. 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)	`Windows`	Si la case est cochée, la taille maximale du fichier de rapport est limitée par la valeur renseignée. 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.
Conserver uniquement les événements récents	`macOS`	Si cette case est cochée, Kaspersky Endpoint Security supprime, à chaque démarrage de la tâche, les informations relatives aux événements non critiques survenus depuis le démarrage précédent de la tâche, mais conserve les notes importantes dans le rapport (par exemple, les informations relatives aux objets malveillants détectés).
Consigner les événements non critiques	`macOS`	Si cette case est cochée, Kaspersky Endpoint Security consigne les événements non critiques (par exemple, les événements informatifs) dans le rapport. Les événements non critiques n'ont aucune incidence sur la protection.
Supprimer les objets après (jours)	`Windows` `macOS` `Linux`	Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. 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)	`Windows` `Linux`	Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. 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	`Windows` `Linux`	**Taille maximale de la Quarantaine (Mo)**. Si la case est cochée, la taille maximale de la Quarantaine est limitée par la valeur renseignée. Lorsque la Quarantaine atteint sa taille maximale, Kaspersky Endpoint Security envoie l'événement *Espace insuffisant dans la Quarantaine* à Kaspersky Security Center et crée un événement dans le journal des événements du système d'exploitation. 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, l'application envoie l'événement correspondant à Kaspersky Security Center et l'enregistre. Pendant ce temps, l'application continue de mettre en quarantaine les nouveaux objets.

Intégration avec KSC

Cette section décrit comment configurer l'intégration de Kaspersky Endpoint Security avec Kaspersky Security Center.

Paramètres d'intégration de Kaspersky Security Center

Paramètres	SE	Description
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation	`Windows` `macOS` `Linux`	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. Cela est nécessaire lors de l'activation de l'application dans un segment isolé du réseau sans accès à Internet à l'aide d'un code d'activation. Si vous activez l'application à l'aide d'un fichier clé, vous ne devez pas disposer d'un accès à Internet. Non applicable si l'application est utilisée en mode Light Agent.
Transfert des données au Serveur d'administration	`Windows` `macOS` `Linux`	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 : • `Windows` **À propos d'une chaîne de développement de menaces**. • `Windows` `macOS` `Linux` **À propos des fichiers de la Quarantaine**. • `Windows` `Linux` **À propos des fichiers de la Sauvegarde**. • `Windows` `Linux` **À propos des fichiers non traités**. • `Windows` `macOS` `Linux` **À propos des appareils installés**. • `Windows` `Linux` **À propos des applications exécutables**. • `Windows` **À propos des erreurs de chiffrement des fichiers**. • `Windows` **Rapport sur l'état des règles du Contrôle évolutif des anomalies**. • `Windows` **Rapport sur les déclenchements des règles du Contrôle évolutif des anomalies**.

Paramètres d'interaction avec le système d'exploitation

pour Linux

Pour fonctionner correctement, l'application doit utiliser l'interception des événements système – opérations sur les fichiers et lancements de processus. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit.

Paramètres d'interaction avec le système d'exploitation

Paramètres	SE	Description
Mécanisme d'interception	`Linux`	Le mécanisme d'interception des événements système utilisé par l'application dans son travail : • **Technologie fanotify**. Si cette option est sélectionnée, l'application utilise la technologie fanotify pour l'interception des événements système. • **Module de noyau mis à jour**. Si cette option est sélectionnée, l'application utilise le module de noyau mis à jour pour l'interception des événements système.
Si le module de noyau mis à jour ne parvient pas à démarrer	`Linux`	Action effectuée par l'application si le module de noyau mis à jour ne parvient pas à démarrer : • **Utiliser la technologie fanotify**. Si cette option est sélectionnée, l'application passe à la technologie fanotify pour l'interception des événements système. • **Désactiver l'interception des événements système (niveau de protection inférieur)**. Si l'application n'utilise pas l'interception des événements système, l'analyse des fichiers en temps réel n'est pas effectuée, et le niveau de protection de l'appareil est réduit. Ce paramètre est disponible si le mécanisme d'interception **Module de noyau mis à jour** est sélectionné.
Source de télémétrie	`Linux`	La source que Kaspersky Endpoint Security utilise pour la collecte des données télémétriques : • **Utiliser uniquement eBPF**. Seule la technologie eBPF est utilisée. • **Par défaut**. La technologie eBPF et le service auditd sont utilisés.
Mode de fonctionnement pour auditd	`Linux`	Dans ce mode, le service auditd enregistre les événements d'audit pour les transmettre ensuite aux solutions de Detection and Response : • **Exclusif**. Si cette option est sélectionnée, Kaspersky Endpoint Security utilise exclusivement le service auditd. Les applications tierces ne peuvent pas se connecter au flux d'audit. • **Non exclusif**. Si cette option est sélectionnée, le service auditd peut accepter plusieurs connexions provenant de différents processus qui utilisent l'audit système.

Paramètres des événements

pour Windows, macOS et Linux

Cette section vous permet de configurer les notifications relatives aux événements sur les appareils gérés et aux événements généraux. Les notifications peuvent être envoyées aux adresses email des utilisateurs de cet espace de travail.

Différents *événements* se produisent pendant le fonctionnement de l'application. Ils peuvent avoir un caractère informatif ou revêtir une importance plus grande. Par exemple, l'application peut utiliser un événement pour signaler une mise à jour réussie de la base de données ou signaler une erreur d'un module qui doit être corrigée.

Les événements de Kaspersky Endpoint Security peuvent être classés selon les niveaux de gravité suivants :

- *Événements critiques* constituent une menace sérieuse pour la sécurité de l'ordinateur (détection d'objets malveillants, vulnérabilités, problèmes liés à Kaspersky Endpoint Security). Un événement critique nécessite votre attention immédiate. Il est recommandé de ne pas désactiver les notifications concernant les événements critiques.

- *Erreurs de fonctionnement* sont des événements qui surviennent à la suite d'un dysfonctionnement de Kaspersky Endpoint Security (erreur de traitement, erreur de configuration des tâches). De tels événements ne menacent pas directement la sécurité de l'ordinateur, mais ils requièrent votre intervention afin d'assurer que Kaspersky Endpoint Security fonctionne correctement et protège vos appareils.

- *Avertissements* ne requièrent pas d'action immédiate de votre part, mais peuvent être le signe de menaces futures pour la sécurité de l'ordinateur.

- *Messages d'information*.

Que les notifications soient activées ou désactivées, Kaspersky Endpoint Security enregistre les informations relatives à tous les événements liés aux applications dans les rapports sur les applications.

Pour chaque événement de Kaspersky Endpoint Security, vous pouvez configurer la façon dont vous souhaitez recevoir les notifications :

- `Windows` **Notifier par email**.

- `Windows` **Enregistrer dans le rapport local**.

- `Windows` `macOS` **Notifier à l'écran**.

- `Windows` `Linux` **Enregistrer dans le journal des événements système**.

Paramètres de la télémétrie

pour Windows, macOS et Linux

Cette section vous permet de configurer l'envoi de la télémétrie des appareils administrés vers les serveurs de collecte de données télémétriques. *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 ou 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.

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.

Vous pouvez administrer les paramètres de synchronisation pour chaque agent intégré dans la section "Agents intégrés" et sélectionner des valeurs optimales en fonction de la charge de votre réseau.

Cette section permet de configurer ce qui suit :

- Règles d'inclusion et d'exclusion de la télémétrie.
- Collecte des données télémétriques à envoyer aux serveurs KATA, aux serveurs de collecte de données télémétriques ou aux serveurs de réponse.

Télémétrie EDR Expert (on-premise)

pour Windows, macOS et Linux

Paramètres de la télémétrie EDR Expert (on-premise)

Paramètres	SE	Description
Télémétrie EDR Expert (on-premise)	`Windows` `macOS` `Linux`	**Importer** et **Exporter**. Vous pouvez exporter les paramètres de la télémétrie EDR Expert (on-premise) 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 fonctionnalités des événements envoyés ou pour migrer la liste vers une autre stratégie.
Exclusions générales	`Windows` `macOS` `Linux`	Pour optimiser les données transmises, vous pouvez configurer des règles d'exclusion pour certains types d'événements. Kaspersky Endpoint Security ne collecte pas de données télémétriques relevant d'une telle règle. Cela vous permet de réduire le trafic et d'éviter de traiter des événements provenant d'objets et de processus de confiance. **Nom de la règle**. **Action** : • **Ne pas collecter**. Si vous sélectionnez cette option, Kaspersky Endpoint Security ne collecte pas les données télémétriques qui satisfont aux conditions de la règle. • **Exclure l'IOA**. Si vous sélectionnez cette option, Kaspersky Endpoint Security ne collecte pas les données télémétriques suite au déclenchement d'une règle IOA. *Indicateur d'attaque (IOA)* est une règle qui contient une description du comportement suspect dans le système qui peut indiquer une attaque ciblée. **Condition**. Condition de déclenchement de la règle. Spécifiez un paramètre de télémétrie, un opérateur conditionnel et la valeur du paramètre. Par défaut, Kaspersky Endpoint Security associe les critères de déclenchement de la règle à un ET logique. Vous pouvez ajouter plusieurs conditions ou groupes de conditions en utilisant les opérateurs logiques ET et OU.
Tous les types d'événements	`Windows` `macOS` `Linux`	Liste des types d'événements pour lesquels la collecte de télémétrie est définie par défaut par Kaspersky. Vous pouvez activer ou désactiver manuellement la télémétrie pour chaque type d'événement et configurer des règles d'exclusion et d'inclusion de la télémétrie.

Télémétrie EDR (KATA) / NDR (KATA)

pour Windows et Linux

Pour améliorer les performances et optimiser la transmission des données vers le serveur de collecte de données télémétriques, vous pouvez configurer des exclusions de télémétrie. Par exemple, vous pouvez choisir de ne pas envoyer les données de communication réseau pour certaines applications.

Paramètres	SE	Description
Processus exclus	`Windows` `Linux`	Kaspersky Endpoint Security ne traite pas les données relatives aux processus à partir de la liste. **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**. • `Windows` **Requête WMI**. • **Canal**. • **LDAP**. • `Windows` **AMSI**.
Communications des réseaux exclus	`Windows` `Linux`	Kaspersky Endpoint Security ne traite pas les données relatives aux communications réseau à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **Nom de la règle**. **Direction**. **Protocole**. **Socket raw**. **Numéro de protocole**. **Adresse locale**. L'adresse réseau de l'ordinateur pour lequel Kaspersky Endpoint Security exclut la télémétrie du trafic réseau. **Port local ou plage**. **Adresse distante**. L'adresse réseau de l'ordinateur pour lequel Kaspersky Endpoint Security exclut la télémétrie du trafic réseau. **Port distant ou plage**. Seul le format IPv4 est pris en charge pour les adresses IP. **Appliquer la règle pour les applications sélectionnées**. Si cette case est cochée, Kaspersky Endpoint Security exclut la télémétrie EDR du trafic réseau pour les fichiers exécutables des applications de la liste.

Paramètres	SE	Description
Opérations sur les fichiers exclus	`Windows` `Linux`	Kaspersky Endpoint Security ne traite pas les opérations sur les fichiers à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **Nom de la règle**. **Nom du fichier ou masque**. Nom du fichier ou masque auquel Kaspersky Endpoint Security applique la règle d'exclusion lors de l'accès au fichier. Kaspersky Endpoint Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque. **Sélectionnez l'opération sur le fichier**. Type d'opération sur le fichier auquel la règle s'applique. **Chemin d'accès 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.

Paramètres	SE	Description
Opérations DNS exclues	`Windows` `Linux`	Kaspersky Endpoint Security ne traite pas les opérations DNS à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Opération DNS** : • **Adresse IP du serveur DNS**. • **Options de requête**. • **État**. • **Nom de domaine**. • **Identifiant du type de paramètres**. • **Données de réponse**. Contenu de la réponse DNS à la requête.

Paramètres	SE	Description
Opérations LDAP exclues	`Windows`	Kaspersky Endpoint Security ne traite pas les opérations LDAP à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Opération LDAP** : • **Zone de recherche LDAP**. Zone de recherche LDAP. Peut présenter l'une des valeurs suivantes : ADS_SCOPE_BASE, ADS_SCOPE_ONELEVEL ou ADS_SCOPE_SUBTREE. • **Filtre**. • **Nom unique pour la recherche d'objets LDAP**. Nom de l'enregistrement dans l'annuaire LDAP. • **Attributs d'objets utilisés pour la recherche d'opérations LDAP**. Attributs définis dans la requête comme valeurs de retour.

Paramètres	SE	Description
Requêtes d'accès exclues au processus	`Windows`	Kaspersky Endpoint Security ne traite pas les demandes d'accès aux processus à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **Nom de la règle**. 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. • **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. **Requêtes d'accès au processus** : • **Type d'opération**. • **Accès demandé au processus**. • **Trace de la pile d'exécution**.

Paramètres	SE	Description
Injections de code exclues	`Windows`	Kaspersky Endpoint Security ne traite pas les injections de code à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Injections de code** : • **Méthode d'accès**. • **Pile d'exécution**. Pile d'appels de l'API au moment de l'interception de la fonctionnalité liée à l'injection de code • **Ligne de commande modifiée**. • **Adresse d'injection**. Adresse située dans l'espace d'adressage du processus cible où le code exécuté à distance a été injecté. Ce champ est laissé vide si l'injection de code a été réussie à l'aide des méthodes SET_WINDOWS_HOOK et ARG_SPOOFING. • **Ligne de commande modifiée**. • **Nom DLL injecté**. Nom de la DLL contenant la routine d'interception et nom de la fonctionnalité à laquelle le contrôle est transmis après l'injection. Ce champ est rempli si l'injection de code a été réalisée à l'aide de la méthode SET_WINDOWS_HOOK. • **Chemin d'accès DLL injecté**. Chemin d'accès à la DLL contenant la routine d'interception. Ce champ est rempli si l'injection de code a été réalisée à l'aide de la méthode SET_WINDOWS_HOOK.

Paramètres	SE	Description
Requêtes WMI exclues	`Windows`	Kaspersky Endpoint Security ne traite pas les requêtes WMI à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Requêtes WMI** : • **Type d'opération 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 de l'événement WMI créé**. • **Code source d'un consommateur d'événements WMI**.

Paramètres	SE	Description
Opérations sur les canaux exclues	`Windows`	Kaspersky Endpoint Security ne traite pas les opérations sur les canaux à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Opérations sur les canaux** : • **Nom du canal**. • **Type d'opération**.

Paramètres	SE	Description
Modifications exclues du registre	`Windows`	Kaspersky Endpoint Security ne traite pas les modifications du registre à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **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. **Modifications du registre** : • **Type d'opération**. • **Emplacement**. Chemin d'accès à la clé de registre dans laquelle la modification a été effectuée. • **Nom de la valeur**. Nom de la valeur modifiée, par exemple, RegistrySizeLimit. • **Valeur**. • **Nom complet d'un fichier de registre**.
Opérations exclues avec les appareils	`Windows`	Kaspersky Endpoint Security ne traite pas les opérations liées aux appareils USB à partir de la liste. Dans la règle d'exclusion, vous pouvez définir les paramètres suivants : **Nom de la règle**. **Type d'appareil**. **Identifiant d'appareil**. **Nom de l'appareil**.

Télémétrie KUMA

pour Windows

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*. Vous pouvez également spécifier le journal d'une application tierce. Pour améliorer les performances et optimiser la transmission des données vers le serveur KUMA, vous pouvez ajouter manuellement des journaux d'événements individuels.

Paramètres de la télémétrie KUMA

Paramètres	SE	Description
Journaux d'événements Windows	`Windows`	Événements des journaux Windows que l'application envoie à KUMA. Vous pouvez ajouter les journaux un par un manuellement ou importer un fichier JSON avec des paramètres. Pour chaque journal des événements, vous pouvez sélectionner la manière dont vous souhaitez qu'il soit envoyé : • **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. Vous pouvez également configurer des 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. Lorsque vous spécifiez plusieurs identifiants d'événement, utilisez des virgules comme délimiteurs.

Agents intégrés

Managed Detection and Response

pour Windows, macOS et Linux

Kaspersky Endpoint Security 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.

Vous devez activer les modules suivants pour que Managed Detection and Response puisse fonctionner :

- Kaspersky Security Network (mode élargi)
- Détection comportementale

L'activation de ces modules est obligatoire. Dans le cas contraire, Kaspersky Managed Detection and Response ne peut pas fonctionner, car il ne reçoit pas les données télémétriques exigées.

Paramètres du module Managed Detection and Response

Paramètres	SE	Description

Fichier de configuration MDR	`Windows`
	`macOS`
	`Linux`
		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 Optimum

pour Windows, macOS et Linux

Kaspersky Endpoint Security inclut un agent intégré pour la solution Kaspersky Endpoint Detection and Response Optimum (ci-après également "EDR Optimum"). *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.

Kaspersky Endpoint Detection and Response analyse les activités potentiellement dangereuses sur les appareils des utilisateurs et fournit aux *responsables de la sécurité* ou à l'*administrateur* des informations au sujet d'une attaque possible afin de prendre des mesures de réponse en temps opportun ou d'appliquer automatiquement les mesures de réponse configurées.

Vous devez activer les modules suivants pour que Endpoint Detection and Response puisse fonctionner :

- 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 liste des modules peut varier selon les plateformes.

Paramètres du module Endpoint Detection and Response

Paramètres	SE	Description
Activer la journalisation avancée de l'activité du système	`Windows` `macOS` `Linux`	Ce paramètre permet de garantir l'exactitude de la tâche **Analyse IOC rétrospective**. Il est associé à une utilisation importante des ressources informatiques.
Isolement du réseau	`Windows` `macOS` `Linux`	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. • connexions initiées par les services de Kaspersky Endpoint Security ; • connexions initiées par l'Agent d'administration de Kaspersky Security Center ;
Déverrouiller automatiquement l'appareil isolé dans (heures)	`Windows` `macOS` `Linux`	L'isolation du réseau peut être désactivée automatiquement après un certain temps ou manuellement.

Paramètres	SE	Description
Exclusions d'isolement du réseau	`Windows` `macOS` `Linux`	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	`Windows` `macOS` `Linux`	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.
Action sur l'exécution ou l'ouverture d'un objet interdit	`Windows` `macOS` `Linux`	**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 système et dans 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 système 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	`Windows` `macOS` `Linux`	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.
Utiliser un emplacement sensible à la casse	`Linux`	Si cette case est cochée, l'application traitera la création de règles comme étant sensible à la casse lors de la création de règles de prévention de l'exécution.
Cloud Sandbox	`Windows` `macOS` `Linux`	*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 détecter les activités malveillantes et prend des décisions concernant la réputation de ces fichiers. 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. Une connexion KSN est nécessaire pour obtenir des informations sur les objets analysés.

Endpoint Detection and Response Expert (on-premises)

pour Windows, macOS et Linux

Endpoint Detection and Response Expert version 7.1 ou version antérieure

Kaspersky Endpoint Security prend en charge le module Kaspersky Endpoint Detection and Response Expert (versions 7.1 et antérieures, ci-après "EDR (KATA)") dans le cadre 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.

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.

Endpoint Detection and Response Expert version 8.0 ou version ultérieure

Kaspersky Endpoint Security prend en charge les solutions Kaspersky de la classe Endpoint Detection and Response Expert (version 8.0 et ultérieures, ci-après également dénommées « EDR Expert (on-premise) »). De telles solutions incluent, par exemple, Kaspersky Symphony XDR. *Endpoint Detection and Response Expert (on-premise)* est une solution de cybersécurité d'entreprise 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.

EDR Expert (on-premise) examine les journaux et les données télémétriques reçus de l'infrastructure de l'entreprise afin de 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-premise), y compris les événements provenant des applications Kaspersky et des produits tiers de sécurité informatique.

Modules requis par Endpoint Detection and Response Expert

Vous devez activer les modules suivants pour que Endpoint Detection and Response Expert puisse fonctionner :

- 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

La liste des modules peut varier selon les plateformes.

Paramètres du module Endpoint Detection and Response Expert (on-premise)

Paramètres	SE	Description
Solution Endpoint Detection and Response Expert	`Windows` `macOS` `Linux`	Des solutions Endpoint Detection and Response Expert auxquelles Kaspersky Endpoint Security peut s'intégrer. • **Endpoint Detection and Response Expert (version 7.1 ou version antérieure)**. • **Endpoint Detection and Response Expert (version 8.0 ou version ultérieure)**.
Paramètres de connexion	`Windows` `macOS` `Linux`	Gérez les paramètres de connexion suivants au serveur KATA ou au serveur de collecte de données télémétriques : • **Délai d'attente de la connexion avec le serveur**. 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.
Envoyer une demande de synchronisation au serveur toutes les (min.) *(disponible uniquement pour Endpoint Detection and Response Expert version 7.1 ou version antérieure)*	`Windows` `macOS` `Linux`	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.

Paramètres	SE	Description
Connexion aux serveurs KATA/Connexion aux serveurs de collecte de données télémétriques	`Windows` `macOS` `Linux`	Saisissez l'adresse IP (IPv4 ou IPv6) et le port de connexion au serveur Kaspersky Anti Targeted Attack Platform ou au serveur de collecte de données télémétriques. Vous pouvez ajouter plusieurs adresses pour le serveur Central Node (KATA) ou pour le 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. Les solutions EDR (KATA) et EDR Expert (on-premise) présentent des architectures différentes. Pour traiter les données télémétriques, EDR Expert (on-premise) utilise un serveur de collecte de données télémétriques, tandis qu'EDR (KATA) utilise un serveur Central Node. Par conséquent, si vous intégrez l'application à EDR Expert (on-premise), vous devez ajouter un serveur de collecte de données télémétriques.
Envoyer la télémétrie à KATA/Envoyer les données télémétriques aux serveurs de collecte de données télémétriques	`Windows` `macOS` `Linux`	Cette fonction permet d'interdire complètement l'envoi des données télémétriques sur le serveur KATA ou sur le serveur de collecte de télémétrie selon la solution choisie. 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 *(disponible uniquement pour Endpoint Detection and Response Expert version 8.0 ou version ultérieure)*	`Windows` `Linux`	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.)	`Windows` `macOS` `Linux`	L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation.
Nombre maximal de paquets d'événements	`Windows`	L'application se synchronise avec le serveur lorsque la mémoire tampon est remplie d'événements.
Activer la limitation des demandes	`Windows` `macOS` `Linux`	Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. 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. 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.
Connexion aux serveurs de réponse *(disponible uniquement pour Endpoint Detection and Response Expert version 8.0 ou version ultérieure)*	`Windows` `macOS` `Linux`	Connexion aux paramètres des serveurs de réponse. Indiquez l'adresse IP du serveur de réponse (IPv4 ou 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.

Paramètres	SE	Description

Paramètres de connexion
(disponible uniquement pour Endpoint Detection and Response Expert version 8.0 ou version ultérieure)
	`Windows`
	`macOS`
	`Linux`
		Configurez les éléments suivants pour la connexion au serveur de réponse :
		• **Délai d'attente de la connexion avec le serveur**. Délai maximal de réponse du serveur de réponse. À l'expiration du délai, Kaspersky Endpoint Security essaie de se connecter à un autre serveur de réponse.
		• **Certificat de serveur**. Certificat TLS permettant d'établir une connexion sécurisée avec le serveur de réponse.
		• **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et le serveur de réponse. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres du serveur de réponse, 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 serveur de réponse, 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.

Network Detection and Response (KATA)

pour Windows et Linux

Kaspersky Endpoint Security 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.

Les modules suivants doivent être activés pour que Network Detection and Response (KATA) fonctionne :

- 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

La liste des modules peut varier selon les plateformes.

Paramètres du module Network Detection and Response (KATA)

Paramètres	SE	Description
Paramètres de connexion aux serveurs KATA	`Windows` `Linux`	**Délai d'attente de la connexion avec le serveur**. 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.
Connexion aux serveurs KATA	`Windows` `Linux`	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 KATA toutes les (min.)	`Windows` `Linux`	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.)	`Windows` `Linux`	L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation.

Paramètres	SE	Description
Activer la limitation des demandes	`Windows` `Linux`	Cette fonctionnalité permet d'optimiser la charge exercée sur l'ordinateur. Si cette fonctionnalité est activée, l'application limite le nombre d'événements transmis. 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. 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.

Sandbox

pour Windows et Linux

Kaspersky Endpoint Security prend en charge l'intégration avec la solution Kaspersky Sandbox et le module Sandbox dans le cadre de la solution Kaspersky Anti Targeted Attack Platform. 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.

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.

Paramètres du module Sandbox

Paramètres	SE	Description
Mode d'intégration	`Windows` `Linux`	**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**. L'application envoie automatiquement les objets à analyser vers la Sandbox. Si nécessaire, l'utilisateur peut également soumettre des fichiers individuels pour analyse à partir du menu contextuel.
Connexion aux serveurs Sandbox	`Windows` `Linux`	**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. Indiquez l'adresse IP du serveur Sandbox (IPv4, Ipv6 ou DNS) et le port de connexion au serveur. **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. Indiquez l'adresse IP du serveur Central Node (IPv4, IPv6 ou DNS) et le port de connexion au serveur.

Paramètres	SE	Description
Paramètres de connexion au serveur	`Windows` `Linux`	**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. **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.
Action en cas de détection d'une menace	`Windows` `Linux`	**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 un objet, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où vous auriez besoin ultérieurement de restaurer l'objet. 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 *Critical Areas Scan*. Par défaut, Kaspersky Endpoint Security vérifie la mémoire du noyau, les processus en cours d'exécution et les secteurs de démarrage. **Créer la tâche Analyse IOC**. Si cette option est sélectionnée, Kaspersky Endpoint Security crée automatiquement la tâche *IOC Scan (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 *IOC Scan*, accédez aux paramètres de la tâche.
Zone de l'analyse IOC	`Windows` `Linux`	**Zones de fichiers critiques**. Si cette option est sélectionnée, Kaspersky Endpoint Security recherche les IOC uniquement dans les zones de fichiers importantes de l'ordinateur, comme les répertoires de profils utilisateur sélectionnés et les objets système critiques. **Zones de fichiers sur les disques système de l'ordinateur**. Si cette option est sélectionnée, Kaspersky Endpoint Security effectue une analyse IOC sur le disque système de l'ordinateur. L'application recherche également les IOC dans le chemin d'accès au fichier où la menace a été détectée, quelle que soit la zone d'analyse sélectionnée.
Exécuter la tâche Analyse IOC	`Windows` `Linux`	**Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer la tâche *IOC Scan* manuellement à tout moment. **Automatiquement**. Mode d'exécution dans lequel Kaspersky Endpoint Security exécute automatiquement la tâche *Analyse IOC* dès qu'une menace est détectée. `Windows` **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.

Intégration avec KUMA

pour Windows et Linux

Kaspersky Endpoint Security 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).

Par défaut, l'envoi d'événements au serveur KUMA est désactivé. Pour garantir le bon fonctionnement de KUMA, activez d'abord l'envoi de données télémétriques vers KUMA dans la section Paramètres généraux → Paramètres de la télémétrie.

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.

Paramètres du module KUMA

Paramètres	SE	Description
Paramètres de connexion au serveur	`Windows` `Linux`	**Délai d'attente de la connexion avec le serveur**. Délai maximal de réponse du serveur KUMA. 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 (voir les instructions dans Kaspersky Unified Monitoring and Analysis Platform). **Utiliser l'authentification bidirectionnelle**. Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Endpoint Security et KUMA. Pour utiliser l'authentification bidirectionnelle, dans la console KUMA, dans les paramètres du connecteur tcp, vous devez sélectionner le **Custom PFX** mode TLS (cf. aide de Kaspersky Unified Monitoring and Analysis Platform). Ensuite, vous devez obtenir un cryptoconteneur et définir un mot de passe pour le protéger. Un *conteneur crypto* est une archive PFX contenant un certificat et une clé privée. Après avoir configuré les paramètres KUMA, vous devez également activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Endpoint Security et charger un cryptoconteneur 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.
Durée d'attente maximale pour l'envoi des événements (sec)	`Windows` `Linux`	L'application se synchronise avec le serveur pour envoyer des événements après l'expiration de l'intervalle de synchronisation.
Utiliser le chiffrement TLS	`Windows` `Linux`	Si cette fonctionnalité est activée, Kaspersky Endpoint Security utilise un certificat TLS pour établir une connexion de confiance avec le serveur KUMA.
Connexion aux serveurs KUMA	`Windows` `Linux`	Paramètres de connexion au serveur KUMA. Spécifiez l'adresse IP (IPv4 ou IPv6), le protocole de connexion et le port pour la connexion au serveur. Vous pouvez ajouter plusieurs adresses de serveur KUMA. 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.

Mode Light Agent

Paramètres de détection des SVM

pour Windows et Linux

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 les fragments des fichiers qui doivent être analysés à la SVM. Les résultats de l'analyse sont disponibles pour toutes les machines virtuelles sur lesquelles le Light Agent est installé (la technologie SharedCache). Ainsi, la technologie SharedCache 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 module Serveur d'intégration est conçu pour assurer l'interaction entre les modules de la solution et l'infrastructure virtuelle. 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.

Paramètres de détection des SVM

Paramètres	SE	Description
Utiliser le Serveur d'intégration	`Windows` `Linux`	Le Serveur d'intégration est utile dans les infrastructures virtuelles à grande échelle, car le Serveur d'intégration répartit automatiquement la charge entre les SVM. Indiquez les des paramètres de connexion au Serveur d'intégration : • L'adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel est installé le Serveur d'intégration. • Numéro de port pour la connexion au Serveur d'intégration. Le numéro de port par défaut est 7271. • Mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte administrateur).
Utiliser la liste d'adresses des SVM définie manuellement	`Windows` `Linux`	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. Vous pouvez saisir plusieurs adresses IP ou noms de domaine complets de SVM à l'aide d'un retour à la ligne. 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.

Paramètres de connexion au Serveur d'intégration

pour Windows et Linux

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. Le Serveur d'intégration tient à jour une liste de SVM auxquelles il est possible de se connecter. Le Light Agent établit une connexion avec le Serveur d'intégration et obtient la liste des adresses des SVM.

Le Serveur d'intégration est utile dans les infrastructures virtuelles à grande échelle, car le Serveur d'intégration répartit automatiquement la charge entre les SVM. Le Serveur d'intégration obtient les informations sur les SVM disponibles, les analyse et fournit aux Light Agents une liste des Serveurs de protection (SVM) optimaux pour la connexion.

Paramètres de connexion au Serveur d'intégration

Paramètres	SE	Description
Adresse	`Windows` `Linux`	Adresse IP au format IPv4 ou nom de domaine complet (FQDN) du Serveur d'intégration. Si l'adresse est indiquée sous la forme d'un nom NetBIOS, localhost ou 127.0.0.1, la connexion au Serveur d'intégration échoue et génère une erreur.
Port	`Windows` `Linux`	Numéro de port pour la connexion au Serveur d'intégration. Le numéro de port par défaut est 7271.
Authentification sur le Serveur d'intégration	`Windows` `Linux`	Mot de passe de l'administrateur du Serveur d'intégration (mot de passe du compte `admin`). Après la connexion au Serveur d'intégration avec des droits d'administrateur, la stratégie reçoit automatiquement le mot de passe de l'`agent` utilisé pour connecter les Light Agents au Serveur d'intégration.

Tag de connexion à la SVM

pour Windows et Linux

Plusieurs Light Agents peuvent se connecter à une SVM. Pour équilibrer les connexions du Light Agent, vous pouvez spécifier une liste distincte de SVM dans la section des paramètres de détection des 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.

Cochez la case **Utiliser le tag de connexion** pour connecter les Light Agents aux SVM à l'aide de tags. Saisissez le 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 `;`.

Algorithme de sélection des SVM

pour Windows et Linux

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.

Paramètres de l'algorithme de sélection des SVM

Paramètres	SE	Description
Utiliser l'algorithme standard de sélection des SVM	`Windows` `Linux`	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. Pour identifier une SVM comme locale, le Light Agent utilise principalement l'emplacement de la SVM dans l'infrastructure virtuelle. Si les SVM se trouvent dans le même hyperviseur que le Light Agent, le Light Agent considère ces SVM comme locales. Dans certaines infrastructures virtuelles, vous devez spécifier manuellement les SVM locales à l'aide d'un fichier de configuration. 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.
Utiliser l'algorithme étendu de sélection des SVM	`Windows` `Linux`	L'algorithme étendu vous permet de spécifier manuellement les critères de sélection de la SVM locale ou de désactiver la recherche de la SVM locale. Pour ce faire, il convient de sélectionner le chemin d'accès à la SVM dans l'infrastructure virtuelle : Hyperviseur, Cluster ou Centre de données. Autrement dit, vous devez sélectionner la zone dans laquelle la SVM locale doit être recherchée. Si le Light Agent ne peut pas se connecter à une SVM locale dans la zone de recherche configurée, il met un terme à ses tentatives de connexion. L'algorithme étendu permet également de désactiver la recherche des SVM locales pour le Light Agent. Dans ce cas, le Light Agent sélectionne les SVM avec le moins de Light Agents connectés dans toute l'infrastructure virtuelle.

Protection de la connexion

pour Windows et Linux

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 d'un chiffrement peut influencer les performances de Kaspersky Security for Virtualization Light Agent.

Annexe 6. Paramètres d'interaction avec les services externes

Kaspersky Endpoint Security utilise les paramètres réseau et de chiffrement suivants pour communiquer avec les services externes.

Adresse réseau du service et protocole	Description
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocole : HTTPS Port : 443	Activation de l'application.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
Protocole : HTTPS
Port : 443
	Mise à jour des bases et des modules de l'application.

Adresse réseau du service et protocole	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 Protocole : HTTP Port : 80	Mise à jour des bases et des modules de l'application.
downloads.upd.kaspersky.com Protocole : HTTPS Port : 443	• Mise à jour des bases et des modules de l'application. • Vérification de l'accès aux serveurs de Kaspersky. Si l'accès aux serveurs via le DNS système échoue, l'application utilisera le DNS public. Ceci est nécessaire pour la mise à jour des bases de l'application et maintenir le niveau de sécurité de l'appareil. L'application utilisera les DNS publics suivants par ordre d'apparition : 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 demandes de l'application peuvent contenir des adresses de domaine et l'adresse IP externe de l'utilisateur, car l'application établit une connexion TCP/UDP avec le serveur DNS. Ces données sont nécessaires, par exemple, pour l'analyse du certificat d'une ressource Internet lors de l'accès via HTTPS. Si l'application utilise un serveur DNS public, les règles de traitement des données sont régies par la Politique de confidentialité de ce service.
ds.kaspersky.com Protocole : HTTPS Port : 443	Utilisation de Kaspersky Security Network.

Adresse réseau du service et protocole	Description

`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-cinfo-geo.kaspersky-labs.com`
Protocole : `KSN`
Port : `443`, `1443`
	Utilisation de Kaspersky Security Network.

`click.kaspersky.com` Protocole : `HTTPS` Port : `443`	Suivez les liens depuis l'interface.

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocole : `HTTP`
Port : `80`
	Infrastructure à clés publiques (ICP).
	Ces serveurs (crl.kaspersky.com) font partie de l'infrastructure à clé publique (PKI) et sont nécessaires pour vérifier la validité des certificats de signature numérique de Kaspersky. Le serveur CRL fournit une liste des certificats révoqués. Le service OCSP vous permet de consulter en temps réel l'état d'un certificat spécifique. Le fonctionnement de ces modules garantit la sécurité des interactions avec les certificats numériques et la protection contre les attaques potentielles.

Interopérabilité avec les solutions Kaspersky

L'application Kaspersky Endpoint Security prend en charge l'interopérabilité avec certaines solutions Kaspersky. Pour une interopérabilité optimale des applications, suivez les recommandations de cette section.

Kaspersky Security Center Linux

Lors de l'utilisation de Kaspersky Endpoint Security for Linux avec Kaspersky Security Center Linux, nous vous recommandons d'utiliser les paramètres décrits dans cet article.

Paramètres recommandés

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent` • `/var/lib/postgresql/<PostgreSQL version>`
Analyse des logiciels malveillants	Enabled	
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces réseau	Enabled	Sélectionner le mode d'interception du trafic réseau eBPF `NetInterceptorMode=UseEBPF`
Protection contre les menaces Internet	Enabled	Utiliser les paramètres par défaut.
Protection contre le chiffrement	Désactivé	–

Module de l'application	État recommandé du module	Recommandations
Analyser les conteneurs	Désactivé	–
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Enabled	Ajouter des zones d'analyse : • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
Vérification de l'intégrité du système	Désactivé	–
Endpoint Detection and Response Expert (on-premises)	Enabled	Utiliser les paramètres par défaut.
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Enabled	Utiliser les paramètres par défaut.
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Certaines restrictions s'appliquent	Pour les actions de réponse, vous ne pouvez pas exclure les objets requis par Kaspersky Endpoint Security for Linux, ni les objets système critiques. Lorsque vous lancez des actions de réponse, assurez-vous qu'elles ne perturbent pas le système et les applications que vous utilisez.
Interface graphique	Non défini	–
plug-in Internet d'administration de Kaspersky Endpoint Security for Linux	Installée	Utiliser les paramètres par défaut.
plug-in MMC d'administration de Kaspersky Endpoint Security for Linux	Installée	Utiliser les paramètres par défaut.
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Enabled	Utiliser les paramètres par défaut.
Protection BadUSB	Désactivé	–

Module de l'application	État recommandé du module	Recommandations
Exclusions globales	Configuré	Si vous installez Kaspersky Security Center à l'aide du script d'installation rapide, ajoutez les points de montage aux exclusions : `/var/lib/postgresql/<PostgreSQL version>/main` où `<PostgreSQL version>` est le numéro de la version du SGBD PostgreSQL que vous utilisez.

Network Detection and Response (KATA)

Lorsque vous utilisez Kaspersky Endpoint Security for Linux avec Network Detection and Response (KATA), nous vous recommandons d'utiliser les paramètres décrits dans cet article.

Consultez également la documentation de la solution Kaspersky Anti Targeted Attack (KATA) Platform.

Paramètres de Kaspersky Endpoint Security for Linux sur les serveurs avec le module Sensor

Paramètres recommandés pour les serveurs Sensor

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
Analyse des logiciels malveillants	Désactivé	–
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces réseau	Désactivé	–
Protection contre les menaces Internet	Désactivé	–
Protection contre le chiffrement	Désactivé	–
Analyser les conteneurs	Enabled	Activez la Surveillance des conteneurs pour analyser les conteneurs et les espaces de noms en cours d'exécution en temps réel `NamespaceMonitoring=Yes`
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–

Module de l'application	État recommandé du module	Recommandations
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Désactivé	–
Vérification de l'intégrité du système	Désactivé	–
Endpoint Detection and Response Expert (on-premises)	Désactivé	–
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Désactivé	–
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Désactivé	–
Interface graphique	Non défini	–
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Désactivé	–
Protection BadUSB	Désactivé	–
Fichiers de traçage	–	Remplacez le répertoire des fichiers de traçage par un répertoire situé en dehors du répertoire `/var/log/kaspersky`. Par exemple, utilisez le répertoire `/var/log/kesl`.
Exclusions globales	Configuré	Excluez les points de montage suivants : • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` L'exclusion des points de montage /tmp et /tmp/* s'applique aux serveurs NDR (KATA) de version 10.0 ou antérieure. • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

Paramètres de Kaspersky Endpoint Security for Linux sur les serveurs avec le module Central Node

Paramètres recommandés pour les serveurs Central Node

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `[container-name:*edr_synchronizer*]/tmp/` • `[container-name:*ids_alert_syncer*]/tmp/` • `[container-name:kata_product_main_1_kata_scanner]/storage` • `[container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql` • `[container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents` • `[container-name:*kata_scanner*]/var/lib/nginx/body` • `[container-name:*kata_scanner*]/apt_spool` • `[container-name:*kata_scanner*]/tmp/` • `[container-name:*kafka*]/tmp/` • `[container-name:*ksn_proxy*]/tmp/` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*preprocessor_icap*]/tmp/` • `[container-name:*preprocessor_span*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*statistics_clickhouse_importer*]/tmp/` • `[container-name:*updates_consistency_checker*]/tmp/` • `[container-name:*web_backend*]/tmp/` • `[container-name:*]/var/opt/kaspersky` • `/tmp/` • `/var/log/kaspersky`
Analyse des logiciels malveillants	Désactivé	–
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces réseau	Désactivé	–
Protection contre les menaces Internet	Désactivé	–
Protection contre le chiffrement	Désactivé	–
Analyser les conteneurs	Enabled	Activez la Surveillance des conteneurs pour analyser les conteneurs et les espaces de noms en cours d'exécution en temps réel `NamespaceMonitoring=Yes`
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Désactivé	–
Vérification de l'intégrité du système	Désactivé	–

Module de l'application	État recommandé du module	Recommandations
Endpoint Detection and Response Expert (on-premises)	Désactivé	–
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Désactivé	–
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Désactivé	–
Interface graphique	Non défini	–
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Désactivé	–
Protection BadUSB	Désactivé	–
Fichiers de traçage	–	Remplacez le répertoire des fichiers de traçage par un répertoire situé en dehors du répertoire `/var/log/kaspersky`. Par exemple, utilisez le répertoire `/var/log/kesl`.
Exclusions globales	Configuré	Ajoutez des points de montage aux exclusions : • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp` • `/tmp/*` L'exclusion des points de montage /tmp et /tmp/* s'applique aux serveurs NDR (KATA) de version 10.0 ou antérieure. • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

Lors de l'utilisation de Kaspersky Endpoint Security for Linux avec Kaspersky Unified Monitoring and Analysis Platform, nous vous recommandons d'utiliser les paramètres décrits dans cet article.

Module de l'application	État recommandé du module	Recommandations
Protection contre les fichiers malicieux	Enabled	Ajoutez des exclusions de la protection : • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
Analyse des logiciels malveillants	Désactivé	–
Analyse des disques amovibles	Désactivé	–
Détection comportementale	Enabled	Exclure le processus de l'analyse `/opt/kaspersky/kuma`
Protection contre les menaces réseau	Enabled	Désactiver le blocage de l'appareil compromis `BlockAttackingHosts=No`
Protection contre les menaces Internet	Désactivé	–
Protection contre le chiffrement	Désactivé	–
Analyser les conteneurs	Désactivé	–
Inventaire	Désactivé	–
Contrôle des appareils	Désactivé	–
Contrôle des applications	Désactivé	–
Pare-feu	Désactivé	–
Contrôle Internet	Désactivé	–
Contrôle de l'intégrité du système	Désactivé	–
Vérification de l'intégrité du système	Désactivé	–
Endpoint Detection and Response Expert (on-premises)	Désactivé	–
Endpoint Detection and Response Expert (cloud)	Désactivé	–
Managed Detection and Response	Désactivé	–
Network Detection and Response (KATA)	Désactivé	–
Intégration avec KUMA	Désactivé	–
Sandbox	Désactivé	–
Actions de réponse	Désactivé	–
Interface graphique	Non défini	–
Agent d'administration	Installée	Utiliser les paramètres par défaut.
Mécanisme d'interception des opérations sur les fichiers	Mécanisme d'interception des événements système basé sur fanotify	Utiliser les paramètres par défaut.
Source de télémétrie des événements système	eBPF+auditd	`TelemetrySource=Default`
Protection contre les Exploits	Désactivé	–
Utilisation de Kaspersky Security Network	Enabled	Utiliser les paramètres par défaut.
Protection contre les menaces par emails	Désactivé	–
Protection BadUSB	Désactivé	–

Sources d'informations sur Kaspersky Endpoint Security

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 peuvent répondre à des questions liées à Kaspersky Endpoint Security, mais également aux 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.

Glossaire

Abonnement

Utilisation de l'application selon les paramètres sélectionnés (date de fin, nombre d'appareils). Vous pouvez suspendre ou renouveler votre abonnement, le renouveler automatiquement ou l'annuler.

Activation de l'application

Passage de l'application en mode complet. L'utilisateur active l'application pendant l'installation ou après celle-ci. Pour activer l'application, l'utilisateur a besoin d'un code d'activation ou d'un fichier clé.

Appareil de confiance

Un appareil auquel un accès complet est autorisé à tout moment pour les utilisateurs spécifiés dans les paramètres de l'appareil 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 d'applications

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky au moment de la publication des bases. Les bases de l'application sont composées par les experts de Kaspersky et sont mises à jour toutes les heures.

Certificat de licence

Document fourni par Kaspersky avec le fichier clé ou le code d'activation. Il contient les informations concernant la licence octroyée.

Clé active

Clé utilisée au moment actuel pour faire fonctionner l'application.

Clé de réserve

Clé qui confirme le droit d'utilisation de l'application, mais non utilisée pour le moment.

Exclusion

Une *exclusion* est un objet exclu de l'analyse par une application de Kaspersky. Vous pouvez exclure de l'analyse des fichiers d'un certain format, des fichiers par masque, une certaine zone (par exemple, un dossier ou une application), des processus d'applications ou des objets par nom selon la classification de l'encyclopédie des virus. Vous pouvez définir des exclusions différentes pour chaque tâche.

Faux positif

Situation qui se produit lorsqu'une application de Kaspersky considère qu'un objet non infecté est infecté car son code est similaire à celui d'un virus.

Groupe d'administration

Ensemble d'appareils réunis dans Kaspersky Security Center en fonction des fonctions exécutées et de l'ensemble des applications de Kaspersky qui y sont installées. Les appareils sont regroupés pour la gestion aisée d'un ensemble. Un groupe d'administration peut inclure d'autres groupes. Pour chacune des applications installées dans le groupe d'administration, des stratégies de groupe peuvent être créées, ainsi que des tâches de groupe.

Licence

Droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence utilisateur final.

Light Agent

Module de Kaspersky Endpoint Security for Virtualization Light Agent. S'installe sur chaque machine virtuelle qu'il faut protéger.

Masque de fichier

Représentation du nom d'un fichier à l'aide de caractères génériques. Les principaux caractères utilisés dans les masques de fichiers sont * et ? (où * représente n'importe quel nombre de caractères, et? représente n'importe quel caractère unique).

Objet infecté

Objet dont un segment de code correspond complètement au segment de code d'une application présentant une menace. Les experts de Kaspersky déconseillent l'utilisation de tels objets.

Objets de démarrage automatique

Ensemble des applications nécessaires pour exécuter et faire fonctionner correctement le système d'exploitation et les logiciels installés sur votre ordinateur. Chaque fois que le système d'exploitation démarre, il exécute ces objets. Il existe des virus qui peuvent infecter ces mêmes objets, ce qui peut conduire, par exemple, à un blocage du démarrage du système d'exploitation.

Paramètres de l'application

Paramètres de l'application communs à tous les types de tâches. Ils régissent le fonctionnement global de l'application, comme ses performances, les rapports et les paramètres de la Sauvegarde.

Protection contre le chiffrement

Activité malveillante des ransomwares visant à chiffrer les fichiers contenant les données des utilisateurs. Les fichiers chiffrés ne sont ni lisibles ni utilisables.

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'administration

Un module de Kaspersky Security Center qui stocke de manière centralisée les informations relatives à toutes les applications Kaspersky installées au sein du réseau d'entreprise. Ce module permet également de gérer ces applications.

Serveur d'intégration

Module de Kaspersky Endpoint Security for Virtualization Light Agent. Effectue une interaction entre les modules de Kaspersky Endpoint Security et l'infrastructure virtuelle.

Serveur Proxy

Service réseau de l'ordinateur qui permet aux clients de lancer des requêtes indirectes vers d'autres services du réseau. Tout d'abord, un client se connecte à un serveur proxy et demande une ressource quelconque (par exemple, un fichier) située sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur spécifié et obtient la ressource depuis ce dernier ou renvoie la ressource depuis son propre cache (si le proxy dispose de son propre cache). Dans certains cas, le serveur proxy peut modifier la requête du client ou la réponse du serveur pour certains objectifs.

Serveurs de mise à jour de Kaspersky

Serveurs HTTP et FTP de Kaspersky à partir desquels les applications de Kaspersky reçoivent les mises à jour de leurs bases de données et de leurs modules.

Stratégie

La stratégie détermine les paramètres de fonctionnement d'une application et l'accès aux paramètres de l'application installée sur les appareils d'un groupe d'administration. Il faut créer une stratégie pour chaque application. Vous pouvez créer un nombre illimité de stratégies différentes pour des applications installées sur les appareils de chaque groupe d'administration, mais seule une stratégie peut être appliquée à la fois à chaque application au sein d'un groupe d'administration.

Stratégie active

Stratégie que l'application utilise actuellement pour contrôler les fuites de données. L'application peut utiliser plusieurs stratégies simultanément.

Stratégie de groupe

Voir Stratégie.

SVM

La machine virtuelle sécurisée est une machine virtuelle spéciale sur laquelle est installé le service scanserver (Serveur de protection, module de Kaspersky Endpoint Security for Virtualization Light Agent).

Système SIEM

Système Security Information and Event Management. Une solution pour gérer les informations et les événements dans le système de sécurité d'une organisation.

Tâche de groupe

Tâche définie pour un groupe d'administration et exécutée sur tous les appareils administrés inclus dans ce groupe d'administration.

Informations sur le code tiers

L'information sur le code tiers se trouve dans le fichier legal_notices.txt, situé dans le dossier d'installation de l'application.

Notice sur les marques de commerce

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

AMD64 est une marque commerciale ou une marque déposée d'Advanced Micro Devices, Inc.

Amazon est une marque commerciale d'Amazon.com, Inc. ou ses affiliés.

Mac, FireWire sont des marques commerciales d'Apple Inc.

Arm est une marque déposée d'Arm Limited (ou de ses filiales) aux États-Unis et/ou dans d'autres pays.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Ubuntu et LTS sont des marques de commerce déposées de Canonical Ltd.

XenServer est une marque déposée ou une marque commerciale de Cloud Software Group, Inc. et/ou filiales aux États-Unis et/ou dans d'autres pays.

Cloudflare, le logo Cloudflare et Cloudflare Workers sont des marques commerciales et/ou des marques déposées de Cloudflare, Inc. aux États-Unis et dans d'autres juridictions.

La marque verbale Grafana et le logo Grafana sont des marques déposées/marques de service ou des marques commerciales/marques de service de Coding Instinct AB aux États-Unis et dans d'autres pays et sont utilisés avec l'autorisation de Coding Instinct. Nous ne sommes pas affiliés, approuvés ou sponsorisés par Coding Instinct ou la communauté Grafana.

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.

Chrome et Google Public DNS sont des marques commerciales de Google LLC.

HUAWEI, EulerOS, FusionSphere sont des marques commerciales de Huawei Technologies Co., Ltd.

Intel et Core sont des marques commerciales d'Intel Corporation ou de ses filiales.

Linux est une marque de Linus Torvalds déposée aux États-Unis et dans d'autres pays.

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++ et Windows sont des marques commerciales du groupe de sociétés Microsoft.

OpenStack est une marque déposée de la OpenStack Foundation aux États-Unis et dans d'autres pays.

Oracle et JavaScript sont des marques déposées d'Oracle et/ou de ses filiales.

Python est une marque de commerce ou une marque déposée de la Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora sont des marques de commerce ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc.

SUSE est une marque de SUSE LLC déposée aux États-Unis et dans d'autres pays.

Kubernetes est une marque déposée de The Linux Foundation aux États-Unis et dans d'autres pays.

Rocky Linux est une marque déposée de The Rocky Enterprise Software Foundation.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, sous licence exclusive de X/Open Company Limited.

Zabbix est une marque déposée de Zabbix SIA.