kaspersky

Kaspersky Endpoint Security for Linux

Contenu

À propos de Kaspersky Endpoint Security 12.1 for Linux

L'application Kaspersky Endpoint Security 12.1 for Linux (également dénommé ici Kaspersky Endpoint Security, l'application) protège les appareils fonctionnant sous les systèmes d'exploitation Linux® contre les différents types de menaces, d'attaques réseau et de tentatives d'escroquerie.

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.

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 menaces sur les fichiers** permet d'éviter l'infection du système de fichiers de l'appareil de l'utilisateur. Le module *Protection contre les menaces sur les fichiers* 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 de logiciels malveillants. 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 du conteneur* vous permet de vérifier les espaces de noms et les conteneurs en cours d'exécution pour détecter les logiciels malveillants 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 sécurisées.

- **Protection contre les menaces réseau**. Le module *Protection contre les menaces réseaux* 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 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 le périphérique client contre les infections lorsque des périphériques 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 de 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, Kaspersky Endpoint Security bloquera l'accès ou affichera 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, 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 composants 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 sont réinitialisés.

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, mais informent uniquement l'utilisateur de la détection d'une menace.

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 Endpoint Detection and Response (KATA) par le module de la solution 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 assure une protection de 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.

Vous pouvez utiliser Kaspersky Endpoint Security comme application conteneur (ci-après dénommée conteneur KESL) à intégrer dans des systèmes externes pour analyser les images de conteneur à partir des référentiels.

La fonctionnalité du conteneur KESL n'est pas prise en charge si l'application Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

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 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 utilisateur graphique.

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.

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

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

1. Installer Kaspersky Endpoint Security sur chaque machine virtuelle qui doit être protégée avec Kaspersky Security for Virtualization Light Agent. Vous pouvez également installer l'application sur un modèle de machine virtuelle.

   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` et `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.

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 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. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Pour activer la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, vous devez en outre ajouter une clé de licence EDR Optimum à la SVM. Les licences destinées à activer les modules de la solution Kaspersky Security for Virtualization Light Agent n'incluent pas cette fonctionnalité.

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 de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Les informations sur la licence utilisée par Light Agent pour Linux peuvent être affichées sur une machine virtuelle protégée avec Light Agent à l'aide de la commande `kesl-control -L --query`.

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 reçoit les mises à jour des bases de données et des modules de l'application du Serveur de protection. Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Les bases de données et les modules sur les machines virtuelles protégées sont mises 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 mises à jour provenant de sources autres qu'un dossier sur la SVM et l'utilisation de tâches de mise à jour par lots ne sont pas prises 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 de données et des modules d'application sur la SVM, la tâche locale spéciale *Mise à jour* est automatiquement lancée sur la machine virtuelle protégée. À la suite de l'exécution de la tâche, Light Agent revient à l'utilisation de l'ensemble précédent de bases du logiciel malveillant.

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 fonctionnalités d'utilisation de l'application en mode Light Agent

Si Kaspersky Endpoint Security est utilisé en mode Light Agent :

- La fonctionnalité du conteneur KESL n'est pas prise en charge.
- 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. L'interaction 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.
- L'intégration avec Kaspersky Symphony XDR n'est pas prise en charge.

Kit de 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 kit de distribution de l'application Kaspersky Endpoint Security contient les fichiers suivants :

- kesl-12.1.0-<numéro de version>.i386.rpm, kesl_12.1.0-<numéro de version>_i386.deb

  Contient 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-12.1.0-<numéro de version>.x86_64.rpm, kesl_12.1.0-<numéro de version>_amd64.deb

  Contient 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-12.1.0-<numéro de version>.aarch64.rpm, kesl_12.1.0-<numéro de version>_arm64.deb

  Contient les principaux fichiers de l'application. Les paquets peuvent être installés sur des systèmes d'exploitation de 64 bits pour l'architecture Arm® conformément au type de gestionnaire de paquets.

- kesl-gui-12.1.0-<numéro de version>.i386.rpm, kkesl-gui-12.1.0-<numéro de version>_i386.deb

  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-12.1.0-<numéro de version>.x86_64.rpm, kesl-gui-12.1.0-<numéro de version>_amd64.deb

  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-12.1.0-<numéro de version>.aarch64.rpm, kkesl-gui-12.1.0-<numéro de version>_arm64.deb

  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-12.1.0.<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**.

- docker-service-kesl64-12.1.0-<numéro de version>.tgz

  Contient les fichiers pour la création de l'image de l'application en conteneur KESL.

- 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 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 KSN complémentaires.

Configurations logicielle et matérielle

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 requise :

- processeur Core™ 2 Duo 1,86 GHz ou supérieur ;
- un secteur de pagination d'au moins 1 Go ;
- 1 Go de RAM pour les systèmes d'exploitation 32 bits, 2 Go pour les systèmes 64 bits ;
- 4 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;
- Lors de l'utilisation d'une interface utilisateur 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.

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 mémoire vive ;
- 3 Go d'espace libre sur le disque dur pour installer l'application et stocker les fichiers temporaires et les fichiers journaux ;
- Lors de l'utilisation d'une interface utilisateur 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 n'est pas prise en charge sur les systèmes d'exploitation basés sur l'architecture Arm.

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 :
  - Debian GNU/Linux 11.0 et suivant
  - Debian GNU/Linux 12.0 et suivant
  - Mageia™ 4

    Sur les appareils sous le système d'exploitation Mageia 4, l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA) n'est pas prise en charge.
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - Alt SP Station de travail version 10
  - Alt SP Server version 10
- Systèmes d'exploitation 64 bits :
  - AlmaLinux OS 8 et suivant
  - AlmaLinux OS 9 et suivant
  - AlterOS® 7.5 et suivant
  - Amazon™ Linux 2
  - 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.10015-16 (release 1) (operational update 1.6)

    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 et suivant
- CentOS Stream 8
- CentOS Stream 9
- Debian GNU/Linux 11.0 et suivant
- Debian GNU/Linux 12.0 et suivant
- EMIAS 1.0 et suivant
- EulerOS 2.0 SP10
- Kylin 10
- Linux Mint 20.3 et suivant
- Linux Mint 21.1 et suivant
- openSUSE Leap 15.0 et suivant
- Oracle Linux 7.3 et suivant
- Oracle Linux 8.0 et suivant
- Oracle Linux 9.0 et suivant
- Red Hat Enterprise Linux 7.2 et suivant
- Red Hat Enterprise Linux 8.0 et suivant
- Red Hat Enterprise Linux 9.0 et suivant
- Rocky Linux 8.5 et suivant
- Rocky Linux 9.1
- SberLinux 8.8 (Dykhtau)
- SberOS 3.2.0.
- SUSE Linux Enterprise Server 12.5 et suivant
- SUSE Linux Enterprise Server 15 et suivant
- Ubuntu® 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- ALT 8 SP Workstation (8.4)
- ALT 8 SP Server (8.4)

- ALT Education 10.1
- ALT Workstation 10.1
- ALT Server 10.1
- Alt SP Station de travail version 10
- Alt SP Server version 10
- Atlant, version Alcyone, 2022.02
- GosLinux 7.17
- GosLinux 7.2
- MSVSPHERE 9.2 ARM
- SERVEUR MSVSPHERE 9.2
- RED OS® 7.3
- RED OS 8.0
- ROSA « Cobalt » 7.9
- ROSA « Chrome » 12
- 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
  - Ubuntu 22.04 LTS
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - Alt SP Station de travail version 10
  - Alt SP Server version 10
  - RED OS 7.3

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.

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 13.2. La gestion de Kaspersky Endpoint Security via la Console d'administration à l'aide du plug-in d'administration mmc est prise en charge.
- Kaspersky Security Center 14. L'administration de Kaspersky Endpoint Security 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 est prise en charge.
- Kaspersky Security Center 14.2 Windows. L'administration de Kaspersky Endpoint Security 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 est prise en charge.
- Kaspersky Security Center 14.2 Linux. L'administration de Kaspersky Endpoint Security via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web est prise en charge.
- Kaspersky Security Center 15 Linux. L'administration de Kaspersky Endpoint Security via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web est prise en charge.
- Kaspersky Security Center 15.1 Linux. L'administration de Kaspersky Endpoint Security via Kaspersky Security Center Web Console à l'aide du plug-in d'administration Web est prise en charge.

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 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

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 (KATA), il est recommandé d'utiliser les versions suivantes de Kaspersky Security Center pour gérer l'application :

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Versions prises en charge de Kaspersky Anti Targeted Attack Platform

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

- Kaspersky Anti Targeted Attack Platform 5.1. Pris en charge avec des restrictions.
- Kaspersky Anti Targeted Attack Platform 6.0.
- Kaspersky Anti Targeted Attack Platform 6.1.

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

Nouveautés

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

- La possibilité d'intégration avec Kaspersky Endpoint Detection and Response Optimum a été implémentée, ce qui protège 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.

- Il est désormais possible d'ajouter deux clés de licence actives à l'application : une clé primaire pour activer l'application et une clé supplémentaire pour activer la fonctionnalité Kaspersky Endpoint Detection and Response Optimum. Une clé supplémentaire est requise si votre licence principale n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum.

- Ajout d'un nouveau module fonctionnel *Contrôle Internet*, *qui* contrôle 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 bloquera l'accès ou affichera un avertissement.

- Une fonction de surveillance de la stabilité de Kaspersky Endpoint Security a été implémentée, qui vous permet de suivre le nombre d'arrêts anormaux de l'application et d'informer l'administrateur du fonctionnement instable de l'application.

- La procédure d'installation de Kaspersky Endpoint Security à l'aide de Kaspersky Security Center Web Console a été améliorée : dans les propriétés du paquet d'installation de l'application, vous pouvez désormais spécifier les paramètres initiaux de l'application qui n'étaient auparavant disponibles que dans le fichier de configuration autoinstall.ini.

- La possibilité de gérer des paramètres supplémentaires de l'application via Kaspersky Security Center Web Console et la Console d'administration de Kaspersky Security Center a été étendue : vous pouvez configurer des paramètres qui ne pouvaient auparavant être configurés qu'en modifiant le fichier de configuration kesl.ini.

- Ajout de la possibilité d'activer ou de désactiver l'utilisation d'exclusions globales et d'exclusions de la Protection contre les menaces sur les fichiers lors de l'exécution de tâches d'analyse.

- La possibilité d'intégration avec Kaspersky Symphony XDR a été implémentée : si l'application Kaspersky Endpoint Security est utilisée en mode standard, l'application peut effectuer les actions de réponse « Analyse des logiciels malveillants » et « Mettre à jour les bases ». Si Kaspersky Endpoint Security est utilisé en mode Light Agent, l'intégration avec Kaspersky Symphony XDR n'est pas prise en charge.

- Implémentation du transfert vers le Serveur d'administration des informations sur tous les appareils installés sur les appareils clients ou connectés à ceux-ci (y compris ceux installés et connectés précédemment et ceux déjà déconnectés) lors de la gestion de l'application à l'aide de Kaspersky Security Center.

- Les règles d'interception du trafic ont été améliorées pour prendre en charge l'interaction des conteneurs sur le même réseau.

- La liste des systèmes d'exploitation pris en charge est mise à jour.

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 périphérique répond aux exigences matérielles et logicielles de l'application.
- Assurez-vous qu'aucun logiciel antivirus tiers n'est installé sur votre périphérique.
- Assurez-vous que l'application Kaspersky Endpoint Agent for Linux n'est pas installée sur votre périphérique. Si Kaspersky Endpoint Agent for Linux est installé, un message s'affiche lors de l'installation et vous invite à le désinstaller manuellement.
- Assurez-vous que la version 5.10 ou supérieure de l'interpréteur Perl est installée sur votre périphérique.
- 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.
- En fonction du système d'exploitation de votre appareil, installez l'un des paquets suivants :
  - Sur un appareil sous SUSE Linux Enterprise Server 15, installez le paquet insserv-compat.
  - Sur un appareil sous Red Hat Enterprise Linux 8 ou RED OS, installez le paquet perl-Getopt-Long.
  - Sur un appareil sous Red Hat Enterprise Linux ou RED OS, installez le paquet perl-File-Copy. Ce paquet est requis pour que le script de configuration initial de l'application fonctionne, mais peut ne pas être présent par défaut.
- 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**).
- Si votre appareil utilise un noyau Linux inférieur à 3.16, pour intégrer Kaspersky Endpoint Detection and Response (KATA), vous devez vous assurer que le service auditd n'est pas en cours d'exécution ou installé.
- Pour que les tâches Gestion du pare-feu, Protection contre les menaces Internet et Protection contre les menaces réseaux fonctionnent, vous devez installer le paquet de l'utilitaire iptables sur votre appareil.
- Pour le fonctionnement du plug-in d'administration de Kaspersky Endpoint Security sur l'appareil sur lequel le Serveur d'administration de Kaspersky Security Center est installé, il faut installer Microsoft® Visual C++® 2015 Redistributable Update 3 RC (cf. https://www.microsoft.com/fr-fr/download/details.aspx?id=52685).
- 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.

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 paquets suivants sont 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 Cloud Platform, TIONICS Cloud Platform, OpenStack, Astra Linux et Alt Virtualization Server doit être installé sur les machines virtuelles.
- 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. Pour plus d'informations sur les modules de la solution, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

Ports utilisés dans le fonctionnement du Light Agent

Port et protocole	Direction	Objectif et description
7271 TCP	Du Light Agent au Serveur d'intégration.	Pour l'interaction entre le Light Agent et le Serveur d'intégration.
8000 UDP	De la SVM au Light Agent.	Pour envoyer des informations sur les SVM disponibles aux Light Agents à l'aide de la liste des adresses SVM.
8000 UDP	Du Light Agent à la SVM.	Pour que le Light Agent reçoive des informations sur l'état de la SVM.
11111 TCP	Du Light Agent à la SVM.	Pour envoyer des demandes de service (par exemple, pour obtenir des informations de licence) du Light Agent au Serveur de protection via une connexion non sécurisée.
11112 TCP	Du Light Agent à la SVM.	Pour envoyer des demandes de service (par exemple, pour obtenir des informations de licence) du Light Agent au Serveur de protection via une connexion sécurisée.
9876 TCP	Du Light Agent à la SVM.	Pour envoyer des demandes d'analyse de fichiers du Light Agent au Serveur de protection via une connexion non sécurisée.
9877 TCP	Du Light Agent à la SVM.	Pour envoyer des demandes d'analyse de fichiers du Light Agent au Serveur de protection via une connexion sécurisée.
80 TCP	Du Light Agent à la SVM.	Mettre à jour les bases de données et les modules d'application de la solution Light Agent.
15000	De Kaspersky	Pour administrer le Serveur de protection via Kaspersky Security

UDP	Security Center à SVM.	Center.
15000 UDP	De Kaspersky Security Center aux Light Agents.	Pour administrer Light Agent via Kaspersky Security Center.
13000 TCP	Du Light Agent à Kaspersky Security Center.	Pour administrer Light Agent via Kaspersky Security Center avec une connexion sécurisée.
14000 TCP	Du Light Agent à Kaspersky Security Center.	Pour administrer le Light Agent via Kaspersky Security Center avec une connexion non sécurisée.

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 et à la configuration 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.

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 le fonctionnement de l'application via 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**

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

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

   - À l'aide de Kaspersky Security Center.

   - À l'aide de la ligne de commande.

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

   La configuration initiale est nécessaire pour activer la protection du périphérique client.

   Si vous avez installé l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, une fois l'installation terminée, préparez l'application à utiliser.

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

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 le fonctionnement de l'application via 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**

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

   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.

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

   - À l'aide de Kaspersky Security Center.

     Avant de commencer l'installation, vous devez configurer les paramètres de configuration initiale de l'application de l'une des manières suivantes :

     - Dans les propriétés du paquet d'installation sous l'onglet **Paramètres** (cette mode est disponible uniquement dans Kaspersky Security Center Web Console).

     - À l'aide du 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).

- À l'aide de 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.

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

   La configuration initiale est nécessaire pour activer la protection du périphérique client.

   Si vous avez installé l'application Kaspersky Endpoint Security à l'aide de Kaspersky Security Center, une fois l'installation terminée, préparez l'application à utiliser.

   Si vous avez installé l'application Kaspersky Endpoint Security à partir de la ligne de commande, une fois l'installation terminée, exécutez le script de configuration initiale ou effectuez la configuration initiale 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 `Specifying the application usage` du script de configuration initiale.
   - Définissez le paramètre `KSVLA_MODE=yes` dans le fichier de configuration d'installation initiale.

   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.

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

L'installation de l'Agent d'administration est requise si vous envisagez d'administrer l'application Kaspersky Endpoint Security à l'aide 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.

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 ;
- à l'aide de la ligne de commande.

À propos de l'installation de l'Agent d'administration à l'aide de Kaspersky Security Center

Avant de démarrer l'installation à distance de l'Agent d'administration à l'aide de Kaspersky Security Center, vous devez préparer l'appareil pour l'installation à distance (cf. l'aide de Kaspersky Security Center, section Préparer l'appareil exécutant le système d'exploitation Linux et installer à distance l'Agent d'administration sur l'appareil exécutant le système d'exploitation Linux).

Pour une installation à distance, utilisez le paquet d'installation de l'Agent d'administration. Vous pouvez télécharger les fichiers requis pour créer le paquet d'installation de l'Agent d'administration sur le site de Kaspersky dans la section **Kaspersky Security Center**.

Pour installer l'Agent d'administration à distance :

1. Créez le paquet d'installation de l'Agent d'administration.

   Lors de la création d'un paquet d'installation, vous devez accepter les termes du Contrat de licence de l'Agent d'administration. Vous pouvez vous familiariser avec le texte du Contrat de licence en lisant le document licence.txt fourni avec l'Agent d'administration.

   Dans les paramètres du paquet d'installation, spécifiez l'adresse du Serveur d'administration auquel l'Agent d'administration doit se connecter et le port de connexion.

2. Installez l'Agent d'administration à l'aide de la tâche d'installation d'application à distance.

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

À propos de l'installation de l'Agent d'administration à l'aide de la ligne de commande

Vous pouvez installer l'Agent d'administration à l'aide de la ligne de commande de l'une des manières suivantes :

- Effectuez l'installation et la configuration initiale en mode silencieux avec un fichier de réponses. 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.

- Installez l'Agent d'administration à partir d'un paquet au format RPM ou DEB selon le type de gestionnaire de paquets, puis effectuez la configuration initiale de l'Agent d'administration à l'aide d'un script en mode interactif. Le script est lancé par la commande :

  - pour système d'exploitation 32 bits :

    ```
    # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
    ```

  - pour système d'exploitation 64 bits :

    ```
    # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

L'installation de l'Agent d'administration doit être démarrée avec les privilèges root.

Pour installer l'Agent d'administration en mode silencieux :

1. Créez un fichier de réponses. Ajoutez au fichier de réponses une liste de paramètres d'installation et de configuration initiale de l'Agent d'administration au format < `paramètre` >=< `valeur` >, chaque paramètre sur une ligne distincte.

   Pour utiliser correctement le fichier de réponses, vous devez inclure les paramètres requis suivants :

   - KLNAGENT_SERVER : nom de domaine complet (FQDN) ou adresse IP du Serveur d'administration.

   - KLNAGENT_AUTOINSTALL : ce paramètre détermine si le mode d'installation silencieuse est activé. Spécifiez la valeur `1`.

   - EULA_ACCEPTED : accord sur les termes du Contrat de licence pour l'Agent d'administration. Vous devez accepter les termes du Contrat de licence pour poursuivre la procédure d'installation. Consultez le texte du Vontrat de licence en lisant le document licence.txt inclus avec l'Agent d'administration. Si vous comprenez et acceptez les termes du Contrat de licence, saisissez la valeur `1`.

Vous pouvez également ajouter d'autres paramètres pour l'installation et la configuration initiale de l'Agent d'administration. Pour une liste complète des paramètres possibles, consultez l'aide de Kaspersky Security Center (section « Installation de l'Agent d'administration pour Linux en mode silencieux (avec fichier de réponses) »).

2. Définissez la valeur de la variable d'environnement KLAUTOANSWERS en saisissant le nom complet du fichier de réponses (y compris le chemin), par exemple comme suit :

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

3. Installez l'Agent d'administration :

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

     ```
     # rpm -i klnagent-<numéro de version>.i386.rpm
     ```

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

     ```
     # rpm -i klnagent64-<numéro de version>.x86_64.rpm
     ```

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

     ```
     # rpm -i klnagent64-<numéro de version>.aarch64.rpm
     ```

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

     ```
     # apt-get install ./klnagent_<numéro de version>_i386.deb
     ```

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

     ```
     # apt-get install ./klnagent64_<numéro de version>_amd64.deb
     ```

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

     ```
     # apt-get install ./klnagent64_<numéro de version>_arm64.deb
     ```

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

Pour administrer l'application Kaspersky Endpoint Security via Kaspersky Security Center, il faut utiliser les plug-ins d'administration suivants de Kaspersky Endpoint Security :

- le plug-in Web 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 d'administration mmc 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 d'administration 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.

Vous pouvez également convertir les stratégies et les tâches créées avec les versions précédentes du plug-in d'administration vers des versions plus récentes.

Installation du plug-in Web de Kaspersky Endpoint Security

Le plug-in Web d'administration de Kaspersky Endpoint Security doit être installé sur un appareil client 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 comme suit :

- 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 peut également vérifier si les plug-ins Internet installés sont à jour et télécharger les mises à jour nécessaires. 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 Web de Kaspersky Endpoint Security :

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

   Une liste des plugins Web 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 **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.

   - Installation d'un plug-in Web à partir d'une source tierce (les archives nécessaires à l'installation des plug-ins Web sont incluses dans le paquet) :

     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 **Ajouter**.

d. 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 client 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 plugin 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 plugins 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 **Avancé**, 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.

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.

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 configurer les paramètres de configuration initiale de l'application dans les propriétés du paquet d'installation (cette méthode est uniquement disponible dans Web Console) ou dans le fichier de configuration autoinstall.ini, inclus dans le paquet d'installation.

Vous pouvez déployer l'application Kaspersky Endpoint Security sur les appareils du réseau d'entreprise de plusieurs manières.

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.

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.

Une fois l'installation de l'application à l'aide de Kaspersky Security Center terminée, vous devez préparer l'application au fonctionnement.

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 périphériques dotés de l'application et configurer des règles automatiques de déplacements des périphériques vers les groupes d'administration. Si les règles de déplacement des périphériques vers les groupes d'administration ne sont pas configurées, Kaspersky Security Center place tous les périphériques 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 envisagez d'utiliser l'application Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, vous devez configurer les paramètres de configuration initiale de l'application dans les propriétés du paquet d'installation créé sous l'onglet **Paramètres**. Vous pouvez également configurer les paramètres de configuration initiale de l'application à l'aide du 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 sur la page de téléchargement de l'application dans la section **Kaspersky Endpoint Security for Linux** (**Paquet de distribution complémentaire -> Files for Product remote installation**).
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-12.1.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
     - kesl-12.1.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
     - kesl-12.1.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
     - kesl-12.1.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)
     - kesl-12.1.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
     - kesl-12.1.0-<numéro de version>_arm64.deb (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec dpkg)
   - Pour installer l'interface utilisateur graphique :
     - kesl-gui-12.1.0-<numéro de version>.i386.rpm (pour un système d'exploitation 32 bits avec rpm)
     - kesl-gui-12.1.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
     - kesl-gui-12.1.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
     - kesl-gui-12.1.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)

- kesl-gui-12.1.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
- kesl-gui-12.1.0-<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 utilisateur 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.

Notez que si l'interface utilisateur graphique n'est pas utilisée, vous devez alors définir la valeur du paramètre `USE_GUI=No` dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini. Dans le cas contraire, l'installation se terminera par une erreur.

Si vous souhaitez utiliser le paquet d'installation créer en vue d'installer l'application sur plusieurs types de systèmes d'exploitation ou de gestionnaires de paquets, placez dans le dossier les fichiers indispensables pour tous ces types de systèmes d'exploitation et de gestionnaires de paquets.

3. 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. Le fichier autoinstall.ini se trouve dans le dossier où vous avez extrait l'archive kesl.zip.

   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.

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

4. Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode standard et souhaitez utiliser des bases de données pré-téléchargées, placez les archives préparées avec les bases de données pour tous les types de systèmes d'exploitation requis dans un dossier, ouvrez le fichier de configuration autoinstall.ini et définissez la valeur du paramètre `UPDATE_EXECUTE=no`. Le fichier autoinstall.ini se trouve dans le dossier où vous avez extrait l'archive kesl.zip.

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 **Ajouter**.

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

3. Sur la première page de l'Assistant, sélectionnez la méthode 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 paquet d'installation démarre.

5. Lors de la création du paquet d'installation, il faut accepter les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité. Sur demande de l'assistant, lisez le Contrat de licence utilisateur final conclu entre vous et Kaspersky et 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.

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 périphériques du réseau de l'entreprise ou de mettre à jour la version de l'application.

Dans les propriétés du paquet d'installation, sous l'onglet **Paramètres**, vous pouvez configurer les paramètres de configuration initiale de l'application (voir le tableau ci-dessous).

La configuration du paquet d'installation de Kaspersky Endpoint Security n'est pas possible dans une version de Kaspersky Security Center Web Console antérieure à 14.2. Utilisez le fichier de configuration autoinstall.ini pour configurer les paramètres.

Paramètres du paquet d'installation

Section	Description
Indiquez la locale	Cochez cette case pour spécifier les paramètres régionaux du service à utiliser dans le cadre du fonctionnement de l'application. Les paramètres régionaux du service au format défini par la norme RFC 3066. Si ce paramètre n'est pas défini, les paramètres régionaux du service par défaut sont utilisés.
Activer l'application	Cochez la case pour activer l'application. Vous pouvez également activer l'application après l'installation. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.

Sélectionnez une source de mises à jour	Spécifiez la source de mise à jour : • **Serveurs de mise à jour de Kaspersky**. • **Kaspersky Security Center**. • **Autres sources sur le réseau local ou sur Internet**. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Exécuter la tâche de mise à jour des bases après l'installation	Cochez cette case pour exécuter la tâche de mise à jour après l'installation de l'application. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Indiquer les paramètres du serveur proxy	Cochez cette case pour spécifier l'adresse du proxy utilisé pour la connexion à Internet. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Installer le code source du noyau	Cochez cette case pour démarrer automatiquement la compilation du module du noyau.
Utiliser l'interface graphique	Cochez cette case pour activer l'utilisation de l'interface utilisateur graphique. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
Indiquer un utilisateur ayant le rôle d'administrateur (admin)	Cochez la case pour spécifier l'utilisateur auquel attribuer le rôle d'administrateur (admin).
Configurer automatiquement SELinux	Cochez la case pour configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security.
Supprimer les utilisateurs des groupes privilégiés	Cochez la case pour supprimer les utilisateurs des groupes privilégiés kesladmin et keslaudit avant d'installer l'application. 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	Cochez la case pour qu'après l'installation, l'application démarre avec les modules de protection et les tâches d'analyse désactivés.

que vous lancez l'application 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 trace. 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.
Utiliser l'application en mode Light Agent	Cochez la case si vous voulez utiliser l'application en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution Kaspersky Security for Virtualization Light Agent). Si cette case n'est pas cochée, l'application est utilisée en mode standard.
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. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.
La machine virtuelle protégée est utilisée comme serveur	Cochez la case si la machine virtuelle sur laquelle l'application sera installée est utilisée comme serveur dans l'infrastructure virtuelle. Le paramètre est appliqué uniquement si l'application est utilisée en mode Light Agent.

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.

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

1. Téléchargez l'archive kesl.zip sur la page de téléchargement de l'application dans la section **Kaspersky Endpoint Security for Linux** (**Paquet de distribution complémentaire -> Files for Product remote installation**).

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-12.1.0-<numéro de version>.i386.rpm (pour système d'exploitation 32 bits avec rpm)
     - kesl-12.1.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
     - kesl-12.1.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
     - kesl-12.1.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)

- kesl-12.1.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
- kesl-12.1.0-<numéro de version>_arm64.deb (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec dpkg)

- Pour installer l'interface utilisateur graphique :
  - kesl-gui-12.1.0-<numéro de version>.i386.rpm (pour un système d'exploitation 32 bits avec rpm)
  - kesl-gui-12.1.0-<numéro de version>_i386.deb (pour système d'exploitation 32 bits avec dpkg)
  - kesl-gui-12.1.0-<numéro de version>.x86_64.rpm (pour systèmes d'exploitation 64 bits avec rpm)
  - kesl-gui-12.1.0-<numéro de version>_amd64.deb (pour système d'exploitation 64 bits avec dpkg)
  - kesl-gui-12.1.0-<numéro de version>.aarch64.rpm (pour systèmes d'exploitation 64 bits pour l'architecture Arm avec rpm)
  - kesl-gui-12.1.0-<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 utilisateur 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.

Notez que si l'interface utilisateur graphique n'est pas utilisée, vous devez alors définir la valeur du paramètre `USE_GUI=No` dans les propriétés du paquet d'installation créé ou dans le fichier de configuration autoinstall.ini. Dans le cas contraire, l'installation se terminera par une erreur.

Si vous souhaitez utiliser le paquet d'installation créer en vue d'installer l'application sur plusieurs types de systèmes d'exploitation ou de gestionnaires de paquets, placez dans le dossier les fichiers indispensables pour tous ces types de systèmes d'exploitation et de gestionnaires de paquets.

3. 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. Le fichier autoinstall.ini se trouve dans le dossier où vous avez extrait l'archive kesl.zip.

   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.

4. Si vous envisagez d'utiliser l'application Kaspersky Endpoint Security en mode standard et souhaitez utiliser des bases de données pré-téléchargées, placez les archives préparées avec les bases de données pour tous les types de systèmes d'exploitation requis dans un dossier, ouvrez le fichier de configuration autoinstall.ini et définissez la valeur du paramètre `UPDATE_EXECUTE=no`. Le fichier autoinstall.ini se trouve dans le dossier où vous avez extrait l'archive kesl.zip.

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 **Additionnel** → **Installation à distance** → **Paquets d'installation**.

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

   L'Assistant de création de paquet démarre.

3. Dans la fenêtre de l'assistant qui s'ouvre, cliquez sur le bouton **Créer le paquet d'installation pour une application de Kaspersky**.

4. Saisissez le nom du nouveau paquet d'installation, puis passez à l'étape suivante.

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.

   Le nom de l'application s'affiche dans la fenêtre.

   Passez à l'étape suivante.

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.

7. 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.

8. 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 **Additionnel** → **Installation à distance** → **Paquets d'installation**. Vous pouvez utiliser le même paquet d'installation à plusieurs reprises.

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

Dans certains cas, vous devrez peut-être créer un paquet d'installation à distance avec des bases de données pré-téléchargées de l'application. Par exemple, si vous installez une application sur un appareil doté du système d'exploitation Astra Linux Special Edition ou si vous souhaitez installer l'application immédiatement avec des bases de données de travail prêtes à l'emploi (afin de ne pas mettre à jour en plus les bases de données ultérieurement).

Pour créer un paquet d'installation avec des bases de données intégrées pour installer l'application :

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 *Mise à jour* dans la Console d'administration de Kaspersky Security Center ou dans 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.

5. 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.

Paramètres du fichier de configuration autoinstall.ini

Paramètre	Description	Valeurs
KSVLA_MODE	Mode d'utilisation de Kaspersky Endpoint Security.	`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.
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.
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` (par défaut) – n'active pas le mode de protection de l'infrastructure VDI.

EULA_AGREED	Paramètre obligatoire. Acceptation du Contrat de licence utilisateur final.	`yes` (valeur par défaut) : pour continuer la procédure d'installation, il faut accepter les dispositions du Contrat de licence utilisateur final. `No` : refuser les dispositions 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 dispositions de la Politique de confidentialité pour poursuivre la procédure d'installation de l'application. `no` : ne pas accepter les dispositions 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.	`yes` : accepter les termes de la déclaration de Kaspersky Security Network et autorisez l'utilisation de KSN. `no` (valeur par défaut) : ne pas accepter les dispositions de la Déclaration de Kaspersky Security Network. Si l'application Kaspersky Endpoint Security est utilisée en mode standard et que vous avez activé l'utilisation de KSN, le mode cloud de l'application est automatiquement activé, dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données des logiciels malveillants.
GROUP_CLEAN	Paramètre obligatoire. Suppression d'utilisateurs des groupes privilégiés kesladmin et keslaudit.	`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.
LOCALE	Paramètre avancé. Paramètres régionaux du service pour la localisation des événements de l'application envoyés à Kaspersky Security Center.	Les paramètres régionaux du service au format défini par la norme RFC 3066. Si le paramètre `Locale` n'est pas défini, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à déterminer la version linguistique du système d'exploitation ou si la version n'est pas compatible avec l'application, la valeur par défaut `en_US.utf8` est sélectionnée.

		La localisation de l'interface utilisateur graphique et le la ligne de commande de l'application dépendent de la localisation renseignée par la variable d'environnement `LANG`. Si la variable d'environnement `LANG` renseigne une localisation qui n'est pas compatible avec l'application Kaspersky Endpoint Security, l'interface utilisateur et la ligne de commande apparaissent en anglais.
INSTALL_LICENSE	Code d'activation ou fichier clé. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	
UPDATER_SOURCE	Source des mises à jour. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`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 des mises à jour.
PROXY_SERVER	Adresse du proxy à utiliser pour la connexion à Internet. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	Adresse du proxy.
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de l'application lors de la configuration. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`yes` (valeur par défaut) : exécuter la tâche de mise à jour. `no` : ne pas lancer la tâche de mise à jour.
KERNEL_SRCS_INSTALL	Lancement automatique de la compilation du module du noyau.	`yes` (valeur par défaut) : compiler le module du noyau. `no` : ne pas compiler le module du noyau.
USE_GUI	Utilisation de l'interface utilisateur graphique.	`yes` : active l'utilisation de l'interface utilisateur graphique.

	Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`no` (par défaut) – désactive l'utilisation de l'interface utilisateur graphique.
ADMIN_USER	Utilisateur auquel est attribué le rôle d'administrateur (admin).	Non
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 configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security.
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 trace. 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.
DISABLE_FILEAV_ACTIONS	Désactivation des fonctions de désinfection et de suppression de fichiers pour les modules de l'application après l'installation. Si les fonctions de désinfection et de suppression de fichiers sont désactivées, si une menace est détectée, l'application ne tente pas de désinfecter ou de supprimer les fichiers dans lesquels une menace est détectée, mais informe uniquement l'utilisateur qu'une menace a été détectée dans les fichiers. Après avoir installé l'application, vous pouvez activer les fonctions de désinfection et de suppression de fichiers à l'aide du paramètre `DisableFileAvActions` dans le fichier de configuration kesl.ini.	`yes` : désactiver les fonctions de désinfection et de suppression de fichiers lors du lancement de l'application après l'installation. `no` (valeur par défaut) : ne pas désactiver les fonctions de désinfection et de suppression de fichiers lors du lancement de l'application après l'installation.

Si vous voulez modifier les paramètres dans le fichier de configuration initiale autoinstall.ini, saisissez les valeurs des paramètres au format <nom du paramètre>=<valeur du paramètre> (l'application ne traite pas les espaces entre le nom du paramètre et sa valeur).

Préparation de l'application pour une utilisation à l'aide de 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 :

- Activer 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 de clés de Kaspersky Security Center.
- Mettre à jour les bases de données et les modules de l'application via la Console d'administration ou Kaspersky Security Center Web Console. 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 d'administration mmc ou du plug-in d'administration Web de Kaspersky Endpoint Security.
- Configurer une stratégie d'administration centralisée de l'application à l'aide de la Console d'administration de Kaspersky Security Center 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 d'administration mmc ou du plug-in d'administration Web 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 administrer les stratégies, vous pouvez utiliser 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 afficher des informations sur la licence utilisée par Kaspersky Endpoint Security dans le cadre d'une solution sur une machine virtuelle protégée à l'aide de la commande `kesl-control -L --query`.

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 des tâches d'administration de l'application à l'aide de la Console d'administration et de Web Console.

Activation de l'application à l'aide de Kaspersky Security Center

L'*activation* est le processus 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 vous envisagez d'utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels, vous n'avez pas besoin d'activer l'application après l'installation. Vous activez Kaspersky Security for Virtualization Light Agent. L'activation s'effectue du côté du Serveur de protection (un module de Kaspersky Security for Virtualization Light Agent). Pour plus de détails, consultez l'aide de Kaspersky Security for Virtualization Light Agent.

La procédure d'activation de l'application Kaspersky Endpoint Security consiste à ajouter la clé de licence de l'application.

Si vous utilisez l'application sous une licence qui n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, pour activer cette fonctionnalité, vous devez ajouter une clé de licence supplémentaire de Kaspersky Endpoint Detection and Response Optimum Add-on (ci-après, la "clé EDR Optimum").

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 périphérique spécifique ou à des périphériques faisant partie d'un groupe d'administration. Vous pouvez créer et exécuter la tâche d'ajout d'une clé via Kaspersky Security Center Web Console ou via la Console d'administration.

- En distribuant aux périphériques clients une clé de licence stockée sur le Serveur d'administration de Kaspersky Security Center.

  Cette méthode permet d'ajouter automatiquement une clé aux périphériques client déjà connectés à Kaspersky Security Center et aux nouveaux périphériques clients. Pour utiliser cette méthode, vous devez d'abord ajouter la clé au stockage des clés sur le Serveur d'administration de Kaspersky Security Center.

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

  Cette méthode permet d'ajouter une clé dans les propriétés du paquet d'installation lors du déploiement de Kaspersky Endpoint Security. L'application sera activée automatiquement après l'installation.

Pour créer une tâche permettant d'ajouter une clé à une application, une tâche permettant d'ajouter une clé à un stockage de clés et une tâche permettant de distribuer une clé aux appareils clients, vous pouvez utiliser la Console d'administration de Kaspersky Security Center ou Kaspersky Security Center Web Console.

Activation dans Kaspersky Security Center Web Console

Avant de créer une tâche pour ajouter une clé à une application ou de distribuer une clé, il faut ajouter la clé au stockage du Serveur d'administration de Kaspersky Security Center.

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 **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 clé** et dans la fenêtre qui s'ouvre, sélectionnez le fichier portant 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 **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 périphériques en fonction de l'option de zone de tâche sélectionnée. 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 clé** et dans la fenêtre qui s'ouvre, sélectionnez le fichier portant 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 *Ajout d'une clé*, ajoutez si vous le souhaitez une *clé de réserve* au périphérique. 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 à une application 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 périphériques administrés**.
4. Cliquez sur **Enregistrer**.

   La clé de licence est alors distribuée automatiquement aux périphériques clients appropriés. Lors de la distribution automatique d'une clé en tant que clé active ou de réserve, la restriction de licence sur le nombre de périphérique (définie dans les propriétés de la clé) est prise en compte. Une fois la restriction de licence atteinte, la distribution de cette clé aux périphériques cesse automatiquement. Vous pouvez afficher le nombre de périphériques auxquels la clé a été ajoutée ainsi que d'autres données dans les propriétés de la clé sous l'onglet **Appareils**.

Vous pouvez surveiller l'utilisation des licences via Kaspersky Security Center Web Console d'une des manières suivantes :

- Consulter le rapport d'utilisation des clés de licence (**Surveillance et rapports → Rapports**).
- Affichez les états des appareils administrés (**Actifs (Appareils) → Appareils administrés**). Si l'application n'est pas activée, le périphérique affiche l'état et la description **Protection désactivée**.
- Consulter les propriétés de la clé (**Opérations → Licences Kaspersky**).

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 Kaspersky Security Center Cloud Console. Dans cette version, vous pouvez effectuer des actions dans votre 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 Kaspersky Security Center Cloud Console. Pour en savoir plus sur Kaspersky Security Center Cloud Console, consultez la documentation de Kaspersky Security Center Cloud Console.

La version d'essai de Kaspersky Security Center Cloud Console ne vous permet pas ensuite de passer à une version commerciale. Tout espace de travail d'évaluation sera automatiquement supprimé avec tout son contenu après trente jours.

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

Vous pouvez effectuer les opérations suivantes lors de l'installation d'une application à l'aide de la ligne de commande :

- Installez une application avec l'interface utilisateur graphique.

  Si l'application 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), l'interface utilisateur graphique n'est pas prise en charge. Vous devez installer uniquement le paquet de l'application sans l'interface utilisateur graphique.

- Installer l'application sans l'interface utilisateur graphique.

- Installez l'interface utilisateur 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 la version du gestionnaire de paquets apt est antérieure à 1.1.X, il faut utiliser le gestionnaire de paquets dpkg/rpm pour effectuer l'installation (en fonction du système d'exploitation).

Une fois l'installation de l'application terminée, vous devez effectuer la configuration initiale de l'application en mode interactif ou en mode automatique.

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

Installation de l'application sans l'interface utilisateur 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-12.1.0-<numéro de version>.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-12.1.0-<numéro de version>.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-12.1.0-<numéro de version>.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_12.1.0-<numéro de version>_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_12.1.0-<numéro de version>_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_12.1.0-<numéro de version>_arm64.deb
```

Installation de l'interface utilisateur graphique

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

```
# rpm -i kesl-gui-12.1.0-<numéro de version>.i386.rpm
```

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

```
# rpm -i kesl-gui-12.1.0-<numéro de version>.x86_64.rpm
```

Pour installer l'interface utilisateur 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-12.1.0-<numéro de version>.aarch64.rpm
```

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

```
# apt-get install ./kesl-gui_12.1.0-<numéro de version>_i386.deb
```

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

```
# apt-get install ./kesl-gui_12.1.0-<numéro de version>_amd64.deb
```

Pour installer l'interface utilisateur 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_12.1.0-<numéro de version>_arm64.deb
```

Configuration initiale de l'application en mode interactif

Une fois que l'application Kaspersky Endpoint Security a été installée via la ligne de commande, la configuration initiale de l'application doit être effectuée en exécutant le script de configuration initiale. Le script de configuration initiale figure dans le kit de distribution de Kaspersky Endpoint Security.

L'exécution de la configuration initiale après l'installation de l'application via la ligne de commande est nécessaire pour activer la protection du périphérique client.

Pour lancer manuellement le script de configuration initiale de Kaspersky Endpoint Security, exécutez la commande suivante :

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

Le script de configuration initiale de Kaspersky Endpoint Security doit être lancé sous les autorisations root après la fin de l'installation du paquet de Kaspersky Endpoint Security. Le script de configuration requiert de Kaspersky Endpoint Security des valeurs de paramètres étape par étape. Lorsque le script 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 a renvoyé le code 0, la configuration initiale de l'application a réussi.

Sélectionnez le mode d'utilisation de l'application

À cette étape, sélectionnez le mode d'utilisation de l'application Kaspersky Endpoint Security :

- Saisissez `yes` si vous souhaitez utiliser Kaspersky Endpoint Security en mode Light Agent pour protéger les environnements virtuels.
- Saisissez `no` si vous souhaitez utiliser Kaspersky Endpoint Security en mode standard.

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.

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.

Sélection des paramètres régionaux du service

À cette étape, l'application affiche la liste des paramètres régionaux du service compatibles au format spécifié par la norme RFC 3066.

Vous devez indiquer les paramètres régionaux du service au format qui figure dans la liste. Cette norme interviendra dans la localisation des événements de l'application envoyés à Kaspersky Security Center, ainsi que dans la localisation du Contrat de licence, de la Politique de confidentialité et de la Déclaration de Kaspersky Security Network.

La localisation de l'interface utilisateur graphique et le la ligne de commande de l'application dépendent de la localisation renseignée par la variable d'environnement `LANG`. Si la variable d'environnement `LANG` renseigne une localisation qui n'est pas compatible avec l'application Kaspersky Endpoint Security, l'interface utilisateur et la ligne de commande apparaissent en anglais.

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 refusez 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 refusez 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 l'application Kaspersky Endpoint Security est utilisée en mode standard et que vous avez activé l'utilisation de Kaspersky Security Network, le mode cloud de l'application est automatiquement activé, dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données des 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.

Vous pouvez attribuer à l'utilisateur le rôle d'administrateur plus tard à n'importe quel moment.

Détermination du type d'intercepteur des opérations de fichier

Cette étape correspond à la définition du type d'intercepteur des opérations de fichier pour le système d'exploitation utilisé. Pour les systèmes d'exploitation qui ne prennent pas en charge la technologie fanotify, la compilation du module du noyau est lancée.

Si les paquets requis ne sont pas détectés lors de la compilation du module noyau, Kaspersky Endpoint Security propose de les installer. En cas d'échec du téléchargement des paquets, un message d'erreur s'affiche.

Si tous les paquets nécessaires sont présents, le module noyau est automatiquement compilé au lancement de la tâche Protection contre les menaces sur les fichiers.

Il est possible de compiler le module du noyau plus tard, après la configuration initiale de l'application Kaspersky Endpoint Security.

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 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, 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 Kaspersky Endpoint Security.

Configuration de la source des mises à jour

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors de la première étape. 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 les sources de mise à jour pour les bases de données et les modules de l'application.

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 le périphérique 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 périphériques au sein de votre entreprise.
- `< adresse Internet >` : 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.
- `< chemin >` : l'application reçoit les mises à jour du répertoire spécifié.

Configuration du serveur proxy

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors de la première étape.

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 :
  - `< Adresse IP du serveur proxy >:< numéro de port >` si l'authentification n'est pas requise pour se connecter au serveur proxy ;

- `<Nom d'utilisateur>:<mot de passe>@<adresse IP du serveur proxy>:<numéro de port>` si une authentification est requise pour se connecter au serveur proxy.

  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 sécurisée et le compte utilisateur peut être compromis.

- Si la connexion à Internet s'opère sans serveur proxy, introduisez la réponse no.

Par défaut, l'application suggère `no`.

Vous pouvez configurer les paramètres du serveur proxy ultérieurement sans utilisation du script de configuration postérieure à l'installation.

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

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors de la première étape. 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. 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 `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.

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

Vous pouvez démarrer la tâche de mise à jour ultérieurement sans utiliser le script de configuration initiale.

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

Cette étape s'affiche uniquement si vous avez choisi d'utiliser Kaspersky Endpoint Security en mode standard lors de la première étape. 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 la mise à jour automatique des bases de données ultérieurement sans utiliser le script de configuration postérieur à l'installation en configurant la planification de 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 de la première étape. 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 sans utilisation du script de configuration initiale.

Configuration initiale de l'application en mode automatique

Vous pouvez réaliser la configuration initiale de l'application en mode automatique.

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

Lorsque le script 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 a renvoyé le code 0, la configuration initiale de l'application a réussi.

Pour mettre à jour correctement les modules de l'application une fois le script terminé, vous devrez peut-être redémarrer l'application. Vérifiez l'état des mises à jour de votre 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.

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

Paramètre	Description	Valeurs
KSVLA_MODE	Mode d'utilisation de Kaspersky Endpoint Security.	`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.
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.
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.
EULA_AGREED	Paramètre obligatoire. Acceptation du Contrat de licence utilisateur final.	`yes` : pour continuer la procédure d'installation, il faut accepter les dispositions du Contrat de licence utilisateur final.

		`No` : refuser les dispositions 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` : accepter les dispositions de la Politique de confidentialité pour poursuivre la procédure d'installation de l'application. `no` : ne pas accepter les dispositions 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.	`yes` : accepter les termes de la déclaration de Kaspersky Security Network et autorisez l'utilisation de KSN. `no` : ne pas accepter les dispositions de la Déclaration de Kaspersky Security Network. Si l'application Kaspersky Endpoint Security est utilisée en mode standard et que vous avez activé l'utilisation de KSN, le mode cloud de l'application est automatiquement activé, dans lequel Kaspersky Endpoint Security utilise une version allégée des bases de données des logiciels malveillants.
GROUP_CLEAN	Paramètre obligatoire. Suppression d'utilisateurs des groupes privilégiés kesladmin et keslaudit.	`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.
LOCALE	Paramètre avancé. Paramètres régionaux du service pour la localisation des événements de l'application envoyés à Kaspersky Security Center.	Les paramètres régionaux du service au format défini par la norme RFC 3066. Si le paramètre `Locale` n'est pas défini, c'est la langue du système d'exploitation qui est utilisée. Si l'application ne parvient pas à déterminer la version linguistique du système d'exploitation ou si la version n'est pas compatible avec l'application, la valeur par défaut `en_US.utf8` est sélectionnée.

		La localisation de l'interface utilisateur graphique et le la ligne de commande de l'application dépendent de la localisation renseignée par la variable d'environnement `LANG`. Si la variable d'environnement `LANG` renseigne une localisation qui n'est pas compatible avec l'application Kaspersky Endpoint Security, l'interface utilisateur et la ligne de commande apparaissent en anglais.
INSTALL_LICENSE	Code d'activation ou fichier clé. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	
UPDATER_SOURCE	Source des mises à jour. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`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 des mises à jour.
PROXY_SERVER	Adresse du proxy à utiliser pour la connexion à Internet. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	Adresse du proxy.
UPDATE_EXECUTE	Lancement de la tâche de mise à jour des bases de l'application lors de la configuration. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.	`yes` : lancer la tâche de mise à jour. `no` : ne pas lancer la tâche de mise à jour.
KERNEL_SRCS_INSTALL	Lancement automatique de la compilation du module du noyau.	`yes` : compiler le module du noyau. `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	`yes` : configurer automatiquement SELinux pour qu'il fonctionne avec

	l'application Kaspersky Endpoint Security.	Kaspersky Endpoint Security. `no` : ne pas configurer automatiquement SELinux pour qu'il fonctionne avec Kaspersky Endpoint Security.
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 trace. 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.
DISABLE_FILEAV_ACTIONS	Désactivation des fonctions de désinfection et de suppression de fichiers pour les modules de l'application après l'installation. Si les fonctions de désinfection et de suppression de fichiers sont désactivées, si une menace est détectée, l'application ne tente pas de désinfecter ou de supprimer les fichiers dans lesquels une menace est détectée, mais informe uniquement l'utilisateur qu'une menace a été détectée. Après avoir installé l'application, vous pouvez activer les fonctions de désinfection et de suppression de fichiers à l'aide du paramètre `DisableFileAvActions` dans le fichier de configuration kesl.ini.	`yes` : désactiver les fonctions de désinfection et de suppression de fichiers lors du lancement de l'application après l'installation. `no` (valeur par défaut) : ne pas désactiver les fonctions de désinfection et de suppression de fichiers lors du lancement de l'application après l'installation.

Si vous voulez modifier les paramètres dans le fichier de configuration initiale de l'application, saisissez les valeurs des paramètres au format <nom du paramètre>=<valeur du paramètre> (l'application ne traite pas les 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 SELinux pour qu'il fonctionne avec l'application :

1. Placez 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 différente de la stratégie par défaut targeted policy, attribuez une étiquette aux fichiers exécutables sources de l'application Kaspersky Endpoint Security suivants conformément à la stratégie SELinux utilisée :
   - /var/opt/kaspersky/kesl/12.1.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.1.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.1.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.1.0.<numéro de version>_<horodatage installation>/opt/kaspersky/kesl/shared/kesl
4. Lancez les tâches suivantes :
   - tâche de protection contre les menaces sur les fichiers :

     ```
     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 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 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`, alors pour exécuter la tâche Démarrer le processus, vous devez configurer en plus le système SELinux.

Pour configurer SELinux pour exécuter la tâche Démarrer le processus :

1. Placez 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.

6. Placez 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.

Pour Astra Linux Special Edition (operational update 1.7) et Astra Linux Special Edition (operational update 1.6)

Pour lancer l'application dans le système d'exploitation Astra Linux Special Edition (operational update 1.7) ou Astra Linux Special Edition (operational update 1.6) :

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
   ```

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
   ```

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

Mise à jour d'une ancienne version de l'application

Vous pouvez réaliser la mise à jour vers Kaspersky Endpoint Security 12.1 for Linux uniquement depuis Kaspersky Endpoint Security 12.0 for Linux.

Il n'est pas possible de mettre à jour Kaspersky Endpoint Security des versions antérieures vers la version 12.1. Si vous disposez d'une version antérieure de Kaspersky Endpoint Security, vous devez d'abord la désinstaller, puis installer Kaspersky Endpoint Security 12.1 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.

   Sans la mise à jour de l'Agent d'administration, il sera impossible de gérer l'application via Kaspersky Security Center.

   > 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 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 utilisez.

3. **Mise à jour de l'application et de l'interface utilisateur 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 et que vous utilisez l'interface utilisateur graphique de l'application, vous devrez également mettre à jour l'interface utilisateur graphique.

   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 dump de la version précédente sont supprimés.

Si Kaspersky Endpoint Security est utilisé en mode standard, il est recommandé d'exécuter la tâche de mise à jour de la base de données après la mise à jour de l'application.

À propos de la mise à jour des plug-ins d'administration 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 Web d'administration de Kaspersky Endpoint Security ;
- le plug-in mmc d'administration de Kaspersky Endpoint Security.

Les stratégies et les tâches configurées pour la version de l'application Kaspersky Endpoint Security 12.0 for Linux 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).

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.

Mise à jour de l'application via Kaspersky Security Center

La mise à jour de l'application et de l'interface utilisateur graphique est effectuée en installant à distance une nouvelle version des paquets de l'application et de l'interface utilisateur 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.

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.

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.

Si vous utilisez une interface graphique, pour la mettre à jour, vous devez d'abord désinstaller la version précédente du paquet de l'interface utilisateur graphique à l'aide de la commande `rpm -e --nodeps kesl-gui` puis installer le paquet contenant les fichiers de l'interface utilisateur graphique 12.1.

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 nouvelles conditions 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, sinon l'utilisation de KSN sera désactivée.

Pour accepter les termes des nouveaux accords lors de la mise à jour, utilisez les variables d'environnement `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.

   - Paquet RPM :

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<numéro de version>.<arch>.rpm [kesl-gui-12.1.0-<numéro de version>.<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 utillisateur graphique installés sur un système d'exploitation avec rpm, il n'est pas recommandé de mettre à jour un seul des paquets.

   - Paquet DEB :

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.1.0-<numéro de version>_<arch>.deb [./kesl-gui_12.1.0-<numéro de version>_<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 dpkg, il n'est pas possible de mettre à jour un seul des paquets.

2. L'application Kaspersky Endpoint Security redémarre automatiquement.

3. Sur certains systèmes d'exploitation, vous devrez peut-être redémarrer le système d'exploitation ; l'application affichera un message à ce sujet.

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 et que, après la mise à jour de l'application, vous souhaitez utiliser les valeurs des paramètres de stratégie et de tâche configurés dans Kaspersky Security Center pour la version précédente de l'application, vous devez convertir les stratégies et les tâches (pour plus de détails, consultez 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. Si vous utilisez Web Console pour gérer votre application, vous devrez créer de nouvelles stratégies et tâches pour la version mise à jour de l'application. Vous pouvez transférer certains 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 des paramètres.

Sur la ligne de commande, les valeurs de la plupart des paramètres sont reprises 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.

Paramètres des exclusions

Après la conversion des tâches dans le plug-in mmc, dans les tâches d'analyse (type ODS) et les tâches d'analyse des conteneurs, les cases **Utiliser les exclusions globales** et **Utiliser les exclusions de la Protection contre les menaces sur les fichiers** seront décochées. La conversion des tâches dans le plug-in Web n'est pas prise en charge.

Après avoir mis à jour l'application à l'aide de la ligne de commande, les paramètres `UseOASExclusions` et `UseGlobalExclusions` sont définis sur `No`.

Paramètres d'utilisation de Kaspersky Security Network

Après la conversion d'une stratégie dans le plug-in mmc, l'option **Ne pas utiliser Kaspersky Endpoint Security** sera sélectionnée dans les propriétés de la stratégie. 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.

Pour démarrer ou reprendre l'utilisation de Kaspersky Security Network, vous avez besoin de :

- sélectionner l'option **Mode standard KSN** ou **Mode avancé KSN** lors de l'utilisation du plug-in mmc ou Web ;
- définir le paramètre `UseKSN` sur `Basic` ou `Extended` lorsque vous utilisez la ligne de commande.

Paramètres d'utilisation du mode cloud

Après la conversion d'une stratégie dans le plug-in mmc, 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 le paramètre `UseKSN=Yes` après la mise à jour et avant la mise à jour, la valeur a été définie sur `CloudMode=Yes`.

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 avancé KSN** et cocher la case **Activer le mode cloud** lorsque vous utilisez le plug-in mmc ou Web ;
- définir les paramètres `UseKSN` et `CloudMode` sur `Yes` lorsque vous utilisez la ligne de commande.

Mode d'interception des opérations sur les fichiers

Si dans la version précédente de l'application, la case **Bloquer l'accès aux fichiers pendant l'analyse** était décochée, alors après la conversion de la stratégie dans le plug-in mmc, le paramètre **Première action** de la tâche Protection contre les menaces sur les fichiers est défini sur **Bloquer**. La conversion des stratégies n'est pas prise en charge dans le plug-in Web.

Le nom du paramètre de la ligne de commande qui détermine le mode d'interception des opérations sur les fichiers a changé dans la nouvelle version de l'application de `InterceptorProtectionMode=Block|Notify` à `FileBlockDuringScan=Yes|No`. Si dans une version précédente de l'application, le paramètre `InterceptorProtectionMode` était défini sur `Notify`, alors après la mise à jour de l'application à l'aide de la ligne de commande, le paramètre `FileBlockDuringScan` est défini sur `No` et le paramètre `FirstAction` de la tâche Protection contre les menaces sur les fichiers est défini sur `Block`.

Suppression d'une application

La procédure de désinstallation de l'application Kaspersky Endpoint Security comprend les étapes suivantes :

1. **Suppression d'une application et de l'interface utilisateur graphique de l'application**

   Vous devez supprimer les paquets de l'application et les paquets de l'interface utilisateur graphique de l'application depuis les appareils protégés, si vous avez utilisé une interface utilisateur graphique.

   Vous pouvez désinstaller le paquet de l'application et le paquet de l'interface utilisateur graphique en même temps, ou vous pouvez désinstaller uniquement le paquet de l'interface utilisateur graphique. Il est impossible de supprimer uniquement le paquet de l'application si le paquet de l'interface utilisateur graphique est installé.

   Vous pouvez désinstaller une 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.

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 plus de détails, 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 le périphérique 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 l'application et l'interface utilisateur graphique installées 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 utilisateur graphique, exécutez la commande suivante :

```
# rpm -e kesl
```

Pour supprimer Kaspersky Endpoint Security installé à l'aide d'un paquet au format DEB, sans l'interface utilisateur graphique, exécutez la commande suivante :

```
# apt-get purge kesl
```

Suppression du paquet de l'interface utilisateur graphique

Pour supprimer l'interface utilisateur graphique installée à l'aide d'un paquet au format RPM, exécutez la commande suivante :

```
# rpm -e kesl-gui
```

Pour supprimer l'interface utilisateur graphique 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.

À propos de la suppression des plug-ins d'administration de Kaspersky Endpoint Security

Le plug-in Web d'administration de Kaspersky Endpoint Security est supprimé dans Kaspersky Security Center Web Console dans la liste des plug-ins installés (**Paramètres** → **Plug-ins Web**).

Pour supprimer le plug-in mmc, utilisez les outils de suppression des applications standard du système d'exploitation. Dans la liste des applications, vous devez sélectionner **Kaspersky Endpoint Security <numéro de version> for Linux** à désinstaller.

Licences de l'application

Cette section contient des informations sur les concepts de base liés aux licences de l'application Kaspersky Endpoint Security.

À propos du contrat de licence utilisateur final

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 consulter les termes du Contrat de licence de Kaspersky Endpoint Security et la Politique de confidentialité, qui décrit le traitement et le transfert des données, des manières suivantes :

- En lisant le texte du fichier license.<identifiant de la langue>. Ce fichier est fourni dans le kit de distribution de l'application.
- Pendant l'installation de l'application Kaspersky Endpoint Security.

  Vous acceptez les termes du Contrat de licence et de la Politique de confidentialité en confirmant votre accord avec le texte du Contrat de licence et de la Politique de confidentialité lors de la création du paquet d'installation de l'application (en cas d'installation à l'aide de Kaspersky Security Center) ou lors de la configuration initiale de l'application (dans le cas d'une installation par ligne de commande). Si vous n'acceptez pas les termes du Contrat de licence et de la Politique de confidentialité, vous devez mettre fin à l'installation de l'application et ne devez pas utiliser l'application.

- Après l'installation de l'application Kaspersky Endpoint Security.

  Après l'installation de l'application, les fichiers contenant le texte du Contrat de licence de l'application Kaspersky Endpoint Security et 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.

Il existe différents types de licence :

- *Évaluation* : une licence gratuite qui permet de découvrir les fonctionnalités de 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.

- *Commerciale* : 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.

À propos du certificat de licence

Un *certificat de licence* est un document que vous recevez avec un fichier clé ou un code d'activation.

Un certificat de licence contient les informations suivantes sur la licence fournie :

- Clé de licence ou numéro de commande
- Informations sur l'utilisateur qui a obtenu la licence
- Informations relatives à l'application qui peut être activée à l'aide de la licence octroyée
- Restriction du nombre de postes couverts par la licence (par exemple, le nombre de périphériques sur lesquels la licence permet l'utilisation de l'application)
- Date de début de validité de la licence
- Date d'expiration de la licence ou période de validité de la licence
- Type de licence

À propos de la clé de licence

Une *clé de licence* est une séquence de bits que vous pouvez appliquer pour activer, puis utiliser l'application conformément aux conditions du Contrat de licence utilisateur final. La clé de licence est créée par les spécialistes de Kaspersky.

Vous pouvez ajouter une clé de licence à l'application à l'aide d'une des méthodes suivantes : en appliquant un *fichier clé* ou en saisissant 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'application.

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.

Les *types* de clés de licence suivants sont disponibles pour l'application Kaspersky Endpoint Security :

- *Clé de l'application* : une clé de licence pour activer les fonctionnalités de l'application Kaspersky Endpoint Security. Les fonctionnalités de l'application disponibles dépendent de la licence associée à la clé de l'application.
- *Clé EDR Optimum* est une clé de licence supplémentaire pour le module complémentaire Kaspersky Endpoint Detection and Response Optimum permettant d'activer la fonctionnalité de Kaspersky Endpoint Detection and

Response Optimum. Cette clé est requise si vous utilisez l'application sous une licence qui n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum.

Une clé de licence peut être 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 active de chaque type par application.

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. 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 lettres et chiffres. Vous devez saisir 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 avec l'extension .key qui vous est fourni par Kaspersky. Le but d'un fichier clé est d'ajouter une clé de licence qui active l'application.

Le fichier clé est envoyé à l'adresse email que vous avez indiquée à l'achat de Kaspersky Endpoint Security ou à la commande de la version d'évaluation de Kaspersky Endpoint Security.

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

Si un fichier clé a été supprimé par accident, vous pouvez le restaurer. Par exemple, vous pourriez avoir besoin du fichier clé pour créer un compte Kaspersky CompanyAccount.

Pour restaurer votre fichier clé, effectuez l'une des actions suivantes :

- Contactez le vendeur de la licence.
- Procurez-vous un fichier clé via le site Internet de Kaspersky avec votre code d'activation.

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 de périphériques 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.

S'agissant des abonnements limités, il se peut que vous bénéficiez d'une période de grâce pour le renouvellement. Au cours de cette période, l'application conserve ses fonctions. 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 de la licence (cf. le tableau ci-dessous).

Une comparaison des fonctionnalités des applications est fournie pour les solutions basées sur des processeurs à architecture Intel. Veuillez contacter votre fournisseur de services pour obtenir des informations sur les licences et les fonctionnalités disponibles pour les solutions basées sur des processeurs à architecture Arm.

Comparaison des fonctionnalités de l'application

Fonction	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security (Desktop)	Kaspersky Security fo Virtual Environmen (Desktop)

Protection contre les menaces sur les fichiers	✓	✓	✓	✓	✓
Protection contre les menaces Internet	✓	✓	✓	✓	✓
Protection contre les menaces réseaux	✓	✓	✓	✓	✓
Gestion du pare-feu	✓	✓	✓	✓	✓
Détection comportementale	✓	✓	✓	✓	✓
Contrôle des périphériques	✓	✓	✓	✓	✓
Analyse des disques amovibles	✓	✓	✓	✓	✓
Protection contre le chiffrement (pour les dossiers partagés)	✓	✓	✓	–	–
Analyse de conteneurs	–	–	–	–	–
Contrôle de l'intégrité du système	–	–	–	–	–
Contrôle des applications	–	✓	✓	✓	✓
Contrôle Internet	✓	✓	✓	✓	✓
Intégration avec Kaspersky Endpoint Detection and Response Optimum	–	–	–	–	–

Fourniture de 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 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 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 de périphériques 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 le périphérique ;
  - 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 périphériques 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 périphériques.
- Liste des états des périphériques 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 du périphérique ; 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 résultat de l'exécution des tâches locales et de groupe et valeurs de leur paramètres.
- 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 composant 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 composant 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 ;
- identificateur 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 le périphérique, 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 du périphérique ; informations relatives aux connexions bloquées (nom, description, nom du périphérique, 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 du périphérique sur lequel le chiffrement malveillant a été détecté, informations relatives au blocage ou au déblocage du périphérique) ;
- paramètres de l'application et paramètres de réseau ;
- informations relatives à la règle du Contrôle des applications appliquée (nom et type) et 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 périphériques 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'isolation 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

Si vous utilisez Kaspersky Security Network en mode avancé, vous acceptez de transmettre automatiquement à Kaspersky toutes les données citées dans la Déclaration de Kaspersky Security Network. En outre, Kaspersky pourra recevoir à des fins d'analyse des fichiers (ou des extraits de fichiers) qui présentent un risque d'utilisation malveillante dans le but de nuire à votre périphérique ou aux données conservées dans son système d'exploitation.

Le fichier ksn_license.<ID de la langue> qui contient le texte de la Déclaration de Kaspersky Security Network figure dans le kit de distribution de l'application.

Données fournies lors de l'utilisation de la solution Kaspersky Anti Targeted Attack Platform

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 de service suivantes, qui peuvent contenir des données personnelles et confidentielles :

- Adresses des serveurs KATA.
- Clé publique du certificat du serveur pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
- Cryptocontainer avec un certificat client pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
- identifiants pour l'autorisation 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 des tâches.
- Noms et mots de passe des comptes sous lesquels vous souhaitez exécuter des tâches.
- Versions de 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 composant EDR (KATA) :
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Nom du périphérique.
  - Adresse IP du périphérique.
  - Adresse MAC du périphérique.
  - Heure locale sur le périphérique.
  - Nom et version du système d'exploitation installé sur le périphérique.
  - Version de Kaspersky Endpoint Security.
  - Date d'édition des bases de données utilisées de l'application.
  - État de la licence.
- Données extraites des requêtes au composant EDR (KATA) dans les rapports sur les résultats de tâche :
  - Adresse IP du périphérique.
  - Identifiant unique.
  - Partie essentielle de l'adresse Internet du serveur.
  - Adresse MAC du périphérique.

- Erreurs d'exécution des tâches et codes de retour.
- États attribués à l'issue des tâches.
- Heure d'achèvement 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, sommes de hachage MD5 et SHA256 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'isolation 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 à distance 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.

- Données dans les paquets de télémétrie :
  - Données sur les fichiers :
    - Identifiant unique du fichier.
    - Chemin d'accès au fichier.
    - Nom du fichier.
    - Taille du fichier.
    - Attributs de 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 unique du fichier du processus.
  - Paramètres de lancement du processus.
  - Identifiants du processus.
  - Identifiant de la session.
  - Date et heure de lancement du processus.
  - Informations sur l'utilisateur et le groupe pour le compte duquel le processus est exécuté (nom et identifiant).
- 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 de 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.

En outre, les informations spécifiées peuvent être stockées dans les fichiers de trace et les fichiers de vidage.

Données fournies lors de l'utilisation de 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) ;
  - identifiant du processus parent (PPID) ;
  - le nom de l'utilisateur qui a démarré le processus ;

- date et heure de lancement 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 de volume ;
  - type de volume.
- Informations sur le système d'exploitation :
  - nom et version du système d'exploitation ;
  - nom 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 ;
  - identifiant 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 requête HTTP ;
- identifiant unique du processus qui a effectué la requête HTTP.

Données pour construire une chaîne de développement des menaces

Les données permettant de créer une chaîne de développement des 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 sur l'objet traité :
  - ID de processus ;
  - identifiant 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 traité ;
- attributs de l'objet traité ;
- 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 en dernier lieu ;
- 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 requête Web traitée ;
- source des liens de la requête web traitée (référent HTTP) ;
- agent de l'utilisateur de la requête Web traitée ;
- type de requête Web traitée (GET ou POST) ;
- port IP local pour la requête Web traitée ;
- port IP à distance pour la requête Web traitée ;
- sens de connexion (entrant ou sortant) de la requête Web traitée ;
- identifiant du processus dans lequel le code malveillant a été injecté.

Concept d'administration de l'application

Pour gérer l'application Kaspersky Endpoint Security, vous pouvez utiliser :

- Kaspersky Security Center ;
- ligne de commande ;
- l'interface utilisateur graphique.

> 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 utilisateur graphique.

L'éventail des actions que vous pouvez effectuer à l'aide de l'interface utilisateur 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 »).

  > Cette aide décrit comment utiliser la Console d'administration de Kaspersky Security Center 14.2 Windows.

- 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 périphérique 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 »).

Cette aide décrit comment utiliser Web Console pour Kaspersky Security Center 15.1 Linux.

- 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 Web.

  Kaspersky Security Center Cloud Console ne prend pas en charge la gestion des paramètres d'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA).

  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.

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).

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 périphériques vers les groupes d'administration. Vous pouvez également déplacer manuellement les périphériques 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 Web 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.

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 périphériques distincts dans le groupe d'administration si la modification de ces paramètres n'est pas interdite par la stratégie.

L'utilisation de profils de stratégie vous permet de configurer de manière plus flexible les paramètres de l'application. 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 sur différents périphériques. Vous pouvez créer et configurer les profils dans la section **Profils de stratégies** des propriétés d'une stratégie.

Chaque paramètre de la stratégie présente un « cadenas » , qui indique si les modifications apportées aux paramètres sont verrouillées dans les stratégies enfants et localement dans les paramètres de l'application. 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.

Les paramètres de fonctionnement de l'application changent conformément aux paramètres de la stratégie après la première application de la stratégie.

Pour plus d'informations sur les stratégies et les profils de stratégie, 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 de périphériques sont exécutées uniquement sur les périphériques sélectionnés dans les paramètres de la tâche. En cas d'ajout de nouveaux périphériques à un ensemble de périphériques 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 la documentation 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 du périphérique indiquées dans les paramètres de la tâche pour détecter les virus et les autres objets malveillants.
- **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 périphériques.
- **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 de mise à jour de la base de données Ajout de 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 pour protéger les environnements virtuels. De plus, certaines fonctionnalités de l'application ne sont pas prises en charge dans le conteneur KESL.

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.

Pour se connecter à Web Console :

1. Dans le navigateur, accédez à `<adresse Internet du Serveur d'administration>:<numéro de port>`.

   La page de connexion s'affiche.

2. 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.

3. 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.

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 la documentation 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.

  > 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. En outre, le réglage de certains paramètres n'est pas pris en charge dans le conteneur KESL.

- Exporter et importer les paramètres d'une stratégie.
- 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 **Ajouter**.

   L'Assistant de création de stratégie démarre.

4. Dans la fenêtre qui s'ouvre, sélectionnez **Kaspersky Endpoint Security 12.1 for Linux**.

Passez à l'étape suivante de l'assistant.

5. Précisez dans quel mode vous utilisez l'application Kaspersky Endpoint Security :

   - **Mode standard de protection des postes de travail et des serveurs** : l'application est utilisée pour protéger les appareils exécutant les systèmes d'exploitation Linux.

   - **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 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.

      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 **Ne pas tenir compte de l'emplacement des SVM** 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**

           Adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel le Serveur d'intégration est installé.

           Si le nom NetBIOS, localhost ou 127.0.0.1 est spécifié comme adresse, la connexion au Serveur d'intégration échoue avec une erreur.

- Port

  Port de connexion au Serveur d'intégration.

  Par défaut, le port 7271 est indiqué.

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 FQDN SVM sur une nouvelle 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 complet correspondant 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 au périphérique. Si cette option est sélectionnée, lors de la prochaine synchronisation du périphérique avec le Serveur d'administration, cette stratégie deviendra active sur le périphérique. Cette option est sélectionnée par défaut.
     - **Inactive**. Une stratégie qui n'est pas actuellement appliquée au périphérique. Si cette option est sélectionnée, la stratégie devient inactive mais reste dans le dossier **Stratégies**. Vous pouvez activer une stratégie inactive.
   - Héritage des paramètres de la stratégie :
     - **Hériter les paramètres de la stratégie parent**. Si cette option est activée, les valeurs des paramètres de la stratégie sont héritées de la stratégie de groupe de niveau supérieur et sont verrouillées. Le bouton bascule est activé par défaut.
     - **Appliquer l'héritage des paramètres pour les stratégies enfants**. Si cette option est activée, les valeurs des paramètres des stratégies enfants sont verrouillées. 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 la 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 **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. De plus, certaines fonctionnalités de l'application ne sont pas prises en charge dans le conteneur KESL.

Vous pouvez configurer les paramètres de stratégie dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la stratégie.

Paramètres de stratégie

Section	Sous-sections
Protection essentielle contre les menaces	Protection contre les menaces sur les fichiers Exclusions de la Protection contre les menaces sur les fichiers Gestion du pare-feu Protection contre les menaces Internet Protection contre les menaces réseaux
Protection avancée contre les menaces	Kaspersky Security Network Protection contre le chiffrement Détection comportementale
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
Contrôle de sécurité	Contrôle des applications Contrôle des périphériques Contrôle de l'intégrité du système Contrôle Internet
Tâches locales	Gestion des tâches Analyse des disques amovibles
Paramètres généraux	Configuration du serveur proxy Paramètres de l'application Paramètres d'analyse du conteneur Paramètres réseau Exclusions globales Paramètres de stockage
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

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.

  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. En outre, le réglage de certains paramètres n'est pas pris en charge dans le conteneur KESL.

- Exporter et importer les paramètres d'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 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 l'espace de travail, sélectionnez 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 **Kaspersky Endpoint Security 12.1 for Linux** 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 de protection des postes de travail et des serveurs** : l'application est utilisée pour protéger les appareils exécutant les systèmes d'exploitation Linux.

   - **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 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.

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 **Ne pas tenir compte de l'emplacement des SVM** 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**

  Adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel le Serveur d'intégration est installé.

  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 le nom NetBIOS, localhost ou 127.0.0.1 est spécifié comme adresse, la connexion au Serveur d'intégration échoue avec une erreur.

- **Port**

  Port de connexion au Serveur d'intégration.

  Par défaut, le port 7271 est indiqué.

b. Cliquez sur **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 FQDN SVM sur une nouvelle 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 complet correspondant 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 menaces sur les fichiers.

    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 menaces sur les fichiers.

    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. 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 l'espace de travail, sélectionnez 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 bloc 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. De plus, certaines fonctionnalités de l'application ne sont pas prises en charge dans le conteneur KESL.

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.

Paramètres de stratégie

Section	Sous-sections
Protection essentielle contre les menaces	Protection contre les menaces sur les fichiers Exclusions de la Protection contre les menaces sur les fichiers Gestion du pare-feu Protection contre les menaces Internet Protection contre les menaces réseaux
Protection avancée contre les menaces	Kaspersky Security Network Protection contre le chiffrement Détection comportementale
Detection and Response	Managed Detection and Response Endpoint Detection and Response (KATA)
Contrôle de sécurité	Contrôle des applications Contrôle des périphériques Contrôle de l'intégrité du système Contrôle Internet
Tâches locales	Gestion des tâches Analyse des disques amovibles
Paramètres généraux	Configuration du serveur proxy Paramètres de l'application Paramètres d'analyse du conteneur Paramètres réseau Exclusions globales Exclusion de mémoire de processus

	Paramètres de stockage
Mode Light Agent	Connexion au serveur d'intégration Paramètres de détection des SVM Tag de connexion à la SVM Algorithme de sélection des SVM Protection de la connexion

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. En outre, le réglage de certains paramètres n'est pas pris en charge dans le conteneur KESL.

- 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 : 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 obtenir 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 utilisateur locale sur l'appareil.

Création des tâches dans Web Console

Pour créer une tâche dans Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **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 **Kaspersky Endpoint Security 12.1 for Linux**.

   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.

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. En outre, le réglage de certains paramètres n'est pas pris en charge dans le conteneur KESL.

- 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 : 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 utilisateur locale sur l'appareil.

Création des tâches dans la Console d'administration

Pour créer une tâche 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 **Kaspersky Endpoint Security 12.1 for Linux** 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.

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 des tâches* de 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 des connexions chiffrées.
- 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*.

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 dans 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 menaces sur les fichiers*. 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 d'analyse de conteneur temporaire.

- *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.

- *Gestion de la sauvegarde*. Cette tâche offre la possibilité d'enregistrer des copies de sauvegarde des fichiers dans la sauvegarde située 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 ne peut pas être démarrée, arrêtée ou supprimée.

- *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 (KATA)*. Cette tâche vous permet d'activer ou de désactiver l'intégration avec Kaspersky Endpoint Detection and Response (KATA) et de définir les paramètres d'intégration.

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 des tâches 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 menaces sur les fichiers	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
Analyser les conteneurs	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
Analyse des disques amovibles	Removable_Drives_Scan	16	RDS
Protection contre les menaces Internet	Web_Threat_Protection	14	WTP
Protection contre les menaces réseaux	Network_Threat_Protection	17	NTP
Protection contre le chiffrement	Anti_Cryptor	13	AntiCryptor
Gestion du pare-feu	Firewall_Management	12	Firewall
Contrôle des applications	Application_Control	21	AppControl
Inventaire	Inventory_Scan	22	InventoryScan
Inventaire (personnalisé)	défini par l'utilisateur	à partir de 100	InventoryScan
Contrôle des périphériques	Device_Control	15	DeviceControl
Détection comportementale	Behavior_Detection	20	BehaviorDetection
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 de la sauvegarde	Backup	10	Backup
Mise à jour	Update	6	Update
Mise à jour (personnalisée)	défini par l'utilisateur	à partir de 100	Update
Annulation de la mise à jour	Rollback	7	Rollback
Annulation de la mise à jour (personnalisée)	défini par l'utilisateur	à partir de 100	Rollback
Licence	License	9	License
Intégration à Kaspersky Endpoint Detection and Response (KATA)	KATAEDR	24	KATAEDR
Contrôle Internet	Web_Control	26	WebControl

Vous pouvez réaliser les opérations suivantes sur les tâches :

- Démarrer et arrêter toutes les tâches prédéfinies et personnalisées, à l'exclusion des tâches de type *Backup* et *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 :

- `Nom` : 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 des tâches localement, des informations uniquement sur les tâches *Scan_File*, *Backup*, *License*, *File_Threat_Protection*, *System_Integrity_Monitoring* et *Anti_Cryptor* s'affichent. Les informations relatives aux autres tâches ne sont pas affichées.

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 <identifiant/nom de la tâche> [--json]
```

où :

- `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la 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 attribué à la nouvelle tâche ;
- `< type de tâche >` : désignation du type de tâche en cours de création.

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 < hemin
d'accès au fichier de configuration > [--json]
```

où :

- `< nom de la tâche >` est le nom attribué à la nouvelle tâche ;
- `< type de tâche >` : désignation du type de tâche en cours de création ;
- `< chemin d'accès au fichier >` : chemin d'accès complet au fichier de configuration dont les paramètres seront utilisés lors de la création de la tâche.
- `--json` : importer les paramètres 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.

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'exclusion des tâches de type *Backup* et *License*.

Vous pouvez suspendre et reprendre les types de tâches *ODS*, *ODFIM* et *InventoryScan*.

Pour lancer la tâche, exécutez la commande :

```
kesl-control --start-task < ID/nom de la tâche > [-W] [--progress]
```

où :

- `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `[-W]` : utilisez cette commande conjointement avec la commande de lancement de la tâche si vous souhaitez activer l'affichage des événements en cours liés à cette tâche.
- `[--progress]` : spécifiez cette clé si vous souhaitez afficher la progression de la tâche.

  Exemple :
  Exécutez une tâche avec l'identifiant 1 et activez l'affichage des événements en cours associés à la tâche :

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

Pour arrêter la tâche, exécutez la commande :

```
kesl-control --stop-task < identifiant/nom de la tâche > [-W]
```

où :

- `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `[-W]` : utilisez cette commande conjointement avec la commande d'arrêt de la tâche si vous souhaitez activer l'affichage des événements en cours liés à cette tâche.

Pour suspendre la tâche, exécutez la commande suivante :

```
kesl-control --suspend-task <identifiant/nom de la tâche>
```

Pour reprendre la tâche, exécutez la commande suivante :

```
kesl-control --resume-task <identifiant/nom de la tâche>
```

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 <identifiant/nom de la tâche>
```

où `<identifiant/nom de la tâche>` est l'identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur 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 <identifiant/nom de la tâche> [--json]
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `--json` : afficher 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 <identifiant/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

- `--file <chemin d'accès au fichier de configuration>` : chemin d'accès au fichier de configuration dans lequel les paramètres de la tâche seront affichés. 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 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 de la tâche 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 d'une tâche à l'aide de clés de la 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 vérifier. 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 `[ExclusiveFromScanScope.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 exclus. 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 <identifiant/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]`

   où :

   - `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

- `--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres de la tâche vont être 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 clés 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 <identifiant/nom de la tâche> <nom du paramètre>=<valeur du paramètre> [<nom du paramètre>=<valeur du paramètre>]
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

- `<nom du paramètre>=<valeur du paramètre>` : nom et 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 <identifiant/nom de la tâche> --add-path <chemin d'accès>
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `--add-path <chemin d'accès>` : ajouter le chemin d'accès au répertoire contenant les objets en cours d'analyse.

  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 <identifiant/nom de la tâche> --del-path <chemin d'accès>
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `--del-path <chemin d'accè>` : supprimer le chemin d'accès au répertoire contenant les objets en cours d'analyse.

  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 <identifiant/nom de la tâche> --add-exclusion <chemin d'accès>
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `--add-exclusion <chemin d'accès>` : ajouter le chemin d'accès au 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 de l'analyse 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 <identifiant/nom de la tâche> --del-exclusion <chemin d'accès>
```

où :

- `<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- `--del-exclusion <chemin d'accès>` : chemin d'accès au répertoire contenant les objets exclus

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 <identifiant/nom de la tâche> --set-to-default
```

où < identifiant/nom de la tâche > est l'identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur 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 <identifiant/nom de la tâche> [--json]
```

où :

- < identifiant/nom de la tâche > : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- --json : afficher 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 <identifiant/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

où :

- < identifiant/nom de la tâche > : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.
- --file <chemin d'accès au fichier de configuration> : chemin d'accès au fichier de configuration dans lequel les paramètres de planification des tâches seront affichés. 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 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.
- Utiliser la ligne de commande pour définir les paramètres individuels de planification de lancement de tâches 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 < identifiant/nom de la tâche > --file < chemin d'accès au fichier de configuration > [--json]`

   où :

   `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

   `--file < chemin d'accès au fichier de configuration >` : chemin complet vers le fichier de configuration à partir duquel les paramètres de planification des tâches 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 < identifiant/nom de la tâche > < nom du paramètre >=< valeur du paramètre > [< nom du paramètre >=< valeur du paramètre >]`

où :

- `< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

- < nom du paramètre >=< valeur du paramètre > : nom et valeur de l'un des paramètres de planification des tâches.

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 les paramètres généraux de l'application à partir de 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.
- Modifier les paramètres généraux de l'application à l'aide d'un fichier de configuration contenant tous les paramètres généraux ou des clés de la 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 la tâche.

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` : 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>` : chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'application seront affichés. 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 paramètres au format JSON. Si vous ne spécifiez pas le commutateur `--json`, les paramètres seront affichés au format INI.

  Exemple :
  Générez les paramètres généraux de l'application dans un fichier nommé kesl_config.ini. Enregistrez le fichier créé dans le répertoire actif :
  ```
  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 de commutateurs 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>` : chemin d'accès complet au fichier de configuration avec les paramètres généraux de l'application.
   - `--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>` est le nom et 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 trace :

```
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> <opération de comparaison> '<valeur>'"`

`"<champ> <opération de comparaison> '<valeur>' et <champ> <opération de comparaison> '<valeur>'"`

où :

- < `field` > : nom du champ de la base de données.
- < `opération de comparaison` > : une des opérations de comparaison suivantes :
  - > : supérieur à.
  - < : inférieur à.
  - `like` : correspond à la valeur spécifiée. Lors de la spécification d'une valeur, vous pouvez utiliser des masques %, par exemple : l'expression logique "FileName like '%etc%'" spécifie la limite "contient le texte "etc" dans le champ FileName".
  - == : égal à.
  - != : pas égal à.
  - >= : supérieur ou égal à
  - <= : inférieur ou égal à
- < `valeur` > : 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 des informations sur certains événements de l'application en cours :

  `kesl-control -W --query "< conditions du filtre >"`
- Afficher des informations sur des événements spécifiques de l'application dans le journal des événements :

  `kesl-control -E --query "< conditions du filtrage >"`
- Afficher des informations sur certains objets dans la sauvegarde :

  `kesl-control -B --query "< conditions du filtrage >"`
- Suppression des objets spécifiques de la sauvegarde :

  `kesl-control -B --mass-remove --query "< conditions du filtre >"`

  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 prédifinie 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 périphériques utilisateurs. Lorsque vous exportez les paramètres, tous les paramètres de l'application (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) 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>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres de l'application seront enregistrés.
- `--json` : exporter les paramètres vers un 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>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés dans l'application.
- `--json` : importer les paramètres 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.

Lors de l'importation de paramètres du fichier, les paramètres `UseKSN` et `CloudMode` reçoivent la valeur `No`. 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.

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.

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, 4 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 de rôles correspondant (voir le tableau *Rôles* ci-dessous). Quand vous retirez un rôle à un utilisateur, cet utilisateur est retiré du groupe rôle 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*.

Rôles utilisateur

Nom du rôle	Rôle dans l'application	Utilisateur du système d'exploitation	Autorisations
Administrateur	admin	kesladmin	Gestion des paramètres de l'application et des paramètres des tâches. Gérer les licences d'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.
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 menaces sur les fichiers.
- 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 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 périphériques administrés s'affiche.

2. Dans la liste, sélectionnez le périphérique sur lequel vous souhaitez démarrer ou arrêter l'application, puis cliquez sur le lien portant le nom du périphérique pour ouvrir la fenêtre des propriétés de ce dernier.
3. Sélectionnez l'onglet **Applications**.
4. Cochez la case en regard de l'application **Kaspersky Endpoint Security 12.1 for Linux**.
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 Internet **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 périphérique 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 périphériques administrés, sélectionnez le périphérique sur lequel vous voulez démarrer ou arrêter l'application, puis dans le menu contextuel du périphérique, choisissez l'option **Propriétés**.
4. Dans la fenêtre **Propriétés : <Nom du périphérique>**, choisissez la section **Applications**.

   Une liste des applications de Kaspersky installées sur le périphérique s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez l'application **Kaspersky Endpoint Security 12.1 for Linux**.
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 dump 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 sécurité de l'appareil et les paramètres 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.

- Dans la ligne de commande à l'aide de la commande `kesl-control --app-info`. La commande affiche des informations sur le fonctionnement de l'application et l'état des modules fonctionnels et des tâches de l'application.

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 périphériques 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 gérés, et dans la fenêtre qui s'ouvre, sélectionnez un groupe d'administration.

   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 du périphérique 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 du périphérique 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 le périphérique sélectionné.
- **Virus détectés** : nombre total d'objets malveillants détectés sur le périphérique 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 périphérique.
- **État de la protection en temps réel** : état actuel de la protection contre les menaces sur les fichiers 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 périphériques 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 de Kaspersky installées sur l'appareil, cliquez sur le nom de l'application **Kaspersky Endpoint Security 12.1 for Linux**.

   La fenêtre des propriétés de l'application s'ouvrira.

La fenêtre **Kaspersky Endpoint Security 12.1 for Linux** affiche les informations suivantes sur 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 menaces sur les fichiers sur l'appareil, par exemple *En cours* ou *Suspendu*.
  - Le groupe **Mises à jour installées** contient les informations sur la mise à jour des modules de 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 de la base 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 composant, 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**, dans la section **Detection and Response**, vous pouvez gérer l'isolation réseau de l'appareil.

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 le périphérique s'affiche dans la partie droite de la fenêtre.
5. Sélectionnez l'application **Kaspersky Endpoint Security 12.1 for Linux** et ouvrez la fenêtre des propriétés de l'application en double-cliquant ou en utilisant le bouton **Propriétés** en bas de la fenêtre.

   La fenêtre **Paramètres de Kaspersky Endpoint Security 12.1 for Linux** s'ouvre.

La fenêtre **Paramètres de Kaspersky Endpoint Security 12.1 for Linux** affiche les informations suivantes sur Kaspersky Endpoint Security :

- La section **Général** contient des informations générales sur l'application installée :
  - **Numéro de version** : numéro de la 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 menaces sur les fichiers 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** : liste des modules dont les mises à jour ont été installées.
- **Bases de l'application** : date et heure de publication de la mise à jour de la base de données de l'application.

- La section **Composants** contient une liste de tâches prédéfinies. Pour chaque composant, 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 active et la clé de licence :

  - **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.

- 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 **Additionnel** 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 suivante :

```
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**. 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 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.
- **Informations sur la licence EDR Optimum**. Informations sur la licence sous laquelle la fonctionnalité Kaspersky Endpoint Detection and Response Optimum est utilisée ou sur l'état de la clé de licence EDR Optimum.
- **État de l'abonnement**. État de l'abonnement. Ce champ apparaît si l'application est exécutée sous un abonnement.
- **Date d'expiration de la licence de l'application**. Date et heure de fin de validité de la licence de l'application au format UTC.
- **Date d'expiration de la licence** de **EDR Optimum**. Date et heure d'expiration de la licence d'utilisation de la fonctionnalité Kaspersky Endpoint Detection and Response Optimum au format UTC.
- **État du fichier MDR BLOB**. État du fichier de configuration BLOB pour l'intégration avec Kaspersky Managed Detection and Response.
- **Date d'expiration de la licence MDR BLOB**. Date et heure de fin de validité de la licence d'utilisation de Kaspersky Managed Detection and Response au format UTC.
- **État de la sauvegarde**. 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.
- **Utilisation de Kaspersky Security Network**. Informations sur l'utilisation de Kaspersky Security Network : `Mode avancé KSN`, `Mode standard KSN` ou `Désactivé`.
- **Mode Light Agent pour protéger les environnements virtuels**. Informations indiquant que l'application est utilisée en mode Light Agent pour protéger les environnements virtuels. Si l'application est utilisée en mode standard, la ligne ne s'affiche pas.
- La **désinfection et suppression des fichiers sont désactivées**. Informations indiquant que le mode de fonctionnement de l'application est activé, dans lequel la désinfection et la suppression des fichiers sur le disque ne sont pas effectuées, quels que soient les paramètres configurés dans les propriétés de la stratégie.
- **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 menaces sur les fichiers**. État de la protection contre les menaces de fichiers en temps réel.
- **Surveillance du conteneur**. État de l'analyse du conteneur en temps réel.
- **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 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 (KATA)**. État d'intégration avec Kaspersky Endpoint Detection and Response (KATA)
- **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 dump. Ce champs s'affiche quand un échec est survenu au lancement antérieur de l'application.

Activation des applications et gestion des clés de licence

L'*activation* est le processus 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.

La procédure d'activation de l'application Kaspersky Endpoint Security consiste à ajouter une clé de licence active de l'application.

Si vous utilisez l'application sous une licence qui n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, pour activer cette fonctionnalité, vous devez ajouter une clé de licence supplémentaire de Kaspersky Endpoint Detection and Response Optimum Add-on (ci-après, la "clé EDR Optimum").

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 séparément. Vous activez Kaspersky Security for Virtualization Light Agent. L'activation s'effectue du côté du Serveur de protection (un module de Kaspersky Security for Virtualization Light Agent) en ajoutant une clé de licence à la SVM. Pour activer la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, vous devez également ajouter la clé EDR Optimum à la SVM.

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

- À distance via Kaspersky Security Center :
  - Lors de l'installation de l'application Kaspersky Endpoint Security. Vous pouvez ajouter une clé de licence au paquet d'installation. L'application sera activée automatiquement après l'installation.
  - Après l'installation de l'application Kaspersky Endpoint Security. Vous pouvez ajouter une clé de licence à une application à l'aide de la tâche d'activation de l'application ou en distribuant une clé de licence située sur le Serveur d'administration aux appareils clients.
- En utilisant la ligne de commande :
  - Lors de la configuration initiale de l'application Kaspersky Endpoint Security.
  - Après l'installation de l'application Kaspersky Endpoint Security. Vous pouvez ajouter et supprimer des clés de licence à l'aide des commandes de gestion.

Vous pouvez également 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.

La clé de réserve ne peut être ajoutée qu'après l'ajout de la clé de licence active.

Vous pouvez afficher des informations sur les clés de licence ajoutées à l'appareil :

- À distance dans Web Console ou dans la Console d'administration. Dans les propriétés de l'application sur l'appareil client, dans la section **Clés de licence**, des informations sur les clés actives et de réserve sont affichées.
- Sur la ligne de commande à l'aide des commandes de gestion.

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 réserve 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 la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, les informations sur les clés de licence EDR Optimum actives et réservées et la licence EDR Optimum s'affichent également.

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 active de l'application, si la clé a été ajoutée :
  - La date et l'heure d'expiration de la licence sous laquelle l'application est utilisée.
  - Le nombre de jours avant l'expiration 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 réserve de l'application. 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 protéger des environnements virtuels, les informations sur la clé de réserve ne s'affichent pas ; la clé de réserve est ajoutée à la SVM.
  - La date et l'heure d'expiration de la licence sous laquelle l'application est utilisée.
  - Le nombre de jours avant l'expiration 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.
- Date d'activation.

- Informations sur la clé EDR Optimum active, si la clé a été ajoutée :
  - La date et l'heure d'expiration de la licence sous laquelle la fonctionnalité Kaspersky Endpoint Detection and Response Optimum a été activée.
  - 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 réserve EDR Optimum. Affiché si l'application est utilisée en mode standard et qu'une clé de réserve EDR Optimum a été ajoutée. Si l'application est utilisée en mode Light Agent pour protéger des environnements virtuels, les informations sur la clé de réserve ne s'affichent pas ; la clé de réserve est ajoutée à la SVM.
  - La date et l'heure d'expiration de la licence sous laquelle la fonctionnalité Kaspersky Endpoint Detection and Response Optimum a été activée.
  - 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.
  - Date d'activation.

Gestion des clés de licence dans la ligne de commande

Pour gérer les clés de licence sur un appareil, vous pouvez utiliser les commandes de gestion des clés de licence.

Avec ces commandes, vous pouvez ajouter à la fois des clés de licence de l'application et des clés de licence EDR Optimum. Vous n'avez pas besoin de spécifier le type de clé dans les commandes.

Les commandes de gestion des clés de licence ne peuvent être exécutées que si l'application est utilisée en mode standard. 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.

Pour supprimer une clé active de l'application, exécutez la commande suivante :

```
kesl-control [-L] --remove-active-key
```

Pour supprimer la clé de réserve de l'application, exécutez la commande suivante :

```
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
```

Mise à jour des bases et des modules de l'application

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, 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 périphérique 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 le périphérique.

Si les bases de données sont complètement périmées, le paquet de mise à jour peut être volumineux, ce qui pourrait provoquer du trafic Internet complémentaire (jusqu'à plusieurs 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*.

L'application crée une tâche prédéfinie *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.

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, 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 Web 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.
- Sélectionnez le mode de téléchargement et d'installation des modules de l'application et des mises à jour de versions de l'application : télécharger et installer, télécharger uniquement ou ne pas télécharger.
- 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.

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 le périphérique :

- 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.

  Les bases de données sont à jour si elles ont été téléchargées il y a moins de trois jours. Par défaut, l'application génère l'événement *Les bases sont dépassées* (*BasesAreOutOfDate*) 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 ne sont pas mises à jour dans un délai de sept jours, l'application génère l'événement *Les bases sont fortement dépassées* (*BasesAreTotallyOutOfDate*).

- 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 du périphérique. Les mises à jour des modules peuvent modifier le comportement des composants de l'application et ajouter de nouvelles fonctionnalités.

  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. Après la mise à jour, il faut redémarrer Kaspersky Endpoint Security.

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.

Après la mise à jour de la version de l'application à l'aide d'un correctif automatique, le mécanisme d'interaction avec le pare-feu du système d'exploitation change : les règles sont gérées à l'aide des utilitaires système iptables et iptables-restore.

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 mise 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.

L'application Kaspersky Endpoint Security prend en charge les scénarios suivants pour la mise à jour des bases antivirus et des modules de l'application :

- 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 réduit le trafic Internet externe et permet une surveillance pratique de la procédure.

  La mise à jour centralisée comprend les étapes suivantes :

  1. Téléchargez le paquet de mise à jour dans un 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 périphériques clients.

     Le paquet de mise à jour est distribué aux périphériques clients via *tâche de mise à jour* de Kaspersky Endpoint Security. Dans les paramètres de la tâche, vous devez sélectionner le Serveur d'administration de Kaspersky Security Center comme source de mise 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 des 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

La procédure de mise à jour des bases et des modules de l'application de Kaspersky Endpoint Security dépend du mode d'utilisation de l'application. Cette section décrit comment mettre à jour une application en mode standard. Si l'application est utilisée en mode Light Agent pour protéger les environnements virtuels, 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. La mise à jour est effectuée à l'aide d'une tâche prédéfinie locale.

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 tâches, sélectionnez l'onglet **Paramètres de l'application** et sélectionnez la section **Sources de mises à jour** dans la liste à droite.

5. 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.

   Si vous gérez l'application à l'aide de Web Console, la liste des sources de mise à jour contient les serveurs de mise à jour de Kaspersky et le Serveur d'administration de Kaspersky Security Center. Si vous gérez une application à l'aide de Kaspersky Security Center Cloud Console, la liste des sources de mise à jour contient les serveurs de mise à jour et les points de distribution de Kaspersky (pour plus d'informations sur les points de distribution, consultez l'aide de Kaspersky Security Center). Vous pouvez ajouter d'autres sources de mise à jour à la liste.

Vous pouvez générer une liste de sources de mise à jour en sélectionnant l'option **Autres sources sur le réseau local ou global**. Vous pouvez désigner des serveurs FTP, HTTP ou HTTPS en tant que sources de 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. L'application s'adresse aux sources de mises à jour dans l'ordre où celles-ci apparaissent dans le tableau.

6. Accédez à 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 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.

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
Sources de mise à jour	Dans ce groupe, vous pouvez sélectionner la source des 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** : le Serveur d'administration de Kaspersky Security Center (cette option est disponible uniquement pour Web Console). • **Points de distribution** (cette option est disponible uniquement pour Kaspersky Security Center Cloud Console). • **Autres sources sur le réseau local ou sur Internet** : serveurs HTTP, HTTPS ou FTP ou répertoires sur les serveurs de réseau local.
Utiliser les serveurs de mise à jour Kaspersky si les autres sources sont inaccessibles	Cette case active ou désactive l'utilisation des serveurs de mise à jour Kaspersky comme sources de mises à jour si les sources de mises à jour sélectionnées ne sont pas accessibles. La case est disponible si dans le groupe **Sources de mise à jour** l'option **Autres sources sur le réseau local ou sur Internet** ou **Kaspersky Security Center** est cochée. Cette case est cochée par défaut.
Sources personnalisées de mises à jour	Le tableau contient la liste des sources de mises à jour des bases de données personnalisées. 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** reprend les serveurs HTTP, HTTPS ou FTP ou les répertoires sur les serveurs de réseau local. • Le bouton bascule indique si la source est utilisée dans la tâche (**Activé** ou **Désactivé**). Vous pouvez activer ou désactiver le bouton bascule dans le tableau, et cocher ou décocher la case **Utiliser cette source** dans la fenêtre **Source des mises à jour**, qui s'ouvre lorsque vous cliquez sur le lien portant le nom de la source). Ce tableau est accessible si l'option **Autres sources sur le réseau local ou sur Internet** a été sélectionnée.

Par défaut, le tableau est vide.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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 comment télécharger les mises à jour de l'application : • **Ne pas télécharger** les mises à jour. Si cet élément de liste est sélectionné, l'application ne peut pas être mise à jour. • **Télécharger seulement** les mises à jour, sans les installer sur les appareils clients (valeur par défaut). • **Télécharger et installer** les mises à jour sur les appareils clients. Après avoir installé les mises à jour, l'application redémarrera automatiquement.

	Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

Mise à jour des bases de données et des modules de l'application dans la Console d'administration

La procédure de mise à jour des bases et des modules de l'application de Kaspersky Endpoint Security dépend du mode d'utilisation de l'application. Cette section décrit comment mettre à jour une application en mode standard. Si l'application est utilisée en mode Light Agent pour protéger les environnements virtuels, 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. La mise à jour est effectuée à l'aide d'une tâche prédéfinie locale.

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 tâches, ouvrez la liste de gauche et sélectionnez l'option **Sources des mises à jour**.
4. 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 mise à jour contient les serveurs de mise à jour Kaspersky et le Serveur d'administration de Kaspersky Security Center. Vous pouvez ajouter d'autres sources de mise à jour à la liste.

   Vous pouvez générer une liste de sources de mise à jour en sélectionnant l'option **Autres sources sur le réseau local ou global**. Vous pouvez désigner des serveurs FTP, HTTP ou HTTPS en tant que sources de 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. 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
Sources de mise à jour	Dans ce groupe, vous pouvez sélectionner la source des 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** : serveurs HTTP, HTTPS ou FTP ou répertoires sur les serveurs de réseau local.
Utiliser les serveurs de mise à jour Kaspersky si les autres sources sont inaccessibles	Cette case active ou désactive l'utilisation des serveurs de mise à jour Kaspersky comme sources de mises à jour si les sources de mises à jour sélectionnées ne sont pas accessibles. La case est disponible si dans le groupe **Sources de mise à jour** l'option **Autres sources sur le réseau local ou sur Internet** ou **Kaspersky Security Center** est cochée. Cette case est cochée par défaut.
Sources personnalisées de mises à jour	Le tableau contient la liste des sources de mises à jour des bases de données personnalisées. 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** reprend les serveurs HTTP, HTTPS ou FTP ou les répertoires sur les serveurs de réseau local. • **État** indique si la source 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**. Ce tableau est accessible si l'option **Autres sources sur le réseau local ou sur Internet** a été sélectionnée. 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Par défaut, le tableau est vide.

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	Dans la liste déroulante, vous pouvez sélectionner comment télécharger les mises à jour de l'application : • **Ne pas télécharger** les mises à jour. Si cet élément de liste est sélectionné, l'application ne peut pas être mise à jour. • **Télécharger seulement** les mises à jour, sans les installer sur les appareils clients (valeur par défaut). • **Télécharger et installer** les mises à jour sur les appareils clients. Après avoir installé les mises à jour, l'application redémarrera automatiquement. Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

Mise à jour des bases de données et des modules de l'application dans la ligne de commande

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.

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 Mise à jour (*Update*) prédéfinie. 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 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 mise à jour

Paramètre	Description	Valeurs
`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 périphériques au sein de votre entreprise. `Custom` : l'application charge les mises à jour à partir d'une source personnalisée reprise dans la section `[CustomSources.item_#]`. Vous pouvez désigner les répertoires des serveurs HTTP, HTTP ou FTP ainsi que tous les répertoires sur tout périphérique monté sur le périphérique client protégé, y compris les répertoires des périphériques distants montés via les protocoles Samba ou NFS.
`UseKLServersWhenUnavailable`	L'application contactera les serveurs de mise à jour de Kaspersky si aucune source	`Yes` (valeur par défaut) : l'application se connecte aux serveurs de mise à jour de Kaspersky si aucune source de mise à jour personnalisée n'est disponible.

	personnalisée n'est disponible.	`No` : l'application ne se connecte pas aux serveurs de mise à jour de Kaspersky si toutes les sources de mise à jour personnalisées sont inaccessibles.
`ApplicationUpdateMode`	Mode de téléchargement et d'installation des mises à jour de l'application.	`Disabled` : ne télécharge et n'installe pas les mises à jour de l'application. `DownloadOnly` (valeur par défaut) : télécharge les mises à jour de l'application, mais ne les installe pas. `DownloadAndInstall` : télécharge et installe automatiquement les mises à jour de l'application. Après avoir installé les mises à jour, l'application redémarrera automatiquement.
`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.
La section **[CustomSources.item_#]** contient les paramètres suivants :		
`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 le périphérique protégé.
`Enabled`	Utilisation de la source de mises à jour spécifiée via le paramètre `URL`. Pour exécuter la tâche, il faut activer l'utilisation d'au moins une source de mise à jour.	`Oui` : l'application utilise une source des mises à jour. `No` : l'application n'utilise pas la source des mises à jour. La valeur par défaut n'est pas définie.

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 périphériques du réseau local de l'organisation à partir d'un répertoire partagé à l'aide de Kaspersky Update Utility. Pour ce faire, un des périphériques 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 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 en savoir plus sur l'utilisation de Kaspersky Update Utility, consultez la base de connaissances de Kaspersky.

3. Configurez les mises 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**.

4. 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 doit correspondre à l'adresse renseignée dans les paramètres de Kaspersky Update Utility.

5. Cochez la case **Utiliser cette source**, puis cliquez sur **OK**.

6. Dans le tableau des sources de mise à jour, définissez l'ordre d'utilisation à l'aide des boutons **Haut** et **Bas**.

7. Enregistrez les modifications apportées aux paramètres de la tâche.

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 restaurer les bases de données vers une version précédente, 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 (Rollback)* ou créer et lancer des tâches personnalisées d'annulation de mise à jour (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 menaces sur les fichiers

Le module Protection contre les menaces sur les fichiers permet d'éviter l'infection du système de fichiers de l'appareil. Le module démarre automatiquement avec les paramètres par défaut au démarrage de Kaspersky Endpoint Security, s'exécute dans la mémoire principale de l'appareil et analyse tous les fichiers ouverts, enregistrés et lancés en temps réel.

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 la protection contre les menaces sur les fichiers est activée et la Surveillance du conteneur 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 menaces sur les fichiers, ainsi que configurer les paramètres de 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 qui doivent être remplies pour que l'application ne recherche pas de virus et autres applications malveillantes dans les objets. 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.
- 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 menaces sur les fichiers, 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 `paramètres de la tâche` de type OAS.

Configuration de la protection contre les menaces de fichiers dans Web Console

Dans Web Console, vous pouvez gérer la protection contre les menaces sur les fichiers dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection de base**→ **Protection contre les menaces sur les fichiers**).

Paramètres du module Protection contre les menaces sur les fichiers

Paramètre	Description
Protection contre les menaces sur les fichiers activée / désactivée	Le commutateur active ou désactive le module Protection contre les menaces sur les fichiers sur tous les appareils administrés. Le bouton bascule est activé par défaut.
Mode de la Protection contre les menaces sur les fichiers	Cette liste déroulante permet de sélectionner le mode de fonctionnement du module Protection contre les menaces sur les fichiers : • **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.
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Bloquer** l' accès à l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde.

	• **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Bloquer** l'accès à l'objet (valeur par défaut).
Zones d'analyse	Cliquez sur le lien **Configurer les zones d'analyse** pour ouvrir la fenêtre **Zones de protection**.
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 de l'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)**. Si la case est décochée, l'application 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 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 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, 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 les fichiers texte	Exclusion temporaire de l'analyse des fichiers au format texte. Si la case est cochée, l'application 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 la case n'est pas cochée, l'application analyse les fichiers texte. 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 : `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`, 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 *ObjectProcessed* dans le journal. Si cette case est cochée, l'application enregistre les événements *ObjectProcessed* dans le journal pour tout objet analysé. Si la case est décochée, l'application n'enregistre pas l'événement dans le journal. La case est décochée par défaut.
Journaliser les objets non traités	Cette case active ou désactive l'enregistrement des événements *ObjectNotProcessed* dans le journal si un fichier ne peut pas être traité pendant l'analyse. Si cette case est cochée, l'application enregistre l'événement *ObjectNotProcessed* dans le journal. Si la case est décochée, l'application n'enregistre pas l'événement dans le journal. La case est décochée par défaut.
Journaliser les objets compactés	Cette case active ou désactive l'enregistrement des événements *PackedObjectDetected* dans le journal pour tout objet compacté détecté. Si cette case est cochée, l'application enregistre l'événement *PackedObjectDetected* dans le journal. Si la case est décochée, l'application n'enregistre pas l'événement 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. Cette case est cochée par défaut.
Utiliser l'analyse heuristique	Cette case active ou désactive l'utilisation de l'analyse heuristique lors de l'analyse d'un objet. Cette 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 serveurs protégés.

Fenêtre Zones de protection

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 de protection reprenant tous les répertoires du système de fichiers local.

Paramètres de la zone de protection

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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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 d'ajout d'une zone de protection

Cette fenêtre permet d'ajouter ou de configurer une nouvelle zone de protection.

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. Si cette case est décochée, l'application ne traite pas cette zone de protection pendant le fonctionnement. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement de l'application en cochant la case. Cette 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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
Chemin	Champ de saisie du chemin du répertoire à inclure dans la zone de protection. 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 :<identifiant>]/<chemin d'accès au répertoire local>`
- `[container-name <nom>]/<chemin d'accès au répertoire local>`
- `[image-id:<identifiant>]/<chemin d'accès au répertoire local>`
- `[image-name:<nom>]/<chemin d'accès au répertoire local>`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id:<identifiant>]`, `[container-name:<nom>]`, `[image-id:<identifiant>]` et `[image-name:<nom>]/<chemin d'accès au répertoire local>`.

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:<nom>][image-name:<nom>]/<chemin d'accès au répertoire local>`
- `[container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>`
- `[image-name:<nom>][image-id :<identifiant>]/<chemin d'accès au répertoire local>`
- `[container-name:<nom>][container-id :<identifiant>][image-name :<nom>]/<chemin d'accès au répertoire local>`
- `[container-name:<nom>][image-id:<identifiant>][container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 de protection. 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Exclusions de la Protection contre les menaces sur les fichiers

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 la protection en fonction des masques et noms de menaces et configurer des exclusions pour les processus.

Dans Web Console, vous pouvez configurer les exclusions de la Protection contre les menaces sur les fichiers dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection de base**→ **Exclusions de la Protection contre les menaces sur les fichiers**).

Paramètres des exclusions de la protection

Paramètre	Description
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 la protection.
Exclusions d'après le 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.
Exclusions d'après le nom de la 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.
Exclusions par processus	Cliquez sur le lien **Configurer les exclusions par processus** pour ouvrir 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

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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 le périphérique. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Fenêtre Exclusions par processus

Le tableau 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, le tableau 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
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.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Processus de confiance

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion basée sur le processus	Champ de saisie du nom de la zone d'exclusion basée sur le processus. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**. Le champ de saisie ne peut être vide.
Utiliser/Ne pas utiliser	Ce commutateur active ou désactive l'exclusion de cette zone pendant le fonctionnement de l'application.

cette exclusion	Le bouton bascule est activé par défaut.
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.
Chemin d'accès au processus exclu	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse.
Système de fichiers, protocole d'accès et chemin	Le bloc 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. • **Monté** : répertoires montés. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique indiquées dans le champ ci-après. La liste déroulante **Protocole d'accès** est accessible si vous avez choisi le type **Monté** dans la liste déroulante des systèmes de fichiers.
Chemin	Dans le champ de saisie, vous pouvez indiquer le chemin du répertoire que vous souhaitez ajouter 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. 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 spécifié dans la section **Système de fichiers, protocole d'accès et chemin**. La liste contient par défaut le masque * (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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).

Configuration de la protection contre les menaces de fichiers dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer la protection contre les menaces sur les fichiers dans les propriétés de la stratégie (**Protection de base** → **Protection contre les menaces sur les fichiers**).

Paramètres du module Protection contre les menaces sur les fichiers

Paramètre	Description
Activer la Protection contre les menaces sur les fichiers	La case active ou désactive le module Protection contre les menaces sur les fichiers sur tous les appareils administrés. Cette case est cochée par défaut.
Mode de la Protection contre les menaces sur les fichiers	Cette liste déroulante permet de sélectionner le mode de fonctionnement du module Protection contre les menaces sur les fichiers : • **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.
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.
Action en cas de détection d'une menace	Le groupe de paramètres contient le bouton **Configurer** qui permet d'ouvrir la fenêtre Action en cas de détection d'une menace pour configurer les actions que l'application doit exécuter sur tout objet infecté détecté.

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
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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Paramètres d'analyse

Cette fenêtre permet de configurer les paramètres d'analyse des fichiers pendant le fonctionnement 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.
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	Champ dans lequel vous pouvez indiquer la taille maximale d'un fichier à analyser en

fichier si sa taille est supérieure à (Mo)	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. Cette 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. Cette 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 périphériques protégés.

Fenêtre Action 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
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Bloquer** l' accès à l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Bloquer** l'accès à l'objet (valeur par défaut).

Exclusions de la Protection contre les menaces sur les fichiers

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 la protection en fonction des masques et noms de menaces et configurer des exclusions pour les processus.

Dans la Console d'administration, vous pouvez configurer les exclusions de la Protection contre les menaces sur les fichiers dans les propriétés de la stratégie (**Protection de base→ Exclusions de la Protection contre les menaces sur les fichiers**).

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion de l'analyse.
Exclusions	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la

d'après le masque	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**. Cliquez sur celui-ci pour ouvrir 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

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Fenêtre Exclusions par processus

Le tableau 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, le tableau 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
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.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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	Chemin d'accès complet au processus que vous souhaitez exclure de l'analyse.

d'accès au processus exclu	
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. Cette case est cochée par défaut.
Chemin d'accès aux fichiers modifiés	Le bloc 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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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/*/fichier` ou `/dir/*/*/fichier`.

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/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.

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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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).

Configuration de la protection contre les menaces de fichiers dans 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 préinstallée de protection contre les menaces sur les fichiers (*File_Threat_Protection*).

La tâche Protection contre les menaces sur les fichiers 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 menaces sur les fichiers à partir de la ligne de commande.

Vous pouvez configurer les paramètres de protection contre les menaces sur les fichiers en modifiant les paramètres de la tâche préinstallée Protection contre les menaces sur les fichiers.

Paramètres de la tâche de protection contre les menaces sur les fichiers

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir pour la tâche Protection contre les menaces sur les fichiers.

Paramètres de la tâche de protection contre les menaces sur les fichiers

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` : analyse les archives. Si la valeur `FirstAction=Recommended` est spéc alors, en fonction du type d'archive, l'application supprime soit l'objet infect soit l'archive entière contenant la mena `No` (valeur par défaut) : n'analyse pas le archives.
`ScanSfxArchived`	Activation de l'analyse uniquement	`Yes` : analyse les archives autoextractib

	des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`No` (valeur par défaut) : n'analyse pas le 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 le fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniqu format texte. `No` (valeur par défaut) : n'analyse pas le messages électroniques au format text
`SkipPlainTextFiles`	Exclusion temporaire de l'analyse des fichiers au format texte. Si la valeur de ce paramètre est `SkipPlainTextFiles=Yes`, l'application n'analysera pas les fichiers texte qui ont été à nouveau utilisés 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.	`Yes` : n'analyse pas les fichiers au forma texte si ceux-ci ont été à nouveau utilis par ce même processus au cours des 1 minutes suivant la dernière analyse. `No` (valeur par défaut) : analyse les fich 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 limitée. Valeur par défaut : 60.
`FirstAction`	Sélection de la première action que l'application va exécuter sur les objets infectés.	`Disinfect` (désinfecter) : l'application tente de désinfecter un objet en enregistrant une copie dans la sauvega Si la désinfection échoue, par exemple, type de l'objet ou le type de la menace l'objet ne peut pas être désinfecté, l'application garde l'objet intact. Si la va de la première action est `Disinfect (Désinfecter)`, il est recommandé de définir une deuxième action via le paramètre `SecondAction`. `Remove` (supprimer) : l'application supp l'objet infecté après avoir créé au préal sa copie de sauvegarde.

		`Recommended` (exécution de l'action recommandée) : l'application sélectionr exécute automatiquement une action s l'objet en fonction des informations rel à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime automatiquement les chevau Troie car ils ne s'intègrent pas à d'autre fichiers et par conséquent, ils n'ont pas besoin d'être désinfectés. `Block` (bloquer) : l'application bloque l'a à un objet infecté. Les informations sur l'objet infecté sont conservées dans le journal. Valeur par défaut : `Recommended`.
`SecondAction`	Sélection de la deuxième action exécutée par l'application sur les objets infectés. L'application exécute la deuxième action si la première échoue.	Les valeurs du paramètre `SecondActi` sont identiques à celles du paramètre `FirstAction`. Si l'option `Block` ou `Remove` est sélectionnée en tant que première acti n'est pas nécessaire d'en choisir une deuxième. Dans les autres cas, il est recommandé d'indiquer deux actions. S vous n'avez pas défini une deuxième ac l'application exécute l'action `Block` (bloquer) en tant que deuxième action. Valeur par défaut : `Block`.
`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 défir le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le param `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=eicar`
		`ExcludeMasks.item_0001=eicar`

`UseExcludeThreats`	Activation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets cont les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les mena 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.	La valeur du paramètre est sensible à la casse. La valeur par défaut n'est pas définie. Exemple : `UseExcludeThreats=Yes`

	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/.
		`ExcludeThreats.item_0000=EIC`
		`Test-*`
		`ExcludeThreats.item_0001=?`
		`rojan.Linux`

`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 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 ob des archives. `No` (valeur par défaut) : n'enregistre pas 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 tr `No` (valeur par défaut) : n'enregistre pas 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'analys heuristique `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique.	`Light` : analyse la moins minutieuse av une charge minimale sur le système. `Medium` : niveau de l'analyse heuristiqu normal avec une charge équilibrée sur l système d'exploitation.

	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.	`Deep` : analyse la plus minutieuse avec charge maximale sur le système d'exploitation. `Recommander` (valeur par défaut) : vale recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisat de la technologie iChecker. `No` : désactive l'utilisation de la technol iChecker.
`ScanByAccessType`	Mode de fonctionnement de la tâche Protection contre les menaces sur les fichiers. Le paramètre `ScanByAccessType` s'applique seulement à la tâche de protection contre les menaces sur les fichiers.	`SmartCheck` (valeur par défaut) : analy fichier en cas de tentative d'ouverture l'analyse à nouveau en cas de tentative fermeture s'il a été modifié. Si un proce lors de son fonctionnement accède plusieurs fois à un fichier et le modifie, l'application analyse à nouveau le fichie uniquement lorsque le processus le fer pour la dernière fois. `OpenAndModify` : analyse le fichier en de tentative d'ouverture et l'analyse à nouveau en cas de tentative de fermet s'il a été modifié. `Open` : analyse le fichier en cas de tent d'ouverture en lecture, ou pour exécuti 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 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 zor 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 de l'élément>=*doc`
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`<chemin d'accès au répertoire local>` : analyse les objets dans le

		répertoire indiqué. Vous pouvez utiliser masques et des tags pour spécifier le chemin.

Vous pouvez utiliser des tags spécia
pour spécifier un conteneur ou une
image :

- [container-id :
  < identifiant >]/< chemin
  d'accès au répertoire loca
- [container-
  name < nom >]/< chemin d'acc
  au répertoire local >
- [image-id:
  < identifiant >]/< chemin
  d'accès au répertoire loca
- [image-name:< nom >]/< chemi
  d'accès au répertoire loca

Vous pouvez également utiliser des
combinaisons uniques des tags
[container-id:< identifiant >]
[container-name:< nom >],
[image-id:< identifiant >] et
[image-name:< nom >]/< chemin
d'accès au répertoire local >

Toute combinaison de tags uniques d
à 4 dans une même zone est possible
L'ordre de liste n'a pas d'importance.

Par exemple :

- [container-name:< nom >]
  [image-name:< nom >]/< chemi
  d'accès au répertoire loca
- [container-id:
  < identifiant >][image-name
  < nom >]/< chemin d'accès au
  répertoire local >
- [image-name:< nom >][image-
  id :< identifiant >]/< chemi
  d'accès au répertoire loca
- [container-name:< nom >]
  [container-id :< identifia
  >][image-name :
  < nom >]/< chemin d'accès au
  répertoire local >
- [container-name:< nom >]
  [image-id:< identifiant >]
  [container-id:< identifiant

`[image-name:<nom>]/<chemi`
`d'accès au répertoire loca`

Vous pouvez utiliser des masques (caractères `?` et `*`) dans les noms et identifiants.

Vous pouvez utiliser le caractère `*` (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère `*` au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère `/` dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère `/`. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole `?` au de n'importe quel caractère unique d un nom de fichier ou de répertoire.

`Shared:NFS` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole NFS.

`Shared:SMB` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole Samba.

`Mounted:NFS` : analyse les répertoires distants montés sur le périphérique via protocole NFS.

`Mounted:SMB` : analyse les répertoires distants montés sur le périphérique via protocole Samba.

`AllRemoteMounted` : analyse tous les répertoires distants montés sur le périphérique via les protocoles Samba NFS.

		`AllShared` : analyse toutes les ressou du système de fichiers du périphérique accessibles via les protocoles Samba e NFS. `< type de système de fichiers >` analyse toutes les ressources du systè fichiers indiqué du périphérique.
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 c de l'analyse).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`< chemin d'accès au répertoire local >` : exclure les objets du répertoi spécifié (y compris les sous-répertoire l'analyse. Vous pouvez utiliser des masc et des tags pour spécifier le chemin.

Vous pouvez utiliser des tags spécia
pour spécifier un conteneur ou une
image :

- [container-id :
  < identifiant >]/< chemin
  d'accès au répertoire loca
- [container-
  name < nom >]/< chemin d'acc
  au répertoire local >
- [image-id:
  < identifiant >]/< chemin
  d'accès au répertoire loca
- [image-name:< nom >]/< chemi
  d'accès au répertoire loca

Vous pouvez également utiliser des
combinaisons uniques des tags
[container-id:< identifiant >]
[container-name:< nom >],
[image-id:< identifiant >] et
[image-name:< nom >]/< chemin
d'accès au répertoire local >

Toute combinaison de tags uniques d
à 4 dans une même zone est possible
L'ordre de liste n'a pas d'importance.

Par exemple :

- [container-name:< nom >]
  [image-name:< nom >]/< chemi
  d'accès au répertoire loca
- [container-id:
  < identifiant >][image-name
  < nom >]/< chemin d'accès au
  répertoire local >
- [image-name:< nom >][image-
  id :< identifiant >]/< chemi
  d'accès au répertoire loca
- [container-name:< nom >]
  [container-id :< identifia
  >][image-name :
  < nom >]/< chemin d'accès au
  répertoire local >
- [container-name:< nom >]
  [image-id:< identifiant >]
  [container-id:< identifiant

		[image-name:<nom>]/<chemi d'accès au répertoire loca Vous pouvez utiliser des masques (caractères ? et *) dans les noms et identifiants. Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire. Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, /dir/*/fichier ou /dir/*/*/fichier. Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, /dir/**/fichier*/ ou /dir/fichier**/. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/fichier est un masq incorrect. Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d un nom de fichier ou de répertoire. Mounted:NFS : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole NFS. Mounted:SMB : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole Samba. AllRemoteMounted : exclut de l'analys tous les répertoires distants montés su périphérique via les protocoles Samba NFS. <type de système de fichiers> : exclure de l'analyse toutes les ressourc système de fichiers de l'appareil spécifi
La section **[ExcludedForProgram.item_#]** contient les paramètres suivants :		
ProgramPath	Chemin d'accès au processus exclu.	<chemin d'accès complet au

		`processus` > : exclut de l'analyse le processus dans le répertoire local spéc
`ApplyToDescendants`	Exclut de l'analyse les processus enfants du processus exclu spécifié par le paramètre `ProgramPath`.	`Yes` : exclut le processus spécifié et to ses processus enfants de l'analyse. `No` (valeur par défaut) : exclut uniquem processus spécifié de l'analyse, n'exclut 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 c de l'analyse).
`Path`	Chemin d'accès au répertoire contenant des fichiers que le processus modifie.	< `chemin d'accès au répertoire local` > : exclut de l'analyse les objets répertoire indiqué. Vous pouvez utiliser masques pour spécifier le chemin.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d un nom de fichier ou de répertoire.

`Shared:NFS` : exclut de l'analyse les ressources du système de fichiers du périphérique accessibles via le protocc NFS.

`Shared:SMB` : exclut de l'analyse les ressources du système de fichiers du périphérique accessibles via le protocc Samba.

`Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole NFS.

`Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole Samba.

`AllRemoteMounted` : exclut de l'analys tous les répertoires distants montés su périphérique via les protocoles Samba NFS.

`AllShared` : exclut de l'analyse toutes ressources du système de fichiers du périphérique partagées via les protoco Samba et NFS.

		<type de système de fichiers> exclut de l'analyse toutes les ressource système de fichiers indiqué du périphé

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 menaces sur les fichiers (*File_Threat_Protection*, ID:1) dans le fichier de configuration à l'aide de la commande :

   ```
   kesl-control --get-settings 1 --file <chemin complet au fichier de configuration> [--json]
   ```

2. Ouvrez le fichier de configuration et ajoutez une section `[ExclusiveForProgram.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 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 menaces sur les fichiers.

Si un fichier accessible via un lien symbolique n'est pas inclus dans la zone d'analyse du module Protection contre les menaces sur les fichiers, l'application n'analyse pas ce fichier. Toutefois, si un tel fichier contient un code malveillant, la sécurité du périphérique est menacée.

Analyse des liens matériels

En cas de traitement d'un fichier contenant plusieurs liens matériels, l'application choisit l'action en fonction de l'action à exécuter sur les objets définie :

- Si l'action **Exécuter l'action recommandée** est sélectionnée, l'application choisit automatiquement l'action et exécute celle-ci sur l'objet d'après les données relatives au danger de la menace détectée dans l'objet et de la possibilité de désinfection de celui-ci.
- Si l'action **Supprimer** est sélectionnée, l'application supprime le lien matériel traité. Les autres liens matériels vers ce fichier ne sont pas traités.
- Si vous sélectionnez l'action **Désinfecter**, l'application désinfecte le fichier source. 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.

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 du périphérique, ainsi que tous les objets montés et communs, accessibles via les protocoles Samba et NFS, selon les paramètres de sécurité recommandés.

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 dans la ligne de commande, ainsi que créer des tâches personnalisées d'analyse des logiciels malveillants.

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.
- Activer ou désactiver l'utilisation des exclusions globales et des exclusions de protection contre les fichiers malveillants pendant l'analyse.
- 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.

Rechercher 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. Cette 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. Cette 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. Cette 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. Cette 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 périphériques protégés.
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté :

	• **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).
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, configurer, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'analyse dans le tableau. Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone dans le tableau. Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone 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.

Cliquez sur le nom de la zone d'analyse pour ouvrir la fenêtre **<Nom de la zone d'analyse>**. Dans cette fenêtre, vous pouvez modifier les paramètres de la zone d'analyse choisie.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **<Nouvelle zone d'analyse>**. Cette fenêtre permet d'indiquer une nouvelle zone d'analyse.

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. Cette 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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba.

	• **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :<identifiant>]/<chemin d'accès au répertoire local>` • `[container-name <nom>]/<chemin d'accès au répertoire local>` • `[image-id:<identifiant>]/<chemin d'accès au répertoire local>` • `[image-name:<nom>]/<chemin d'accès au répertoire local>` Vous pouvez également utiliser des combinaisons uniques des tags `[container-id:<identifiant>]`, `[container-name:<nom>]`, `[image-id:<identifiant>]` et `[image-name:<nom>]/<chemin d'accès au répertoire local>`. 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:<nom>][image-name:<nom>]/<chemin d'accès au répertoire local>` • `[container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>` • `[image-name:<nom>][image-id :<identifiant>]/<chemin d'accès au répertoire local>` • `[container-name:< nom >][container-id :< identifiant >][image-name :<nom>]/<chemin d'accès au répertoire local>` • `[container-name:<nom>][image-id:<identifiant>][container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>` 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 Zones d'analyse

Vous pouvez configurer les paramètres de la zone d'analyse pour la tâche Analyse des logiciels malveillants. L'application vous permet d'analyser les fichiers, les secteurs d'amorçage, la mémoire du périphérique 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. Cette 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.
Vérifier la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire du périphérique client. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si cette case n'est pas cochée, l'application ne vérifie pas la mémoire du noyau ni 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.
Périphériques à analyser	Cliquez sur le lien **Configurer les masques de périphérique** pour ouvrir la fenêtre **Zone d'analyse**, où vous pouvez définir les périphériques dont les secteurs de démarrage doivent être analysés.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des périphériques, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom de périphérique **/**** (tous les périphériques).

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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 menaces sur les fichiers pendant l'exécution de la tâche.

Paramètres des exclusions de l'analyse

Paramètre	Description
Configurer les 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. Cette case est cochée par défaut.
Utiliser les exclusions de la Protection contre les menaces sur les fichiers	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les menaces sur les fichiers pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exceptions du module Protection contre les menaces sur les fichiers. Cette case est cochée par défaut.

Fenêtre Zones d'exclusion

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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 le périphérique. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >] et [image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Rechercher 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 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.
Action en cas de détection d'une menace	Le groupe de paramètres contient le bouton **Configurer** qui permet d'ouvrir la fenêtre **Action en cas de détection d'une menace** pour configurer les actions que l'application doit exécuter sur tout objet infecté détecté.

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
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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

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 du périphérique 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. Cette 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.
Vérifier la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire du périphérique. 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.
Périphériques à analyser	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Zone d'analyse**, où vous pouvez définir les périphériques 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. Cette case est cochée par défaut.
Utiliser les exclusions de la Protection contre les menaces sur les fichiers	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les menaces sur les fichiers pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exceptions du module Protection contre les menaces sur les fichiers. Cette case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des périphériques, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom de périphérique **/**** (tous les périphériques).

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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. Cette 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	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.

format de messagerie	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. Cette 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. Cette 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 périphériques protégés.

Fenêtre Action 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
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).

Section Exclusions

Une *exclusion de l'analyse* 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 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**. Cliquez sur celui-ci pour 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

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >] et [image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Rechercher 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 préinstallée 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 des tâches.
- À l'aide de la commande `kesl-control --scan-file`, vous pouvez effectuer une *analyse personnalisée* des fichiers et répertoires spécifiés.

Paramètres de la tâche préinstallée Analyse des logiciels malveillants

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir pour la tâche Analyse des logiciels malveillants.

Paramètres de la tâche Analyse des logiciels malveillants.

Paramètre	Description	Valeurs
`ScanFiles`	Activation de l'analyse des fichiers.	`Yes` (valeur par défaut) : analyser les fi `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 mé 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 ob 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 arc Si la valeur `FirstAction=Recommende` spécifiée, alors, en fonction du type d'archive, l'application supprime soit l'ol infecté, soit l'archive entière contenant 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) : analyse les arc 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 le fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniqu format texte. `No` (valeur par défaut) : n'analyse pas le messages électroniques au format text
`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 limitée. Valeur par défaut : 0.
`FirstAction`	Sélection de la première action que l'application va exécuter sur les objets infectés.	`Disinfect` (désinfecter) : l'application tente de désinfecter un objet en enregistrant une copie dans la sauvega Si la désinfection échoue, par exemple, type de l'objet ou le type de la menace l'objet ne peut pas être désinfecté, l'application garde l'objet intact. Si la va de la première action est `Disinfect (Désinfecter)`, il est recommandé de définir une deuxième action via le paramètre `SecondAction`. `Remove` (supprimer) : l'application supp l'objet infecté après avoir créé au préal sa copie de sauvegarde.

		`Recommended` (exécution de l'action recommandée) : l'application sélectionr exécute automatiquement une action s l'objet en fonction des informations rel à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime automatiquement les chevau Troie car ils ne s'intègrent pas à d'autre fichiers et par conséquent, ils n'ont pas besoin d'être désinfectés. `Skip` (ignorer) : l'application ne tente p désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infe sont conservées dans le journal. Valeur par défaut : `Recommended`.
`SecondAction`	Sélection de la deuxième action exécutée par l'application sur les objets infectés. L'application exécute la deuxième action si la première échoue.	Les valeurs du paramètre `SecondActi` sont identiques à celles du paramètre `FirstAction`. Si l'option `Skip` ou `Remove` est sélecti en tant que première action, il n'est pas nécessaire d'en choisir une deuxième. D les autres cas, il est recommandé d'indi deux actions. Si vous n'avez pas défini u deuxième action, l'application exécute l'action `Skip` (ignorer) en tant que deu action. Valeur par défaut : `Skip`.
`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 défir le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le param `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 la valeur 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=eicar`
		`ExcludeMasks.item_0001=eicar`

`UseExcludeThreats`	Activation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets cont les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les mena 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	La valeur du paramètre est sensible à la casse. La valeur par défaut n'est pas définie.

	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/.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EIC`
		`Test-*`
		`ExcludeThreats.item_0001=?`
		`rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exceptions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions globales. `No` : ne pas utiliser les exceptions globa
`UseOASExclusions`	Activez l'utilisation des exceptions de la Protection contre les menaces sur les fichiers lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exceptions de la Protection contre les menaces sur les fichiers. `No` : ne pas utiliser les exceptions de la Protection contre les menaces sur les fichiers.
`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 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 ob des archives. `No` (valeur par défaut) : n'enregistre pas 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 tr `No` (valeur par défaut) : n'enregistre pas 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'analys 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 av une charge minimale sur le système. `Medium` : niveau de l'analyse heuristiqu normal avec une charge équilibrée sur l système d'exploitation. `Deep` : analyse la plus minutieuse avec charge maximale sur le système d'exploitation. `Recommander` (valeur par défaut) : vale recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisat de la technologie iChecker. `No` : désactive l'utilisation de la technol iChecker.
`DeviceNameMasks.item_#`	Une liste de noms d'appareils dont les secteurs d'amorçage seront vérifiés par l'application. 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 de l'appareil>` vérifier les secteurs d'amorçage des appareils dont le nom contient le masq indiqué. Valeur par défaut : `/**` (tout ensemble 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 zor 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	`<chemin d'accès au répertoire`

	contenant les objets à vérifier.	`local` > : analyse les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur le périphérique via protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur le périphérique via protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur le périphérique via les protocoles Samba NFS. `AllShared` : analyse toutes les ressou du système de fichiers du périphérique accessibles via les protocoles Samba e NFS. `< type de système de fichiers >` analyse toutes les ressources du systè fichiers indiqué du périphérique.
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).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`< chemin d'accès au répertoire local >` : exclure les objets du répertoi spécifié (y compris les sous-répertoire l'analyse. Vous pouvez utiliser des masc pour spécifier le chemin.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d 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 exclusion de type `/.snapshots/*/snapshot/`.

`Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole NFS.

`Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole Samba.

`AllRemoteMounted` : exclut de l'analys tous les répertoires distants montés su périphérique via les protocoles Samba NFS.

`<type de système de fichiers>` exclut de l'analyse toutes les ressource système de fichiers indiqué du périphér

		Les répertoires distants sont exclus l'analyse par l'application uniquement s'ils ont été montés avant le lanceme de la tâche. Les répertoires distants montés après le lancement de la tâch ne sont pas exclus de l'analyse.

Analyse personnalisée des fichiers et répertoires

Vous pouvez effectuer une analyse personnalisée des fichiers et répertoires spécifiés à l'aide de la commande `kesl-control --scan-file`.

Une analyse personnalisée est effectuée avec des 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 d'accès>` : chemin d'accès au fichier ou au répertoire que vous souhaitez vérifier. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.
- `--action <action>` : action que l'application va exécuter sur les objets infectés. Si vous ne spécifiez pas la clé `--action` , l'application effectuera l'action recommandée.

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 disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir 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 fi `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 secteurs d'amorçage.
`ScanComputerMemory`	Activation de la tâche d'analyse de la mémoire des processus et de la	`Yes` : analyser la mémoire des processu la mémoire du noyau.

	mémoire du noyau.	`No` (valeur par défaut) : ne pas analyser mémoire des processus et la mémoire noyau.
`ScanStartupObjects`	Activation de l'analyse des objets de démarrage.	`Yes` : analyser les objets de démarrage `No` (valeur par défaut) : ne pas analyser 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 arc Si la valeur `FirstAction=Recommende` spécifiée, alors, en fonction du type d'archive, l'application supprime soit l'ol infecté, soit l'archive entière contenant 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) : analyse les arc 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 le fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniqu format texte. `No` (valeur par défaut) : n'analyse pas le messages électroniques au format text
`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 limitée. Valeur par défaut : 0.
`FirstAction`	Sélection de la première action que l'application va exécuter sur les objets infectés.	`Disinfect` (désinfecter) : l'application tente de désinfecter un objet en enregistrant une copie dans la sauvega Si la désinfection échoue, par exemple, type de l'objet ou le type de la menace l'objet ne peut pas être désinfecté, l'application garde l'objet intact. Si la va de la première action est `Disinfect (Désinfecter)`, il est recommandé de définir une deuxième action via le paramètre `SecondAction`.

		`Remove` (supprimer) : l'application supp l'objet infecté après avoir créé au préal sa copie de sauvegarde. `Recommended` (exécution de l'action recommandée) : l'application sélectionr exécute automatiquement une action s l'objet en fonction des informations rel à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime automatiquement les chevau Troie car ils ne s'intègrent pas à d'autre fichiers et par conséquent, ils n'ont pas besoin d'être désinfectés. `Skip` (ignorer) : l'application ne tente p désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infe sont conservées dans le journal. Valeur par défaut : `Recommended`.
`SecondAction`	Sélection de la deuxième action exécutée par l'application sur les objets infectés. L'application exécute la deuxième action si la première échoue.	Les valeurs du paramètre `SecondActi` sont identiques à celles du paramètre `FirstAction`. Si l'option `Skip` ou `Remove` est sélecti en tant que première action, il n'est pas nécessaire d'en choisir une deuxième. D les autres cas, il est recommandé d'indi deux actions. Si vous n'avez pas défini u deuxième action, l'application exécute l'action `Skip` (ignorer) en tant que deu action. Valeur par défaut : `Skip`.
`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 défir le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le param `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=eicar`
		`ExcludeMasks.item_0001=eicar`

`UseExcludeThreats`	Activation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets cont les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les mena 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	La valeur du paramètre est sensible à la casse. La valeur par défaut n'est pas définie.

	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/.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EIC`
		`Test-*`
		`ExcludeThreats.item_0001=?`
		`rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exceptions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions globales. `No` : ne pas utiliser les exceptions globa
`UseOASExclusions`	Activez l'utilisation des exceptions de la Protection contre les menaces sur les fichiers lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exceptions de la Protection contre les menaces sur les fichiers. `No` : ne pas utiliser les exceptions de la Protection contre les menaces sur les fichiers.
`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 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 ob des archives. `No` (valeur par défaut) : n'enregistre pas 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 tr `No` (valeur par défaut) : n'enregistre pas 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'analys 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 av une charge minimale sur le système. `Medium` : niveau de l'analyse heuristiqu normal avec une charge équilibrée sur l système d'exploitation. `Deep` : analyse la plus minutieuse avec charge maximale sur le système d'exploitation. `Recommander` (valeur par défaut) : vale recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisat de la technologie iChecker. `No` : désactive l'utilisation de la technol iChecker.
`DeviceNameMasks.item_#`	Une liste de noms d'appareils dont les secteurs d'amorçage seront vérifiés par l'application. 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 de l'appareil>` vérifier les secteurs d'amorçage des appareils dont le nom contient le masq indiqué. Valeur par défaut : `/**` (tout ensemble 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 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 zor 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>` : analyse les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole NFS. `Shared:SMB` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur le périphérique via protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur le périphérique via protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur le périphérique via les protocoles Samba NFS. `AllShared` : analyse toutes les ressou du système de fichiers du périphérique accessibles via les protocoles Samba e NFS. `<type de système de fichiers>` analyse toutes les ressources du systè fichiers indiqué du périphérique.
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).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`<chemin d'accès au répertoire local>` : exclure les objets du répertoi spécifié (y compris les sous-répertoire l'analyse. Vous pouvez utiliser des masc pour spécifier le chemin.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d 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 exclusion de type `/.snapshots/*/snapshot/`.

`Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole NFS.

`Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole Samba.

`AllRemoteMounted` : exclut de l'analys tous les répertoires distants montés su périphérique via les protocoles Samba NFS.

`<type de système de fichiers>` exclut de l'analyse toutes les ressource système de fichiers indiqué du périphér

		Les répertoires distants sont exclus l'analyse par l'application uniquement s'ils ont été montés avant le lanceme de la tâche. Les répertoires distants montés après le lancement de la tâch 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.

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.
- 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.

Vérification 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 de 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. Cette 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. Cette 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.
Informer 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.
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. Cette 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. Cette 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 périphériques protégés.
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage.

	• **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).
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, configurer, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'analyse dans le tableau. Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone dans le tableau. Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone 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. Cliquez sur le nom de la zone d'analyse pour ouvrir la fenêtre **<Nom de la zone d'analyse>**. Dans cette fenêtre, vous pouvez modifier les paramètres de la zone d'analyse choisie. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **<Nouvelle zone d'analyse>**. Cette fenêtre permet d'indiquer une nouvelle zone d'analyse.

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. Cette 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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :<identifiant>]/<chemin d'accès au répertoire local>`
- `[container-name <nom>]/<chemin d'accès au répertoire local>`
- `[image-id:<identifiant>]/<chemin d'accès au répertoire local>`
- `[image-name:<nom>]/<chemin d'accès au répertoire local>`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id:<identifiant>]`, `[container-name:<nom>]`, `[image-id:<identifiant>]` et `[image-name:<nom>]/<chemin d'accès au répertoire local>`.

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:<nom>][image-name:<nom>]/<chemin d'accès au répertoire local>`
- `[container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>`
- `[image-name:<nom>][image-id :<identifiant>]/<chemin d'accès au répertoire local>`
- `[container-name:<nom>][container-id :<identifiant>][image-name :<nom>]/<chemin d'accès au répertoire local>`
- `[container-name:<nom>][image-id:<identifiant>][container-id:<identifiant>][image-name:<nom>]/<chemin d'accès au répertoire local>`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 Zones 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 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. Cette case est cochée par défaut.
Vérifier la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire du périphérique client. Si cette case est cochée, l'application vérifie la mémoire du noyau et les processus en cours d'exécution. Si cette case n'est pas cochée, l'application ne vérifie pas la mémoire du noyau ni les processus en cours d'exécution. Cette 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. Cette case est cochée par défaut.
Périphériques à analyser	Cliquez sur le lien **Configurer les masques de périphérique** pour ouvrir la fenêtre **Zone d'analyse**, où vous pouvez définir les périphériques dont les secteurs de démarrage doivent être analysés.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des périphériques, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom de périphérique **/**** (tous les périphériques).

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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 les 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. Cette case est cochée par défaut.
Utiliser les exclusions de la Protection contre les menaces sur les fichiers	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les menaces sur les fichiers pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exceptions du module Protection contre les menaces sur les fichiers. Cette case est cochée par défaut.

Fenêtre Zones d'exclusion

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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 le périphérique. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Vérification des zones importantes 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 de 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.
Action en cas de détection d'une menace	Le groupe de paramètres contient le bouton **Configurer** qui permet d'ouvrir la fenêtre **Action en cas de détection d'une menace** pour configurer les actions que l'application doit exécuter sur tout objet infecté détecté.

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
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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Paramètres de 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. Cette case est cochée par défaut.
Vérifier la mémoire du noyau et les processus en cours d'exécution	La case active ou désactive l'analyse de la mémoire du périphérique. 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. Cette 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. Cette case est cochée par défaut.
Périphériques à analyser	Ce groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Zone d'analyse**, où vous pouvez définir les périphériques 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. Cette case est cochée par défaut.
Utiliser les exclusions de la Protection contre les menaces sur les fichiers	La case à cocher active ou désactive l'utilisation des exclusions configurées de la Protection contre les menaces sur les fichiers pendant l'exécution de l'application. Si la case est cochée, l'application exclut de l'analyse les objets spécifiés dans les exceptions du module Protection contre les menaces sur les fichiers. Cette case est cochée par défaut.

Fenêtre Zones d'analyse

Le tableau contient les masques des noms des périphériques, dont les secteurs de démarrage doivent être analysés par l'application. Par défaut, le tableau contient le masque de nom de périphérique **/**** (tous les périphériques).

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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. Cette 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. Cette 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.

	Cette 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 périphériques protégés.

Fenêtre Action 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
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).

Section Exclusions

Une *exclusion de l'analyse* 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 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**. Cliquez sur celui-ci pour 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

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >]` et `[image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Vérification des zones importantes dans 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) : n'analyse pas le 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 mé 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 ob de démarrage. `No` : ne pas analyser les objets de démarrage.
`ScanArchived`	Activation de l'analyse des archives (y compris les archives autoextractibles SFX).	`Yes` (valeur par défaut) : analyse les arc Si la valeur `FirstAction=Recommende` spécifiée, alors, en fonction du type d'archive, l'application supprime soit l'ol infecté, soit l'archive entière contenant menace. `No` : n'analyse pas les archives.

	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.	
`ScanSfxArchived`	Activation de l'analyse uniquement des archives autoextractibles (archives comprenant un module d'extraction d'exécutable).	`Yes` (valeur par défaut) : analyse les arc 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 le fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniqu format texte. `No` (valeur par défaut) : n'analyse pas le messages électroniques au format text
`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 limitée. Valeur par défaut : 0.
`FirstAction`	Sélection de la première action que l'application va exécuter sur les objets infectés.	`Disinfect` (désinfecter) : l'application tente de désinfecter un objet en enregistrant une copie dans la sauvega Si la désinfection échoue, par exemple, type de l'objet ou le type de la menace l'objet ne peut pas être désinfecté, l'application garde l'objet intact. Si la va de la première action est `Disinfect (Désinfecter)`, il est recommandé de définir une deuxième action via le paramètre `SecondAction`. `Remove` (supprimer) : l'application supp l'objet infecté après avoir créé au préal sa copie de sauvegarde. `Recommended` (exécution de l'action recommandée) : l'application sélectionn exécute automatiquement une action s l'objet en fonction des informations rel à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime automatiquement les chevau Troie car ils ne s'intègrent pas à d'autre fichiers et par conséquent, ils n'ont pas besoin d'être désinfectés.

		`Skip` (ignorer) : l'application ne tente p désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infe sont conservées dans le journal. Valeur par défaut : `Recommended`.
`SecondAction`	Sélection de la deuxième action exécutée par l'application sur les objets infectés. L'application exécute la deuxième action si la première échoue.	Les valeurs du paramètre `SecondActi` sont identiques à celles du paramètre `FirstAction`. Si l'option `Skip` ou `Remove` est sélecti en tant que première action, il n'est pas nécessaire d'en choisir une deuxième. D les autres cas, il est recommandé d'indi deux actions. Si vous n'avez pas défini u deuxième action, l'application exécute l'action `Skip` (ignorer) en tant que deu action. Valeur par défaut : `Skip`.
`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 défir le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le param `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 la valeur 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=eicar`
		`ExcludeMasks.item_0001=eicar`

`UseExcludeThreats`	Activation de l'exclusion de l'analyse des objets contenant les menaces indiquées par le paramètre `ExcludeThreats.item_#`.	`Yes` : exclut de l'analyse les objets cont les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les mena 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.
		La valeur du paramètre est sensible à la casse.
		La valeur par défaut n'est pas définie.
		Exemple :
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EIC`
		`Test-*`
		`ExcludeThreats.item_0001=?`
		`rojan.Linux`

	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/.	
`UseGlobalExclusions`	Activez l'utilisation des exceptions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions globales. `No` : ne pas utiliser les exceptions globa
`UseOASExclusions`	Activez l'utilisation des exceptions de la Protection contre les menaces sur les fichiers lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exceptions de la Protection contre les menaces sur les fichiers. `No` : ne pas utiliser les exceptions de la Protection contre les menaces sur les fichiers.
`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 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 ob des archives. `No` (valeur par défaut) : n'enregistre pas 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 tr `No` (valeur par défaut) : n'enregistre pas 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'analys heuristique `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique.	`Light` : analyse la moins minutieuse av une charge minimale sur le système.

	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.	`Medium` : niveau de l'analyse heuristiqu normal avec une charge équilibrée sur l système d'exploitation. `Deep` : analyse la plus minutieuse avec charge maximale sur le système d'exploitation. `Recommander` (valeur par défaut) : vale recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisat de la technologie iChecker. `No` : désactive l'utilisation de la technol iChecker.
`DeviceNameMasks.item_#`	Une liste de noms d'appareils dont les secteurs d'amorçage seront vérifiés par l'application. 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 de l'appareil>` vérifier les secteurs d'amorçage des appareils dont le nom contient le masq indiqué. Valeur par défaut : `/**` (tout ensemble 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 zor 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>` : analyse les objets dans le répertoire indiqué. `Shared:NFS` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole NFS.

		`Shared:SMB` : analyse les ressources d système de fichiers du périphérique accessibles via le protocole Samba. `Mounted:NFS` : analyse les répertoires distants montés sur le périphérique via protocole NFS. `Mounted:SMB` : analyse les répertoires distants montés sur le périphérique via protocole Samba. `AllRemoteMounted` : analyse tous les répertoires distants montés sur le périphérique via les protocoles Samba NFS. `AllShared` : analyse toutes les ressou du système de fichiers du périphérique accessibles via les protocoles Samba e NFS. `< type de système de fichiers >` analyse toutes les ressources du systè fichiers indiqué du périphérique.
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).
`Path`	Le chemin d'accès au répertoire contenant les objets exclus.	`< chemin d'accès au répertoire local >` : exclut de l'analyse les objets répertoire indiqué. Vous pouvez utiliser masques pour spécifier le chemin.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d 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 exclusion de type `/.snapshots/*/snapshot/`.

< `chemin d'accès au répertoire local` > : exclure les objets du répertoi spécifié (y compris les sous-répertoire l'analyse. Vous pouvez utiliser des masq pour spécifier le chemin.

Vous pouvez utiliser le caractère * (astérisque) pour former un masque nom de fichier ou de répertoire.

Vous pouvez saisir le caractère * au d'un ensemble de caractères (y comp un ensemble vide) quelconque devar caractère / dans le nom du fichier ou du répertoire. Par exemple, `/dir/*/fichier` ou `/dir/*/*/fichier`.

Vous pouvez saisir deux caractères * consécutifs pour remplacer n'import quel ensemble de caractères (y com un ensemble vide) dans le nom du fichier ou du répertoire, y compris le caractère /. Par exemple, `/dir/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` est un masq incorrect.

Vous pouvez utiliser le symbole ? au de n'importe quel caractère unique d 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 exclusion de type `/.snapshots/*/snapshot/`.

`Mounted:NFS` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole NFS.

`Mounted:SMB` : exclut de l'analyse les répertoires distants montés sur le périphérique via le protocole Samba.

`AllRemoteMounted` : exclut de l'analys tous les répertoires distants montés su périphérique via les protocoles Samba NFS.

`<type de système de fichiers>` exclut de l'analyse toutes les ressource système de fichiers indiqué du périphér

		Les répertoires distants sont exclus l'analyse par l'application uniquement s'ils ont été montés avant le lanceme de la tâche. Les répertoires distants montés après le lancement de la tâch 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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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** → **Tâches locales** → **Analyse des disques amovibles**).

Paramètres du module Analyse des disques amovibles

Paramètre	Description
Analyse des disques amovibles activée / désactivée	Le bouton bascule active ou désactive l'analyse des disques amovibles lors de la connexion au périphérique de l'utilisateur. Le bouton bascule est désactivé 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 au périphérique 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, 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*.
Action à réaliser en cas de connexion	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 au périphérique de l'utilisateur :

d'un lecteur CD / DVD	• **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, 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 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 dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres d'analyse des disques amovibles dans les propriétés de la stratégie (**Tâches locales** → **Analyser les disques amovibles**).

Paramètres du module Analyse des disques amovibles

Paramètre	Description
Activer l'analyse des disques amovibles à la connexion au périphérique	La case active ou désactive l'analyse des disques amovibles lors de la connexion au périphérique 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 au périphérique 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, 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*.
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 au périphérique 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, 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 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 dans la ligne de commande

Sur la ligne de commande, vous pouvez gérer l'analyse des disques amovibles à l'aide de la tâche prédéfinie Analyser les disques amovibles (*Removable_Drives_Scan*).

Par défaut, la tâche d'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.

Paramètre	Description	Valeurs
`ScanRemovableDrives`	Activation de l'analyse des disques amovibles lors de la connexion au périphérique. 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, 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.
`ScanOpticalDrives`	Activation de l'analyse des lecteurs CD/DVD et des disques Blu-ray lors de la connexion au périphérique.	`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, 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 du conteneur* vous permet de vérifier les conteneurs et les espaces de noms en cours d'exécution en temps réel.
- À l'aide des tâches *Analyse du conteneur*, vous pouvez analyser des conteneurs et des images à la demande.

L'application prend en charge l'intégration avec le système d'administration de conteneurs Docker, l'environnement CRI-O, les utilitaires Podman et runc est prise en charge.

Pour utiliser les tâches Analyse des conteneurs, vous avez besoin d'une licence incluant cette fonctionnalité.

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 menaces sur les fichiers doit être activé. Les paramètres de protection contre les menaces sur les fichiers sont utilisés lors de l'analyse du conteneur 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 Surveillance du conteneur dans la ligne de commande est affiché comme « `La tâche est disponible et n'est pas en cours d'exécution` », dans Kaspersky Security Center, il est affiché 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.

Configuration de la surveillance des conteneurs dans Web Console

Dans Web Console, vous pouvez gérer le fonctionnement du module *Surveillance du conteneur* dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres d'analyse des conteneurs**).

Paramètre	Description
Analyse des espaces de noms et de conteneurs activée/désactivée	Le commutateur active ou désactive la vérification en temps réel des espaces des noms et des conteneurs. Le bouton bascule est activé par défaut.
Action sur le conteneur en cas de détection d'une menace	Vous pouvez 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 le conteneur 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.
Utiliser Docker	La case permet d'activer ou de désactiver l'utilisation de l'environnement Docker. Cette case est cochée par défaut.
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. Cette 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. Cette 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. Cette 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.

Configuration de la surveillance des conteneurs dans la Console d'administration

Dans la Console d'administration, vous pouvez gérer le fonctionnement du module Surveillance du conteneur dans les propriétés de la stratégie (**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. Cette 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	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour 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.

Paramètres d'analyse de conteneur

Paramètre	Description
Utiliser Docker	La case permet d'activer ou de désactiver l'utilisation de l'environnement Docker. Cette case est cochée par défaut.

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. Cette 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. Cette 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.
Utiliser runc	La case permet d'activer ou de désactiver l'utilisation de l'utilitaire runc. Cette 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 de commutateurs 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` : 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>` : chemin d'accès au fichier dans lequel les paramètres généraux de l'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 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>` : chemin complet vers le fichier de configuration avec les paramètres généraux de l'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` > est le nom et la valeur de l'un des paramètres généraux de l'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.

L'intégration avec le système d'administration de conteneurs Docker, l'environnement CRI-O, les utilitaires Podman et runc est prise en charge.

Pour utiliser la tâche, vous devez posséder la licence qui couvre cette fonction.

Vous pouvez exécuter des analyses des conteneurs et configurer les paramètres d'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 personnalisées des conteneurs. Vous pouvez configurer les paramètres de numérisation en modifiant les paramètres de la tâche.

Paramètres de la tâche Analyser les conteneurs

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. Cette 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. Cette 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. Cette 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. Cette 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 périphériques protégés.
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.

Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).
Analyser les conteneurs	La case active ou désactive l'analyse des conteneurs. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les conteneurs à analyser. Cette 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	Vous pouvez 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 le conteneur 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. Cette 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 Analyser les conteneurs, 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. Cette case est cochée par défaut.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Analyse du conteneur dans la Console d'administration

Dans la Console d'administration, vous pouvez analyser les conteneurs et les images à l'aide de la tâche *Analyser les conteneurs*.

Vous pouvez créer et lancer des tâches d'analyse personnalisées des conteneurs. 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 Analyser les conteneurs

Paramètre	Description
Analyse	Ce groupe de paramètres contient les boutons qui permettent d'ouvrir les fenêtres de configuration des paramètres d'analyse des conteneurs et des paramètres généraux de l'analyse.
Action en cas	Le groupe de paramètres contient le bouton **Configurer** qui permet d'ouvrir la fenêtre

de détection d'une menace	**Action en cas de détection d'une menace** pour configurer les actions que l'application doit exécuter sur tout objet infecté détecté.

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 des conteneurs et des images.

Paramètres d'analyse des conteneurs et des images

Paramètre	Description
Analyser les conteneurs	La case active ou désactive l'analyse des conteneurs. Si la case est cochée, vous pouvez indiquer un nom ou un masque de nom pour les conteneurs à analyser. Cette 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 le conteneur 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. Cette 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	Cette case active ou désactive l'analyse de toutes les couches des images et des

chaque couche	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. Cette 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. Cette 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. Cette 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. Cette 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 périphériques protégés.

•

Fenêtre Action 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
Première action	La liste déroulante permet de sélectionner la première action que l'application exécutera sur l'objet infecté détecté : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter (valeur par défaut). • **Ignorer** l'objet.
Deuxième action	Cette liste déroulante permet de sélectionner la deuxième action que l'application exécutera sur l'objet infecté détecté si la première action échoue : • **Désinfecter** l'objet. Une copie de l'objet infecté sera placée vers la sauvegarde. • **Supprimer** l'objet. Une copie de l'objet infecté sera placée dans le Stockage. • **Exécuter l'action recommandée** sur l'objet en fonction des données sur le niveau de la menace détectée dans le fichier et de la possibilité de le désinfecter. • **Ignorer** l'objet (valeur par défaut).

•

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.

	Cette case est cochée par défaut.

Fenêtre Exclusions d'après le masque

Vous pouvez configurer l'exclusion des objets de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 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 menace.

Cliquez sur le bouton **Supprimer** pour que Kaspersky Endpoint Security supprime la menace sélectionnée des exclusions.

Le bouton est disponible si au moins un nom de menace a été sélectionné dans la liste.

Cliquez sur un nom de menace dans le tableau pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de modifier le nom de la menace à exclure de l'analyse.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nom de la menace**. Cette fenêtre permet de définir le nom de la menace à exclure de l'analyse.

Analyse du conteneur dans 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 des *analyses personnalisées* des conteneurs et des images spécifiés.

Paramètres de la tâche Analyser les conteneurs

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 Analyser les conteneurs

Paramètre	Description	Valeurs
`ScanContainers`	Analyse du conteneur défini par le masque. Vous pouvez spécifier des 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 définies par	`Yes` (valeur par défaut) : analyse les images

	le masque. Vous pouvez spécifier des masques à l'aide du paramètre `ImageNameMask`.	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. `Non` (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. 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 Analyser les conteneurs

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 arc Si la valeur `FirstAction=Recommende` spécifiée, alors, en fonction du type d'archive, l'application supprime soit l'ol infecté, soit l'archive entière contenant 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) : analyse les arc 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 le fichiers des bases de données email.
`ScanPlainMail`	Activation de l'analyse des messages électroniques au format texte (plain text).	`Yes` : analyse les messages électroniqu format texte. `No` (valeur par défaut) : n'analyse pas le messages électroniques au format text
`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 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.
`FirstAction`	Sélection de la première action que l'application va exécuter sur les objets infectés.	`Disinfect` (désinfecter) : l'application tente de désinfecter un objet en enregistrant une copie dans la sauvega Si la désinfection échoue, par exemple, type de l'objet ou le type de la menace l'objet ne peut pas être désinfecté, l'application garde l'objet intact. Si la va de la première action est `Disinfect (Désinfecter)`, il est recommandé de définir une deuxième action via le paramètre `SecondAction`. `Remove` (supprimer) : l'application supp l'objet infecté après avoir créé au préal sa copie de sauvegarde.

		`Recommended` (exécution de l'action recommandée) : l'application sélectionr exécute automatiquement une action s l'objet en fonction des informations rel à la menace détectée dans l'objet. Par exemple, Kaspersky Endpoint Security supprime automatiquement les chevau Troie car ils ne s'intègrent pas à d'autre fichiers et par conséquent, ils n'ont pas besoin d'être désinfectés. `Skip` (ignorer) : l'application ne tente p désinfecter ou de supprimer un objet infecté. Les informations sur l'objet infe sont conservées dans le journal. Valeur par défaut : `Recommended`.
`SecondAction`	Sélection de la deuxième action exécutée par l'application sur les objets infectés. L'application exécute la deuxième action si la première échoue.	Les valeurs du paramètre `SecondActi` sont identiques à celles du paramètre `FirstAction`. Si l'option `Skip` ou `Remove` est sélecti en tant que première action, il n'est pas nécessaire d'en choisir une deuxième. D les autres cas, il est recommandé d'indi deux actions. Si vous n'avez pas défini u deuxième action, l'application exécute l'action `Skip` (ignorer) en tant que deu action. Valeur par défaut : `Skip`.
`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 défir le paramètre `ExcludeMasks.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets définis par le param `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=eicar`
		`ExcludeMasks.item_0001=eicar`

`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 cont les menaces définies par le paramètre `ExcludeThreats.item_#`. `No` (valeur par défaut) : n'exclut pas de l'analyse les objets contenant les mena 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.	La valeur du paramètre est sensible à la casse. La valeur par défaut n'est pas définie. Exemple : `UseExcludeThreats=Yes`

	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/.
		`ExcludeThreats.item_0000=EIC`
		`Test-*`
		`ExcludeThreats.item_0001=?`
		`rojan.Linux`

`UseGlobalExclusions`	Activez l'utilisation des exceptions globales lors de l'analyse.	`Yes` (valeur par défaut) : utiliser les exclusions globales. `No` : ne pas utiliser les exceptions globa
`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 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 ob des archives. `No` (valeur par défaut) : n'enregistre pas 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 tr `No` (valeur par défaut) : n'enregistre pas 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'analys heuristique ; `No` : désactive l'analyse heuristique.
`HeuristicLevel`	Niveau de l'analyse heuristique.	`Light` : analyse la moins minutieuse av une charge minimale sur le système.

	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.	`Medium` : niveau de l'analyse heuristiqu normal avec une charge équilibrée sur l système d'exploitation. `Deep` : analyse la plus minutieuse avec charge maximale sur le système d'exploitation. `Recommander` (valeur par défaut) : vale recommandée.
`UseIChecker`	Activation de l'utilisation de la technologie iChecker.	`Yes` (valeur par défaut) : active l'utilisat de la technologie iChecker. `No` : désactive l'utilisation de la technol iChecker.

Analyse personnalisée du conteneur et des images

Vous pouvez effectuer des analyses personnalisées des conteneurs et des images spécifiés 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 des conteneurs 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 exécuter une analyse personnalisée des conteneurs, exécutez la commande suivante :

```
kesl-control --scan-container <conteneur/image [:tag ]>
```

où `<conteneur/image [:tag ]>` est le nom ou l'identifiant 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/*/fichier` ou `/dir/*/*/fichier`.

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/**/fichier*/` ou `/dir/fichier**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.

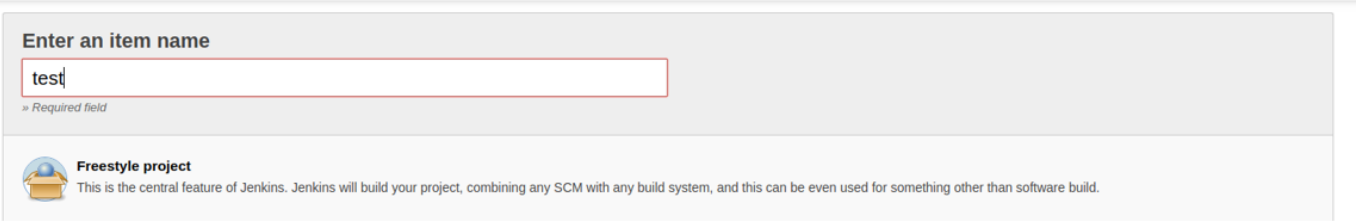
Exemples :
Analyse du conteneur baptisé my_container :
`kesl-control --scan-container my_container`
Analysez l'image baptisée my_image (toutes les balises) :
`kesl-control --scan-container my_image*`

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 :

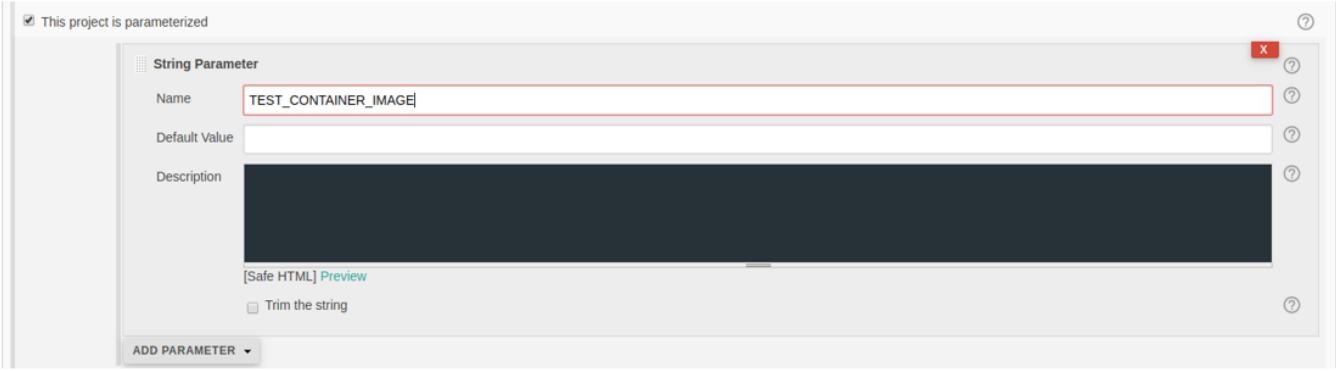
1. Installez Kaspersky Endpoint Security sur un nœud Jenkins.
2. Installez Docker Engine sur un nœud Jenkins.
   Pour en savoir plus, reportez-vous à la documentation de Docker Engine.
3. Octroyez les privilèges d'administrateur de l'application Kaspersky Endpoint Security à l'utilisateur Jenkins :
   `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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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.

Avant l'activation du module Gestion du pare-feu, il est conseillé de désactiver les autres outils de gestion du pare-feu du système d'exploitation.

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.

Dans les systèmes d'exploitation Red Hat Enterprise Linux et CentOS 8, les règles de pare-feu créées à l'aide de l'application Kaspersky Endpoint Security ne peuvent être affichées qu'à l'aide des lignes de commande (commande `kesl-control -F --query`).

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.
- 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.

- Définissez les adresses réseau pour qu'elles correspondent aux zones réseau prédéfinies. Vous pouvez ajouter des adresses IP ou des sous-réseaux aux zones réseau et supprimer des adresses des zones réseau.

- Activer ou désactiver l'ajout automatique de règles d'autorisation pour les ports de l'Agent d'administration.

Pour éviter d'éventuels problèmes sur les systèmes équipés de nftables, l'application Kaspersky Endpoint Security utilise les utilitaires système iptables et iptables-restore lors de l'ajout de règles pour le pare-feu du système d'exploitation. L'application crée la chaîne de règles d'autorisation spéciale kesl_bypass et l'ajoute en tête de la liste mangle des utilitaires iptables et ip6tables. Les règles de la chaîne kesl_bypass permettent d'exclure le trafic de l'analyse par Kaspersky Endpoint Security. La modification des règles de cette chaîne s'opère à l'aide des outils du système d'exploitation. Lors de la suppression de l'application, la chaîne de règles kesl_bypass dans iptables et ip6tables est supprimée uniquement si elle était vide.

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 le trafic réseau entrant et sortant via des ports spécifiques du protocole de données sélectionnés.

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. Une priorité d'exécution des règles dynamiques est supérieure à une priorité de règles de paquet 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 un ensemble de règles dynamiques (à l'aide de la commande `kesl-control -F --query`), mais vous ne pouvez pas en modifier les paramètres.

À propos des noms de zone de réseau prédéfinies

Une *zone réseau prédéfinie* est un groupe spécifique d'adresses ou de sous-réseaux IP. En utilisant une zone réseau prédéfinie, 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. La zone réseau peut être utilisée comme valeur du paramètre d'adresse distante lors de la création d'une règle de paquet réseau. Kaspersky Endpoint Security comporte trois zones réseau prédéfinies avec des noms spécifiques :

- **Publics**. Ajoutez une adresse réseau ou un sous-réseau à cette zone s'ils sont affectés à des réseaux non protégés par une application antivirus, un pare-feu ou un filtre (réseau de cybercafé par exemple).
- **Local**. Ajoutez une adresse réseau ou un sous-réseau à cette zone s'ils sont affectés à des réseaux dont les utilisateurs ont accès aux fichiers et imprimantes sur ce périphérique (LAN ou réseau domestique par exemple).
- **De confiance**. Cette zone est destinée à un réseau sécurisé dans lequel le périphérique n'est pas exposé aux attaques ou aux tentatives d'accès non autorisées.

Vous ne pouvez pas créer ou supprimer une zone réseau. Vous pouvez ajouter ou supprimer des adresses IP ou des sous-réseaux de la zone réseau.

Gestion du pare-feu dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de gestion du pare-feu dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection de base** → **Gestion du pare-feu**).

Paramètres du module Gestion du pare-feu

Paramètre	Description
Gestion du pare-feu activée/désactivée	Ce bouton bascule active ou désactive la Gestion du pare-feu. Le bouton bascule est désactivé par défaut.
Règles de paquet réseau	Cliquez sur le lien **Configurer les règles pour les paquets réseau** pour ouvrir la fenêtre **Règles de paquet réseau**. Cette fenêtre permet de configurer une liste de règles de paquets réseau exécutées par le composant Gestion du pare-feu lorsqu'il détecte la tentative de connexion réseau.
Réseaux disponibles	Cliquez sur le lien **Configurer les réseaux disponibles** pour 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.
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. Cette 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 périphériques dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
Adresse distante	Adresses réseau des appareils distants qui peuvent envoyer et/ou recevoir des paquets réseau.
Direction	Direction de l'activité réseau contrôlée.
Protocole	Type de protocole de transfert de données pour lequel l'activité réseau est surveillée.
Ports locaux	Numéros de port des appareils locaux entre lesquels la connexion est contrôlée.
Ports distants	Numéros de port des appareils distants entre lesquels la connexion est surveillée.
Type ICMP	Type ICMP. Le module Gestion du pare-feu contrôle les messages d'un type spécifié envoyés par un hôte ou une passerelle.
Code ICMP	Code ICMP. Le module Gestion du pare-feu surveille 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.
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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Règle de paquet réseau

Cette fenêtre permet de configurer la règle de paquet réseau.

Paramètres de règle de paquet de réseau

Paramètre	Description
Nom de la règle	Le champ de saisie pour le nom de la règle de paquet réseau.
Action	Dans la liste déroulante, 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).
Protocole	Dans la liste déroulante, 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**
Préciser le type d'ICMP	Cette case permet de préciser le type ICMP. Le module Gestion du pare-feu contrôlera les messages du type indiqué envoyés par l'hôte ou la passerelle. Si cette case est cochée, le champ de saisie du type ICMP s'affiche. Cette case s'affiche uniquement si les protocoles de transfert de données **ICMP** ou **ICMPv6** ont été sélectionnés dans la liste déroulante **Protocole**. La case est décochée par défaut.
Préciser le	Cette case permet de préciser le code ICMP. Le module Gestion du pare-feu surveillera les

code ICMP	messages du type spécifié (dans le champ sous la case **Préciser le type d'ICMP**) et avec le code spécifié (dans le champ sous la case **Préciser le code ICMP**) envoyés par l'hôte ou la passerelle. Si cette case est cochée, le champ de saisie du code ICMP s'affiche. Cette case s'affiche uniquement si les protocoles de transfert de données **ICMP** ou **ICMPv6** ont été sélectionnés dans la liste déroulante **Protocole** ; de plus, elle n'est visible que si vous avez cochez la case **Préciser le type d'ICMP**. La case est décochée par défaut.
Direction	Cette liste déroulante permet de définir la direction de l'activité réseau surveillée : • **Paquets entrants** (valeur par défaut). Si cet élément est sélectionné, le module Gestion du pare-feu contrôle les paquets entrants. • **Entrant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle l'activité réseau entrante. • **Entrants/Sortants**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle à la fois l'activité réseau entrante et sortante. • **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 les paquets sortants. • **Sortant**. Si cet élément est sélectionné, le module Gestion du pare-feu contrôle l'activité réseau sortante.
Adresse distante	Dans la liste déroulante, vous pouvez préciser les adresses réseau des périphériques distants qui peuvent envoyer et recevoir des paquets réseau. • **Toute adresse** (valeur par défaut). Si cet élément est sélectionné, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des périphériques distants avec toute adresse IP. • **Toutes les adresses sous-réseau**. Si vous avez sélectionné cette option, la règle du réseau contrôle les paquets réseau envoyés et reçus par des périphériques distants avec des adresses IP associées au type de réseau sélectionné dans la liste déroulante : **Réseaux publics**, **Réseaux locaux** ou **Réseaux approuvés**. • **Adresse spécifiée**. Si cet élément est sélectionné, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des périphériques distants portant les adresses IP spécifiées dans le champ **Adresse**.
Préciser les ports distants	Cette case permet de spécifier les numéros de port des périphériques distants entre lesquels la connexion doit être contrôlée. Si cette case est cochée, le champ de saisie des numéros de port s'affiche. Cette case s'affiche uniquement si les protocoles de transfert de données **TCP** ou **UDP** ont été sélectionnés dans la liste déroulante **Protocole**. La case est décochée par défaut.
Adresse locale	Dans la liste déroulante, vous pouvez renseigner les adresses réseau des périphériques 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 périphériques hébergeant

	Kaspersky Endpoint Security et portant n'importe quelle adresse IP. • **Adresse spécifiée**. Si cet élément est sélectionné, la règle du réseau contrôle les adresses réseau des périphériques spécifiées dans le champ **Adresse** hébergeant Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
Préciser les ports locaux	Cette case permet de spécifier les numéros de port des périphériques locaux entre lesquels la connexion doit être contrôlée. Si cette case est cochée, le champ de saisie des numéros de port s'affiche. Cette case s'affiche uniquement si les protocoles de transfert de données **TCP** ou **UDP** ont été sélectionnés dans la liste déroulante **Protocole**. La case est décochée par défaut.
Enregistrer les événements	Cette case permet de définir si les actions de la règle de réseau doivent être prises en compte dans le rapport. Si la case est cochée, l'application enregistre les actions des règles du réseau dans le rapport. Si la case est décochée, l'application n'enregistre pas les actions des règles du réseau dans le rapport. La case est décochée par défaut.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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 Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de gestion du pare-feu dans les propriétés de la stratégie (**Protection de base** → **Gestion du pare-feu**).

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**. Cliquez sur celui-ci pour ouvrir la fenêtre **Règles de paquet 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**. Cliquez sur celui-ci pour 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.
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. Cette 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 périphériques dotés de Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
Adresse distante	Adresses réseau des appareils distants 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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Ajout d'une règle de paquet réseau

Cette fenêtre permet de configurer les paramètres de la règles de paquet réseau ajouté.

Paramètres de règle de paquet de 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**
Direction	Vous pouvez définir la direction de l'activité réseau surveillée : • **Paquets entrants**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle les paquets entrants. • **Entrant**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle l'activité réseau entrante. • **Entrants/Sortants**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle à la fois l'activité réseau entrante et sortante. • **Paquets entrants/sortants**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle à la fois les paquets entrants et sortants. • **Paquets sortants**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle les paquets sortants. • **Sortant**. Si cette option est sélectionnée, le module Gestion du pare-feu contrôle l'activité réseau sortante.
Type ICMP	Vous pouvez indiquer le type ICMP. Le module Gestion du pare-feu contrôlera les messages du type indiqué envoyés par l'hôte ou la 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 les numéros de port des périphériques distants 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 les numéros de port des périphériques 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 distantes	Vous pouvez préciser les adresses réseau des périphériques 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 périphériques distants avec toute adresse IP. • **Adresse spécifiée**. Si vous sélectionnez cette option, la règle du réseau contrôle les paquets réseau envoyés et/ou reçus par des périphériques distants portant les adresses IP spécifiées dans le champ en-dessous. • **Par type de réseau**. Si vous avez sélectionné cette option, la règle du réseau contrôle les paquets réseau envoyés et reçus par des périphériques 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 périphériques 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 périphériques hébergeant Kaspersky Endpoint Security et portant n'importe quelle adresse IP. • **Adresse spécifiée**. Si vous avez sélectionné cette option, la règle du réseau contrôle les adresses réseau des périphériques spécifiées dans le champ ci-dessous dotés Kaspersky Endpoint Security et qui peuvent envoyer et/ou recevoir des paquets réseau.
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 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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 préinstallée 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 d'une tâche préinstallée à l'aide de la commande de gestion des paramètres des tâches.

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 Kaspersky Endpoint Security 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`	Nom de la règle de paquet réseau.	Valeur par défaut : `Packet rule #<n>`, où n est l'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 périphériques distants 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` à `65535`.
`LocalPorts`	Numéros de port des périphériques 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` à `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.
`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` : contrôle les connexions entrantes. `Outgoing` ou `Out` : contrôle les connexions sortantes. `IncomingPacket` ou `InPacket` : contrôle les paquets entrants. `OutgoingPacket` ou `OutPacket` : contrôle les paquets sortants.

		`IncomingOutgoingPacket` ou `InOutPacket` : contrôle les paquets entrants et sortants.
`RemoteAddress`	Adresses réseau des périphériques distants qui peuvent envoyer et recevoir des paquets réseau.	`Any` (valeur par défaut) : contrôle les paquets réseau envoyés et/ou reçus par des périphériques 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/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.
`LocalAddress`	Adresses réseau des périphériques 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 périphériques 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/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.
`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.		
`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 de paquets réseau dans 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>[:<plage de
ports>]] [--local <adresse locale>[:<plage de ports>]] [--at <index>]
```

où :

- `--name <nom de la règle>` : nom de la règle de paquet réseau.
- `--action <action>` : action à réaliser sur les connexions définies dans cette règle de paquet réseau.
- `--protocol <протокол>` : type de protocole de transfert de données pour lequel vous souhaitez surveiller l'activité réseau.
- `--direction <direction>` : direction de l'activité réseau surveillée.
- `--remote <adresse distante[:<plage de ports>]>` : adresse réseau de l'appareil à distance. Vous pouvez spécifier le nom d'une zone réseau prédéfinie comme adresse distante.
- `--local <adresse locale[:<plage de ports>]>` : adresse réseau de l'appareil sur lequel l'application Kaspersky Endpoint Security est installée.
- `--at <index>` : index 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.

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 <index>`

où :

- `--name <nom de la règle>` : nom de la règle de paquet réseau.
- `--index <index>` : index actuel de la règle dans la liste des règles de 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 <index>`
- `kesl-control --move-rule --index <index> --at <index>`

où :

- `--name <nom de la règle>` : nom de la règle de paquet réseau.
- `--index <index>` : index actuel de la règle dans la liste des règles de paquets réseau.
- `--at <index>` : nouvel index de la règle dans la liste des règles de paquets réseau.

Configuration des zones réseau dans la ligne de commande

Pour ajouter une adresse réseau à la zone, exécutez la commande suivante :

`kesl-control --add-zone --zone <zone> --address <adresse>`

où :

- `--zone <zone>` : nom prédéfini de la zone réseau. Valeurs possibles : `Public`, `Local`, `Trusted`.
- `--address <adresse>` : adresse réseau ou sous-réseau.

Pour supprimer une adresse réseau d'une zone, exécutez l'une des commandes suivantes :

- `kesl-control --del-zone --zone <zone> --address <adresse>`
- `kesl-control --del-zone --zone <zone> --index <index de l'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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

Les connexions actuelles pour les ports TCP interceptés sont réinitialisées lorsque la protection contre les menaces réseau est activée.

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 sécurisées pour vérifier le trafic HTTPS.

  Pour analyser le trafic FTP, le contrôle de tous les ports réseau doit être configuré dans les paramètres d'analyse des connexions sécurisées.

Lorsque vous ouvrez un site, l'application effectue les opérations suivantes :

1. Vérifie la sécurité du site Internet à l'aide des bases de l'application téléchargées.
2. Vérifie la sécurité du site Internet à l'aide d'une analyse heuristique, si cette fonction est activée.

Lors de l'analyse heuristique, l'application 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 Internet 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 Internet.

Lors d'une tentative d'ouverture d'un site Internet 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.

Kaspersky Endpoint Security ajoute à la liste de la table mangle des utilitaires iptables et ip6tables une chaîne d'autorisation spéciale de règles kesl_bypass qui vous permet d'exclure le trafic de l'analyse réalisée par l'application. Si des règles d'exclusion de trafic sont configurées dans la chaîne, elles affectent le fonctionnement du module Protection contre les menaces Internet.

Configuration de la protection contre les menaces Web dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de protection contre les menaces Internet dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection de base**→ **Protection contre les menaces Internet**).

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Protection contre les menaces Internet activée / désactivée	Ce bouton bascule active ou désactive la Protection contre les menaces Internet. Le bouton bascule est désactivé par défaut.
Action en cas de détection d'une menace	Cette section permet d'indiquer l'action que l'application effectue sur les ressources Internet où un objet dangereux a été détecté : • **Informer** l'utilisateur lorsqu'un objet dangereux est détecté dans le trafic Internet. Le composant Protection contre les menaces Internet autorise le téléchargement de cet objet sur le périphérique. 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.

	• **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).
Détecter les objets malveillants	Cette case active ou désactive la vérification des liens par rapport aux bases de données d'adresses Internet malveillantes. Cette 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. Cette 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.
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.
Adresses Internet de confiance	Ce tableau contient les adresses et les 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. 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). Par défaut, le tableau est vide. Vous pouvez ajouter, modifier et supprimer des adresses Internet dans le tableau. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Adresse Internet

Cette fenêtre permet d'ajouter une adresse Internet ou un masque d'adresse Internet à la liste des adresses Internet de 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.

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).

Configuration de la protection contre les menaces Web dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de protection contre les menaces Internet dans les propriétés de la stratégie (**Protection de base → 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 composant 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. Le composant Protection contre les menaces Internet autorise le téléchargement de cet objet sur le périphérique. 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.

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).

Vous pouvez ajouter, modifier et supprimer des adresses Internet dans la liste.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Adresse Internet

Cette fenêtre permet d'ajouter une adresse Internet ou un masque d'adresse Internet à la liste des adresses Internet de 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.

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. Cette 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. Cette 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.
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 Web dans 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 préinstallée 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 protection contre les menaces Internet en modifiant les paramètres de la tâche préinstallée 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.
`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 légales 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 des connexions chiffrées

Les paramètres d'analyse des connexions sécurisées sont utilisés dans le fonctionnement des modules Protection contre les menaces Internet et Contrôle Internet. Le module Protection contre les menaces Internet peut déchiffrer et inspecter le trafic réseau transmis via des connexions chiffrées. Par défaut, l'analyse des connexions chiffrées est activée.

Vous pouvez activer ou désactiver l'analyse des connexions chiffrées, ainsi que configurer les paramètres d'analyse :

- Sélectionner l'action que l'application entreprend lorsqu'elle détecte un certificat non approuvé.
- Sélectionner l'action à effectuer lorsqu'une erreur d'analyse de connexion chiffrée 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 chiffrées 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 une liste de ports réseau contrôlés par l'application. Vous pouvez spécifier certains ports réseaux ou certaines plages de ports réseaux à analyser.

Lors de la modification des paramètres d'analyse des connexions chiffrées, l'application génère l'événement *NetworkSettingsChanged*.

Configuration de l'analyse des connexions chiffrées dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'analyse des connexions chiffrées dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres réseau**).

Paramètres d'analyse des connexions chiffrées

Paramètre	Description
Analyse des connexions chiffrées activée/désactivée	Ce bouton bascule active ou désactive l'analyse des connexions chiffrées. Le bouton bascule est activé par défaut.
Certificats racines de confiance	Le lien **Administrer les certificats racines de confiance** ouvre la fenêtre Certificats racines de confiance, dans laquelle vous pouvez configurer la liste des certificats de confiance. Les certificats de confiance sont utilisés lors de l'analyse des connexions chiffrées.
Navigation vers un domaine dont le certificat n'est pas fiable	Vous pouvez sélectionner l'action que l'application entreprendra lors du déplacement vers 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.

Accéder à un domaine avec une erreur lors de l'analyse des connexions chiffrées	Vous pouvez sélectionner l'action que l'application entreprendra lors du déplacement vers un domaine avec une erreur lors de la vérification des connexions sécurisées : • **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	Vous pouvez choisir la manière dont l'application vérifie 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	Le lien **Configurer les domaines de confiance** ouvre la fenêtre **Domaines de confiance**, dans laquelle vous pouvez configurer la liste des noms de domaine de confiance.
Contrôler 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 ne vérifie que les ports réseau indiqués dans l'option **Ports contrôlés**. Cette option est la sélection par défaut.
Ports contrôlés	Cliquez sur le lien **Configurer les paramètres des ports réseau** pour ouvrir la fenêtre **Ports contrôlés**, où vous pouvez préciser les ports réseau que l'application vérifiera.

Fenêtre Certificats racines de confiance

Vous pouvez configurer la liste des certificats que l'application Kaspersky Endpoint Security considérera comme fiables. La liste des certificats de confiance est utilisée lors de l'analyse des connexions cryptées.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre d'ajout d'un certificat de confiance

Dans cette fenêtre, vous pouvez ajouter un certificat que l'application Kaspersky Endpoint Security considérera comme fiable.

Le lien **Ajouter un certificat** ouvre une fenêtre standard de sélection d'un fichier. Spécifiez le chemin d'accès au fichier au format DER ou PEM contenant le certificat.

Après que vous avez sélectionné un fichier de certificat, la fenêtre affiche des informations sur le certificat et le chemin d'accès au fichier.

Fenêtre Domaines de confiance

Cette liste contient les noms de domaine et les masques de nom de domaine qui seront exclus de l'analyse des connexions chiffrées.

Exemple : `*exemple.fr`. Par exemple, `*exemple.fr/*` 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Ports contrôlés

Le tableau contient les ports réseau que l'application analysera si l'option **Contrôler uniquement les ports réseau sélectionnés** est sélectionnée dans la fenêtre **Paramètres réseau** dans le groupe **Ports contrôlés**.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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 de l'analyse des connexions chiffrées dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres d'analyse des connexions chiffrées dans les paramètres de la stratégie (**Paramètres généraux** → **Paramètres réseau**).

Paramètres d'analyse des connexions chiffrées

Paramètre	Description
Activer l'analyse des connexions chiffrées	La case active ou désactive l'analyse des connexions chiffrées. Cette case est cochée par défaut.
Navigation vers un domaine dont le certificat n'est pas fiable	Dans la liste déroulante, vous pouvez sélectionner l'action que l'application exécutera lors du déplacement vers un domaine avec un certificat douteux : • **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.
Accéder à un domaine avec une erreur lors de l'analyse des connexions chiffrées	Dans la liste déroulante, vous pouvez sélectionner l'action que l'application exécutera lors du déplacement vers un domaine avec une erreur lors de la vérification des connexions sécurisées : • **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	Dans la liste déroulante, vous pouvez choisir la manière dont l'application vérifie 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** qui ouvre la fenêtre Certificats racines de confiance dans laquelle vous pouvez configurer une liste des certificats de confiance. Les certificats de confiance sont utilisés lors de l'analyse des connexions chiffrées.
Paramètres des ports réseau	Le groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre Ports contrôlés.

Fenêtre Domaines de confiance

Cette liste contient les noms de domaine et les masques de nom de domaine qui seront exclus de l'analyse des connexions chiffrées.

Exemple : `*exemple.fr`. Par exemple, `*exemple.fr/*` 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Certificats racines de confiance

Vous pouvez configurer la liste des certificats que l'application Kaspersky Endpoint Security considérera comme fiables. La liste des certificats de confiance est utilisée lors de l'analyse des connexions cryptées.

Les informations suivantes sont affichées pour chaque certificat :

- **Objet** : l'objet du certificat ;
- **Numéro de série** : numéro de série du certificat ;
- **Délivré par** : l'émetteur du certificat ;

- **Valide à partir du** : date de début de validité du certificat ;
- **Date d'expiration** : date de fin de validité du certificat ;
- **Empreinte SHA256** : empreinte du certificat SHA256.

Par défaut, la liste des certificats est vide.

Vous pouvez ajouter et supprimer des certificats.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Ajout d'un certificat

Dans cette fenêtre, vous pouvez 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 Ports contrôlés

Paramètres des ports réseau

Paramètre	Description
Contrôler 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 la sélection 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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 de l'analyse des connexions chiffrées dans la ligne de commande

La ligne de commande fournit des commandes de gestion spéciales pour gérer les paramètres d'analyse des connexions chiffrées. À l'aide des commandes de gestion des paramètres d'analyse des connexions chiffrées, vous pouvez :

- Configurer les paramètres d'analyse des connexions chiffrées.
- Afficher les exclusions depuis l'analyse des connexions chiffrées.
- Effacer la liste des domaines que l'application a automatiquement exclus de l'analyse.
- Gérer la liste des certificats que l'application considère comme fiables.

Affichage et modification des paramètres de vérification des connexions chiffrées

Vous pouvez afficher et modifier les paramètres d'analyse des connexions chiffrées à l'aide des commandes de gestion spéciales :

- Vous pouvez afficher les valeurs actuelles des paramètres d'analyse des connexions chiffrées vers la console ou vers un fichier de configuration. Vous pouvez utiliser ce fichier pour modifier les paramètres.
- Vous pouvez modifier tous les paramètres d'analyse des connexions chiffrées 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 d'analyse des connexions chiffrées.
- Vous pouvez modifier des paramètres individuels à l'aide de commutateurs 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 des connexions chiffrées.

Pour afficher les valeurs actuelles des paramètres d'analyse des connexions chiffrées à la console, exécutez la commande suivante :

```
kesl-control --get-net-settings [--json]
```

où `--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 d'analyse des connexions chiffrées 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>` : chemin d'accès au fichier dans lequel les paramètres de l'analyse des connexions chiffrées 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 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 des connexions chiffrées à l'aide d'un fichier de configuration :

1. Affichez les paramètres généraux de l'application dans un 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>` : chemin complet vers le fichier de configuration avec les paramètres d'analyse des connexions chiffrées.
   - `--json` : importer les paramètres d'un fichier de configuration au format JSON dans l'application. 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 des connexions chiffrées spécifiées dans le fichier seront importées dans l'application.

Pour modifier les paramètres d'analyse des connexions chiffrées 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>` est le nom et la valeur de l'un des paramètres d'analyse des connexions chiffrées.

Les valeurs des paramètres spécifiés pour analyser les connexions chiffrées 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 un utilisateur, 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 de confiance

Pour ajouter un certificat à la liste des certificats 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 souhaitez ajouter, au format PEM ou DER.

Pour supprimer un certificat de la liste des certificats de confiance, exécutez la commande suivante :

```
kesl-control --remove-certificate <objet du certificat>
```

Pour consulter la liste des certificats 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.

Protection contre les menaces réseaux

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

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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.

Pour vérifier le trafic réseau, la tâche de protection contre les menaces réseaux 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.

La protection contre les menaces réseau est activée par défaut si les paramètres de protection contre les menaces réseau sur l'appareil sont définis via une stratégie. Si votre appareil utilise des paramètres configurés localement, la protection contre les menaces réseau est désactivée par défaut.

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*.

Kaspersky Endpoint Security ajoute à la liste de la table mangle des utilitaires iptables et ip6tables une chaîne d'autorisation spéciale de règles kesl_bypass qui vous permet d'exclure le trafic de l'analyse réalisée par l'application. Si des règles d'exclusion de trafic sont configurées dans la chaîne, elles affectent le fonctionnement de la tâche Protection contre les menaces réseaux. Par exemple, pour exclure le trafic http sortant, vous devez ajouter la commande suivante : `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Configuration de la protection contre les menaces réseau dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de protection contre les menaces réseau dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection de base**→ **Protection contre les menaces réseau**).

Paramètres du module Protection contre les menaces réseau

Paramètre	Description
Protection contre les menaces réseaux activée / désactivée	Ce bouton bascule active ou désactive la Protection contre les menaces réseaux. Le bouton bascule est activé 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 du périphérique attaquant et consigner les informations sur l'activité réseau détectée (valeur par défaut) dans le journal.
Blocage des périphériques attaquants activé / désactivé	Ce bouton bascule active ou désactive le blocage de l'activité réseau en cas de détection d'une tentative d'attaque réseau. Le bouton bascule est activé par défaut.
Bloquer l'hôte attaquant pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un périphérique attaquant (en minutes). Une fois le délai spécifié écoulé, l'application Kaspersky Endpoint Security autorise l'activité réseau en provenance de ce périphérique. Valeurs disponibles : entier de 1 à 32768. Valeur par défaut : 60.
Exclusions	Le tableau contient une liste d'adresses IP à partir desquelles les attaques réseau ne sont pas bloquées. Par défaut, la liste est vide. Vous pouvez ajouter, configurer et supprimer des adresses IP dans le tableau. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Adresse IP

Vous pouvez ajouter et modifier des adresses IP au départ desquelles l'application Kaspersky Endpoint Security ne bloquera pas les attaques réseau.

Adresses IP

Paramètre	Description
Saisissez l'adresse IP	Champ de saisie pour une adresse IP. Vous pouvez spécifier des adresses IP aux formats IPv4 et IPv6.

Configuration de la protection contre les menaces réseau dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de protection contre les menaces réseau dans les propriétés de la stratégie (**Protection de base** → **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 réseaux. Cette case est cochée 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 du périphérique 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. Cette case est cochée par défaut.
Bloquer l'hôte attaquant pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un périphérique attaquant (en minutes). Une fois le délai spécifié écoulé, l'application Kaspersky Endpoint Security autorise l'activité réseau en provenance de ce périphérique. Valeurs disponibles : entier de 1 à 32768. Valeur par défaut : 60.
Exclusions	Le groupe de paramètres contient le bouton **Configurer** qui ouvre la fenêtre **Exclusions** dans laquelle vous pouvez renseigner la liste d'adresse IP qui ne seront pas bloquées en cas d'attaque réseau en provenance de celles-ci.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre Adresse IP

Vous pouvez ajouter et modifier des adresses IP au départ desquelles l'application Kaspersky Endpoint Security ne bloquera pas les attaques réseau.

Adresses IP

Paramètre	Description
Saisissez l'adresse IP	Champ de saisie pour une adresse IP. Vous pouvez spécifier des adresses IP aux formats IPv4 et IPv6.

Configuration de la protection contre les menaces réseau dans 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 préinstallée 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 protection contre les menaces réseau en modifiant les paramètres de la tâche réinstallée Protection contre les menaces réseau.

Paramètres de la tâche de protection contre les menaces réseaux

Paramètre	Description	Valeurs
`ActionOnDetect`	Actions à entreprendre 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) : bloque l'activité réseau et consigne dans le journal les informations la concernant.
`BlockAttackingHosts`	Blocage de l'activité réseau à partir des périphériques 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 périphériques (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 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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

Si la protection contre le chiffrement est activée, Kaspersky Endpoint Security vérifie les actions des appareils distants 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 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 par 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 par 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 par 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.

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 par chiffrement dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de protection contre le chiffrement dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection avancée** → **Protection contre le chiffrement**).

Paramètres du module Protection contre le chiffrement

Paramètre	Description
Protection contre le chiffrement activée / désactivée	Ce bouton bascule active ou désactive la protection des fichiers des répertoires locaux avec accès réseau par protocoles SMB/NFS contre le chiffrement à distance malveillant. Le bouton bascule est désactivé par défaut.
Zones de protection	Cliquez sur le lien **Configurer la zone de protection** pour ouvrir la fenêtre **Zones de protection**.
Action lorsque le chiffrement est détecté	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 hôte douteux pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un périphérique douteux (en minutes). 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 4294967295. Valeur par défaut : 30.
Exclusions	Cliquez sur le lien **Configurer les exclusions** pour ouvrir la fenêtre **Zones d'exclusion**.
Exclusions d'après le masque	Cliquez sur le lien **Configurer les exclusions par masque** pour ouvrir la fenêtre **Exclusions d'après le masque**.

Fenêtre Zones de protection

Le tableau contient les zones de protection du composant Protection contre le chiffrement. 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 de protection

Paramètre	Description
Nom de la zone	Nom de la zone de protection.
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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Kaspersky Endpoint Security protège 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 d'ajout d'une zone de protection

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	Champ de saisie du nom de la zone de protection. Ce nom sera affiché dans le tableau de

zone	la fenêtre **Zones de protection**. 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 composant. Si cette case est décochée, l'application ne traite pas cette zone de protection pendant le fonctionnement du composant. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement du composant en cochant la case. Cette 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. • **Partagé** affiche les ressources du système de fichiers du serveur accessibles via le protocole Samba ou NFS. • **Tous les systèmes partagés** affiche les ressources du système de fichiers du serveur 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. La liste déroulante est accessible si l'élément **Général** est sélectionné dans la liste déroulante des systèmes de fichiers.
Chemin	Champ de saisie du chemin du répertoire à 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Ce champ est accessible si le type **Local** a été choisi dans la liste déroulante des systèmes de fichiers. Le champ ne peut être vide. Par défaut, c'est le chemin **/** qui est utilisé (dossier racine).

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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Zones d'exclusion

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette 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 le périphérique. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >] et [image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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).

Configuration de la protection par chiffrement dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de protection contre le chiffrement dans les propriétés de la stratégie (**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**. Cliquez sur celui-ci pour 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
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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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 composant. Si cette case est décochée, l'application ne traite pas cette zone de protection pendant le fonctionnement du composant. Par la suite, vous pouvez inclure cette zone dans les paramètres du fonctionnement du composant en cochant la case. Cette case est cochée par défaut.
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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Paramètres de la protection

Paramètres de la protection

Paramètre	Description
Action lorsque le chiffrement est détecté	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 hôte douteux pendant (minutes)	Champ qui permet de spécifier la durée de blocage d'un périphérique douteux (en minutes). À l'expiration du délai indiqué, l'application Kaspersky Endpoint Security retire les hôtes douteux de la liste des périphériques 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 4294967295. Valeur par défaut : 30.

Fenêtre Zones d'exclusion

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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. Cette case est cochée par défaut.
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 le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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 :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name < nom >]/< chemin d'accès au répertoire local >`
- `[image-id:< identifiant >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >]/< chemin d'accès au répertoire local >`

Vous pouvez également utiliser des combinaisons uniques des tags `[container-id: < identifiant >], [container-name:< nom >], [image-id:< identifiant >] et [image-name:< nom >]/< chemin d'accès au répertoire local >.`

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:< nom >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[container-id:< identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`
- `[image-name:< nom >][image-id :< identifiant >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][container-id :< identifiant >][image-name :< nom >]/< chemin d'accès au répertoire local >`
- `[container-name:< nom >][image-id:< identifiant >][container-id: < identifiant >][image-name:< nom >]/< chemin d'accès au répertoire local >`

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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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. Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse. Le bouton est accessible si au moins un masque est sélectionné dans la liste. Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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 de l'analyse, 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.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime le masque sélectionné des noms des fichiers exclus de l'analyse.

Le bouton est accessible si au moins un masque est sélectionné dans la liste.

Cliquez sur le masque pour ouvrir la fenêtre **Masque d'objet**. Cette fenêtre permet de modifier, dans le champ **Définir le masque de l'objet**, le modèle des noms des fichiers que Kaspersky Endpoint Security exclut de l'analyse.

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).

Configuration de la protection par chiffrement dans 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 Protection contre le chiffrement

Paramètre	Description	Valeurs
ActionOnDetect	Active les blocages des périphériques 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 périphérique compromis est bloqué et si vous modifiez la valeur du paramètre `BlockTime`, la durée de blocage de ce périphérique 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 la valeur 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	Valeur par défaut : `All shared directories`.

	complémentaires sur la zone de protection.	
`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).
`Path`	Chemin d'accès au répertoire contenant les objets protégés.	`< chemin d'accès au répertoire local >` : protéger le 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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` : protège les ressources partagées via SMB. `Shared:NFS` : protège les ressources partagées 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).
`Path`	Chemin d'accès au répertoire contenant les objets à exclure de la protection.	`< chemin d'accès au répertoire local >` : exclut 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 le périphérique client via le protocole NFS. `Mounted:SMB` : exclure de la protection les répertoires distants montés sur le périphérique client via le protocole Samba. `AllRemoteMounted` : exclut de la protection tous les répertoires distants montés sur le périphérique 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*.

-H – préfixe indiquant 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 réseaux.

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>` : Adresse IP de l'appareil ou du sous-réseau (IPv4 /IPv6, y compris les adresses abrégées). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

Pour consulter la liste des périphériques 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 périphériques, saisissez la commande suivante :

```
kesl-control --allow-hosts <adresse>
```

où `<adresse>` est 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.

Pour utiliser le module, vous devez posséder la licence qui couvre cette fonction.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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.
- Sélectionnez l'action que Kaspersky Endpoint Security effectuera lorsqu'il détectera une tentative de lancement d'une application répondant aux règles : *appliquer les règles* ou *tester les règles* et informer d'une tentative de lancement d'une application répondant aux règles.

Vous pouvez obtenir des informations sur les applications installées sur les appareils protégés à l'aide de la tâche Inventaire.

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. Exception : cat script.py | python.

À propos des règles du contrôle des applications

Une *règle du côntrole des applications* est un ensemble de paramètres qui contiennent les conditions de déclenchement de la règle et les actions du module Côntrole 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'application* est un groupe d'applications qui possèdent des caractéristiques communes. 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.
- *Désactivé* : la règle est désactivée et n'est pas utilisée pour le contrôle des applications.
- *Essai* : 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.

Configuration du contrôle des applications 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** → **Contrôle de sécurité** → **Contrôle des applications**).

Paramètres du module Contrôle des applications

Paramètre	Description
Contrôle des applications activé / désactivé	Le commutateur active ou désactive le Contrôle des appareils. Le bouton bascule est désactivé par défaut.
Action en cas d'exécution d'applications interdites par les règles	Action que Kaspersky Endpoint Security exécutera lorsqu'il détectera une tentative de démarrage d'une application qui répond aux règles configurées : • **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. • **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.
Mode du Contrôle des applications	Mode de fonctionnement du composant 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	Cliquez sur le lien **Configurer la règle** pour 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). Lorsque vous sélectionnez cet élément de la liste, l'application applique les règles spécifiées dans la stratégie ainsi que les règles locales configurées sur l'appareil protégé.

Fenêtre Règles du Contrôle des applications

Le tableau **Règles du Contrôle des applications** contient des onglets avec des règles pour chaque mode de fonctionnement du Contrôle des applications : **Liste de refus (active)** et **Liste d'autorisation**. Par défaut, le tableau des règles du contrôle des applications des deux onglets est vide.

Paramètres des règles du contrôle des applications

Paramètre	Description
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 ajouter, modifier et supprimer des règles du contrôle des applications.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Fenêtre Règle du Contrôle des applications

Cette fenêtre permet de configurer les paramètres de la règle du Contrôle des applications.

Configuration de la règle du Contrôle des applications

Paramètre	Description
Description de la règle	Description de la règle du Contrôle des applications.
État	Vous pouvez 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	Cliquez sur le lien **Sélectionner une catégorie** pour ouvrir la fenêtre **Catégories d'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. 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** : le type d'accès (autorisation ou interdiction de lancer des applications). Le bouton bascule active ou désactive le 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Catégories d'applications

Cette fenêtre vous permet d'ajouter une nouvelle catégorie ou de configurer les paramètres de catégorie pour une règle de 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 catégorie	Barre de recherche pour les catégories d'applications ajoutées.
Ajouter	Cliquez sur ce bouton pour lancer l'assistant de création d'une catégorie. Suivez les indications de l'assistant.
Modifier	Cliquez sur le bouton pour ouvrir la fenêtre des propriétés des catégories qui permet de modifier les paramètres des catégories.
Supprimer	Lorsque vous cliquez sur le bouton, la catégorie sélectionnée est supprimée. La catégorie **Golden Image (locale)** ne peut pas être supprimée.

Fenêtre Sélectionner l'utilisateur ou le groupe

Cette fenêtre permet d'indiquer l'utilisateur local ou de domaine ou le groupe d'utilisateurs pour lequel vous souhaitez configurer la règle.

Configuration de la règle du Contrôle des applications

Paramètre	Description
Manuel	Si cette option est sélectionnée, dans le champ ci-dessous, vous devez saisir le nom de l'utilisateur local ou de domaine ou le nom du groupe d'utilisateurs qui sera soumis à la règle du Contrôle des applications.
Liste des groupes ou des utilisateurs	Si cette option est sélectionnée, dans la zone de recherche, vous pouvez saisir des critères de recherche pour le nom d'utilisateur ou le nom du groupe d'utilisateurs auquel la règle du Contrôle des applications s'appliquera, ou sélectionner le nom du groupe d'utilisateurs dans la liste ci-dessous.

Configuration du contrôle des applications dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres du contrôle des applications dans les paramètres de la stratégie (**Contrôle 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 du Contrôle des applications	Mode de fonctionnement du composant 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**. Cliquez sur celui-ci pour 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). Lorsque vous sélectionnez cet élément de la liste, l'application applique les règles spécifiées dans la stratégie ainsi 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 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/Modifier une règle**.

Vous pouvez ajouter, modifier et supprimer des règles du contrôle des applications.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Ajouter une nouvelle règle

Cette fenêtre permet de configurer les paramètres de la règle du contrôle des applications.

Ajout de la règle de 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	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Catégories d'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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Catégories d'applications

Cette fenêtre vous permet d'ajouter une nouvelle catégorie ou de configurer les paramètres de catégorie pour une règle de 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 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 indications de l'assistant.
Modifier	Cliquez sur le bouton pour ouvrir la fenêtre des propriétés des catégories qui permet de modifier les paramètres des catégories.

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 de contrôle des applications

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Nom d'utilisateur ou de groupe	Nom de l'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 dans 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 d'autorisations d'applications ou si vous interdisez le lancement de toutes les applications et/ou d'applications ayant un impact sur le fonctionnement de Kaspersky Endpoint Security, vous devrez exécuter la commande `kesl-control --set-settings` avec l'argument `--accept` lors de la modification des paramètres de la tâche à l'aide du fichier de configuration ou à l'aide des clés de la ligne de commande.

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 de contrôle des applications.

Paramètres de la tâche Contrôle des applications

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir 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 de 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 de 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 :		
`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 le nom du 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 le nom du 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	Vous pouvez utiliser des masques pour spécifier le nom du fichier.

	règle.	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 le nom du 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.
`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` : 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>` : nom d'un utilisateur auquel la règle est appliquée. `@<nom de groupe>` : nom d'un groupe d'utilisateurs auquel la règle est appliquée.
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` : 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 >` : nom d'un utilisateur auquel la règle est appliquée. `@< nom de groupe >` : nom d'un groupe d'utilisateurs auquel la règle est appliquée.

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>` : chemin d'accès au fichier de configuration avec les paramètres des catégories.

Le fichier avec les paramètres des catégories doit avoir la structure suivante :

```
[
   {
     "Exclude" : [ "(FilePath like <chemin d'accès complet au fichier exécutable de
    l'application>)", "(FileHash == <hachage du fichier exécutable>)" ],
     "GUID" : "<identifiant unique de la 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" : "<identifiant unique de la 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. Le paramètre `Name` est obligatoire ; si vous ne précisez pas le nom de la catégorie, elle ne sera pas créée ou sera supprimée. Le paramètre `GUID` est également obligatoire ; si vous ne le précisez pas, une erreur s'affichera et la catégorie ne sera pas créée. Le paramètre `GUID` doit être spécifié sans tirets.

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.

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>` : 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>` : chemin d'accès au fichier de configuration avec les paramètres des catégories.

Consultation de la liste des catégories créées

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.

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>` : chemin d'accès complet au fichier de configuration au format JSON dans lequel les paramètres seront affichés.
- `--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 d'applications créées, 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>` : noms des catégories sur lesquelles vous souhaitez afficher des 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 au format JSON, dans lequel sera affichée la liste des catégories.
- `--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 de contrôle des applications, exécutez la commande suivante :

```
kesl-control --get-settings 21 [--file <chemin d'accès au fichier de configuration>] [--json]
```

où :

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres seront affichés.

`--json` : afficher les données au format JSON.

Kaspersky Endpoint Security affichera les informations suivantes sur les règles de contrôle des applications :

- mode de fonctionnement du module Contrôle des applications ;
- l'action que le Contrôle des applications entreprendra lorsqu'il détectera 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 fonctionnement de la règle du Contrôle des applications ;
- nom de la catégorie des applications à laquelle la règle s'applique ;
- type d'accès attribué à l'utilisateur ou au groupe d'utilisateurs ;
- utilisateur ou un groupe d'utilisateurs auxquels la règle du contrôle des applications s'applique.

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 <chemin d'accès au fichier de configuration>] [--json]
```

où :

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés.

`--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
```

Analyse de l'inventaire

La tâche Analyse de l'inventaire permet d'obtenir des informations sur tous les fichiers exécutables des applications conservés sur les périphériques clients. L'obtention d'informations relatives aux applications installées sur les périphériques peut être utile dans la création des règles du contrôle des applications par exemple.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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).
- Activer ou désactiver l'ajout des applications détectées sur l'appareil par la tâche Inventaire à la catégorie des applications « Golden Image ».
- 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.

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 le périphérique 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 Analyse de l'inventaire

Paramètre	Description
Ajouter des fichiers à la catégorie Image dorée	La case active ou désactive l'ajout des applications détectées sur l'appareil par la tâche Analyse de l'inventaire à la catégorie des applications « Golden Image ». Si la case est cochée, vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles du contrôle des applications. La case est décochée par défaut.
Analyser tous les fichiers exécutables	La case active ou désactive l'analyse des fichiers exécutables. Cette 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). Cette case est cochée par défaut.
Analyser les scripts	La case active ou désactive l'analyse des scripts. Cette 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, configurer, supprimer, déplacer vers le haut ou déplacer vers le bas les zones d'inventaire dans le tableau. Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone dans le tableau. Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone 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. Cliquez sur le nom de la zone d'analyse pour ouvrir la fenêtre **<Nom de la zone d'analyse>**. Dans cette fenêtre, vous pouvez modifier les paramètres de la zone d'analyse choisie. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **<Nouvelle zone d'analyse>**. Cette fenêtre permet d'indiquer une nouvelle zone d'analyse.

Fenêtre d'ajout d'une zone d'analyse

Cette fenêtre permet d'ajouter ou de modifier une zone d'analyse pour la tâche d'analyse de l'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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 de la tâche. La liste contient par défaut le masque ***** (tous les objets). Vous pouvez ajouter, modifier et supprimer des masques. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 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

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

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 d'analyse de l'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. Cette 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 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

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 le périphérique 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 Analyse de l'inventaire

Paramètre	Description
Ajouter des fichiers à la catégorie Image dorée	La case active ou désactive l'ajout des applications détectées sur l'appareil par la tâche Analyse de l'inventaire à la catégorie des applications « Golden Image ». Si la case est cochée, vous pouvez utiliser la catégorie des applications « Golden Image » dans les règles du contrôle des applications. La case est décochée par défaut.
Analyser tous les fichiers exécutables	La case active ou désactive l'analyse des fichiers exécutables. Cette 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). Cette case est cochée par défaut.
Analyser les scripts	La case active ou désactive l'analyse des scripts. Cette case est cochée par défaut.
Zones d'inventaire	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Zone d'analyse**.

La section **Zones d'exclusion** de la tâche Analyse de l'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 Analyse de l'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.

Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone dans le tableau.

Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau.

Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau.

Le bouton est accessible dès que vous sélectionnez une zone 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.

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 Analyse de l'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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 Exclusions

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Zones d'exclusion	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Zones d'exclusion**. Cette fenêtre permet de définir la liste des zones d'exclusion du contrôle.

Fenêtre Zones d'exclusion

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.

Paramètres de zone d'exclusion

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 cette exclusion est appliquée par l'application.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

Fenêtre <Nouvelle zone d'exclusion>

Cette fenêtre permet d'ajouter ou de modifier des zones d'exclusion de l'analyse pour la tâche Analyse de l'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. Cette 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 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre. 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).

Inventaire dans la ligne de commande

Depuis la ligne de commande, vous pouvez inventorier les 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.

- Utilisation des tâches personnalisées d'inventaire (tâches de type *InventoryScan*). Vous pouvez démarrer, arrêter, suspendre et reprendre les tâches d'utilisateur manuellement et configurer la planification de lancement des tâches.

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'analyse de l'inventaire

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir pour la tâche Analyse de l'inventaire.

Paramètres de la tâche d'analyse de l'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.
`CreateGoldenImage`	Ajout des applications trouvées sur l'appareil par la tâche Analyse de l'inventaire à la catégorie des applications "Golden Image". Si vous utilisez le paramètre `CreateGoldenImage=Yes`, vous pouvez utiliser la catégorie des applications "Golden Image" dans les règles du contrôle des applications.	`Yes` : ajouter les applications détectées à la catégorie d'applications « Golden Image ». `No` (valeur par défaut) . ne pas ajouter les applications détectées à la catégorie d'applications Golden Image.
La section **[ScanScope.item_#]** contient les paramètres suivants :		
`AreaDesc`	La description de la zone d'inventaire contient des informations complémentaires sur 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	Valeur par défaut : `*` (analyser tous les objets).

	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.	
`Path`	Le chemin d'accès au répertoire contenant les objets à vérifier.	`< chemin d'accès au répertoire local >` : analyse les objets dans le répertoire indiqué. Valeur par défaut : `/usr/bin`
La section **[ExcludedFromScanScope.item_#]** contient les paramètres suivants.		
`AreaDesc`	La description de la zone d'exclusion d'inventaire contient des informations complémentaires sur la zone d'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 de l'analyse 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 le périphérique, 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 Analyse de l'inventaire.
- **Nombre d'applications**. Le nombre d'applications trouvées sur le périphérique.
- Liste des applications contenant les informations suivantes :

- **Chemin**. Chemin d'accès à l'application.
- **Hash**. La somme de hash de l'application.
- **Type**. Type d'application. Par exemple : `Script`, `Exécutable`.
- **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 Analyse de l'inventaire doit être exécutée à nouveau.

Contrôle des périphériques

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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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* pour interdire 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.

    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.
- **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 *En fonction 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.

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. 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 fanotify, le verrouillage de la lecture du répertoire n'est pas pris en charge.

Lorsque vous activez le module Contrôle des appareils pour la première fois, l'événement *L'accès à l'appareil est autorisé* est généré pour tous les appareils détectés avec un type d'appareil ou de bus connu, et lors des lancements ultérieurs, les événements répétés pour ces appareils ne sont pas générés s'il y a eu aucun changement dans les paramètres de contrôle de ces appareils.

Lorsque vous désactivez le module Contrôle des appareils, l'application déverrouille l'accès aux appareils bloqués.

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.
- Sélectionnez le mode d'accès au 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 périphériques de confiance* sont des périphériques auxquels les utilisateurs ont un accès complet. Vous pouvez ajouter des appareils à la liste des appareils de confiance par ID ou masque d'ID d'appareil. 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.

  Si vous contrôlez l'application à l'aide de la ligne de commande, vous pouvez afficher les ID des appareils connectés en exécutant la commande `kesl-control --get-device-list` sur l'appareil client.

  Si vous gérez une application à l'aide de Kaspersky Security Center, les informations sur les appareils installés sur les appareils clients ou connectés à ceux-ci peuvent être transférées au Serveur d'administration. Le transfert d'informations 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).

- Configurer le calendrier d'accès pour les appareils (uniquement pour les disques durs, les lecteurs amovibles, les disquettes et les lecteurs de CD/DVD).

  > Si le blocage de l'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.

> 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.

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** → **Contrôle de sécurité** → **Contrôle des applications**).

Paramètres du module Contrôle des appareils

Paramètre	Description
Contrôle des périphériques activé / désactivé	Ce bouton bascule active ou désactive le Contrôle des périphériques. Le bouton bascule est activé par défaut.
Configurer les périphériques de confiance	Cliquez sur ce lien pour ouvrir la fenêtre **Appareils de confiance**. Cette fenêtre permet d'ajouter des périphériques à une liste de périphériques de confiance par identifiant ou via une sélection dans une liste de périphériques découverts sur les périphériques clients.
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 sélectionné et génère un événement relatif à la détection d'une tentative d'accès à l'appareil. • **Bloquer** (valeur par défaut). Lorsque cette option est sélectionnée, Kaspersky Endpoint Security applique le mode d'accès spécifié pour l'appareil ou le bus.
Configurer les paramètres d'accès pour les types d'appareils	Cliquez sur ce lien pour ouvrir la fenêtre **Types de périphériques**. Dans cette fenêtre, vous pouvez configurer les paramètres d'accès des appareils en fonction de leur type.
Configurer les paramètres d'accès pour les bus de connexion	Cliquez sur ce lien pour ouvrir la fenêtre **Bus de connexion**. Cette fenêtre permet de configurer les paramètres d'accès pour les bus de connexion.

Fenêtre Périphériques de confiance

Le tableau contient la liste des périphériques de confiance. Par défaut, le tableau est vide.

Paramètres du périphérique de confiance.

Paramètre	Description
ID du périphérique	ID d'un périphérique de confiance.
Nom de l'appareil	Nom d'un appareil de confiance.
Type de périphérique	Type d'un périphérique de confiance (par exemple, Disque dur ou Lecteur de carte intelligente).
Nom du périphérique client	Nom du périphérique client auquel se connecte un périphérique de confiance.
Commentaire	Commentaire lié à un périphérique de confiance.

Cette fenêtre permet d'ajouter des périphériques à une liste de périphériques de confiance par ID ou en sélectionnant le périphérique requis dans une liste de périphériques existants sur l'ordinateur.

Vous pouvez modifier et supprimer des périphériques de confiance dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Vous pouvez également importer une liste d'appareils à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste d'appareils ajoutés vers un fichier à l'aide du bouton **Exporter**. Lors de l'importation, vous serez invité à remplacer la liste des appareils de confiance ou à ajouter des appareils à une liste existante.

Fenêtre Périphérique de confiance (ID du périphérique)

Cette fenêtre permet d'ajouter un périphérique à la liste des périphériques de confiance sur la base de son ID.

Ajout d'un périphérique par ID

Paramètre	Description
ID du périphérique	Champ de saisie de l'ID ou d'un masque d'ID du périphérique. Vous pouvez saisir manuellement l'ID ou copier l'ID du périphérique requis à partir de la liste **Périphériques détectés sur les périphériques clients**. 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.
Commentaire	Champ de saisie pour un commentaire (facultatif). Le champ est disponible une fois que vous avez saisi l'ID du périphérique et cliqué sur le bouton **Suivant**.

Fenêtre Périphérique de confiance (Liste des périphériques détectés)

Dans cette fenêtre, vous pouvez ajouter un périphérique à une liste de périphériques de confiance en sélectionnant dans une liste de périphériques découverts sur les périphériques clients administrés.

Les informations sur les appareils existants sont disponibles uniquement 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 les propriétés de la stratégie de l'Agent d'administration, 15 minutes par défaut). Si vous créez une stratégie et qu'aucune autre n'est active, la liste sera vide.

Ajout d'un périphérique à partir de la liste

Paramètre	Description
Type de périphérique	Cette liste déroulante permet de sélectionner le type de périphériques à afficher dans le tableau **Périphériques détectés sur les périphériques clients**.
Masque d'ID du périphérique	Champ de saisie d'un masque d'ID du périphérique.
Commentaire	Champ de saisie pour un commentaire (facultatif). Ce champ est disponible une fois que vous avez sélectionné un ou plusieurs périphériques et cliqué sur le bouton **Suivant**.

Cliquez sur le bouton **Filtre** pour ouvrir la fenêtre dans laquelle vous pouvez configurer le filtrage des informations relatives aux périphériques.

Fenêtre Types du périphérique

Cette fenêtre permet de configurer des règles d'accès pour différents types de périphérique.

Règles d'accès pour les types de périphérique

Paramètre	Description

Paramètres d'accès aux appareils de stockage	Ce tableau contient les colonnes suivantes :
	• **Type** : types de périphérique (par exemple, Disques durs, Imprimantes).
	• **Mode d'accès** : mode d'accès aux appareils de ce type. Vous avez le choix parmi les modes d'accès suivants :
	  • **Autoriser** pour octroyer un accès aux périphériques de ce type.
	  • **Bloquer** pour interdire l'accès aux périphériques de ce type.
	  • **Dépend du bus** (valeur par défaut) pour autoriser ou bloquer l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion utilisé pour connecter un appareil.
	  • **En fonction des règles** autorise ou bloque l'accès aux périphériques, selon une règle d'accès et sa planification. Vous pouvez configurer la règle d'accès et sa planification en cliquant sur le type de périphérique requis.

Paramètres d'accès aux autres appareils	Ce tableau contient les colonnes suivantes :
	• **Type** : type d'appareil (par exemple, Appareils de saisie, Cartes audio).
	• **Mode d'accès** : mode d'accès aux appareils de ce type. Vous avez le choix parmi les modes d'accès suivants :
	  • **Autoriser** pour octroyer un accès aux périphériques de ce type.
	  • **Bloquer** pour interdire l'accès aux périphériques de ce type. Veuillez noter que pour les adaptateurs réseau, le mode d'accès **Bloquer** ne peut pas être sélectionnée.
	  • **Dépend du bus** (valeur par défaut) pour autoriser ou bloquer l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion utilisé pour connecter un appareil.

Fenêtre Paramètres d'accès aux appareils

Dans cette fenêtre, vous pouvez configurer le mode d'accès et les règles d'accès pour le type d'appareils sélectionné.

Paramètres d'accès aux appareils

Paramètre	Description
Mode d'accès	Mode d'accès aux appareils de type sélectionné : • **Autoriser** pour octroyer l'accès aux périphériques du type sélectionné.

aux appareils	• **Bloquer** pour interdire l'accès aux périphériques du type sélectionné. • **Dépend du bus** (valeur par défaut) pour autoriser ou bloquer l'accès aux périphériques en fonction d'une règle d'accès pour un bus de connexion utilisé pour connecter un périphérique. • **En fonction des règles** autorise ou bloque l'accès aux périphériques, selon une règle d'accès et sa planification.

Règles d'accès aux appareils	Le tableau contient une liste de règles d'accès et se compose des colonnes suivantes :
	• **Planification d'accès** : noms des planifications d'accès en vigueur.
	• **Utilisateurs et/ou groupes d'utilisateurs** : noms d'utilisateurs ou noms de groupes d'utilisateurs auxquels la règle d'accès s'appliquera.
	• **Accès** : mode d'accès à l'horaire :
	  • **Autoriser** (octroyer l'accès aux appareils du type sélectionné).
	  • **Bloquer** (interdire l'accès aux appareils du type sélectionné).
	• **Statut** : statut de fonctionnement de la règle d'accès :
	  • **Activé** : la règle est activée, le Contrôle des appareils applique cette règle pendant son fonctionnement.
	  • **Désactivé** : la règle est désactivée et n'est pas utilisée lors du fonctionnement du Contrôle des appareils.
	Le tableau contient par défaut une planification d'accès intitulée **Planification par défaut**. Celle-ci garantit l'accès intégral aux périphériques pour tous les utilisateurs (sélection de l'option **\Tous** dans la liste des utilisateurs et des groupes) à tout moment, même si l'accès via le bus de connexion est autorisé pour ce type de périphérique.
	Vous pouvez ajouter, modifier ou supprimer des règles d'accès.
	Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.
	Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre Règle d'accès aux périphériques

Cette fenêtre permet de configurer la règle d'accès au périphérique.

Règle d'accès au périphérique

Paramètre	Description
Configuration de la règle d'accès aux périphériques	Mode d'accès aux appareils de type sélectionné : • **Autoriser** (valeur par défaut) pour octroyer un accès aux périphériques du type sélectionné. • **Bloquer** pour interdire l'accès aux périphériques du type sélectionné.

Utilisateurs et/ou groupes d'utilisateurs	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle d'accès s'applique. La valeur par défaut est **\Tous** (tous les utilisateurs). Vous pouvez ajouter, modifier et supprimer des utilisateurs ou des groupes d'utilisateurs. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.
État	Statut de fonctionnement de la règle d'accès : • **Activé** : la règle est activée, le Contrôle des appareils applique cette règle pendant son fonctionnement. • **Désactivé** : la règle est désactivée et n'est pas utilisée lors du fonctionnement du Contrôle des appareils.
Planifier l'accès aux périphériques	Planification de l'accès des utilisateurs spécifiés aux périphériques. La valeur par défaut est **Planification par défaut**. Vous pouvez spécifier une planification différente.

Fenêtre Sélectionner l'utilisateur ou le groupe

Cette fenêtre permet d'indiquer l'utilisateur local ou de domaine ou le groupe d'utilisateurs pour lequel vous souhaitez configurer la règle d'accès.

Configuration d'une règle d'accès

Paramètre	Description
Manuel	Si cette option est sélectionnée, dans le champ ci-dessous, vous devez saisir le nom de l'utilisateur local ou de domaine ou le nom du groupe d'utilisateurs qui sera soumis à la règle d'accès au périphérique.
Liste des groupes ou des utilisateurs	Si cette option est sélectionnée, dans la zone de recherche, vous pouvez saisir des critères de recherche pour le nom d'utilisateur ou le nom du groupe d'utilisateurs auquel la règle d'accès au périphérique s'appliquera, ou sélectionner le nom du groupe d'utilisateurs dans la liste ci-dessous.

Fenêtre Planifications

Cette fenêtre permet d'indiquer la planification de la règle d'accès au périphérique sélectionnée.

Vous pouvez ajouter, modifier et supprimer des planifications d'accès.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Vous ne pouvez pas supprimer la **Planification par défaut**.

Fenêtre Planification d'accès

Cette fenêtre permet de configurer les planifications d'accès aux périphériques. Vous pouvez configurer des planifications uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs CD/DVD.

Si la case **Bloquer l'accès aux fichiers pendant l'analyse** est décochée dans la section **Paramètres généraux** -> **Paramètres de l'application**, il n'est pas possible de bloquer l'accès à l'aide de la planification d'accès aux appareils.

Planifier l'accès aux périphériques

Paramètre	Description
Nom	Champ de saisie du nom de la planification d'accès. Le nom de l'horaire doit être unique.
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	Le commutateur détermine le mode d'accès aux appareils qui utilisent ce bus pour la connexion : • **Autoriser** (valeur par défaut) permet d'accéder aux appareils connectés à l'aide de ce bus de connexion. • **Bloquer** : interdire l'accès aux appareils connectés via ce bus de connexion.

Configuration du contrôle des appareils dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres du contrôle des appareils dans les paramètres de la stratégie (**Contrôle de sécurité** → **Contrôle des appareils**).

Paramètres du module Contrôle des appareils

Paramètre	Description
Activer le contrôle des périphériques	Cette case active ou désactive le composant Contrôle des périphériques. Cette case est cochée par défaut.
Périphériques de confiance	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Périphériques de confiance**. Cette fenêtre permet d'ajouter un périphérique à une liste de périphériques de confiance par identifiant ou via une sélection dans une liste de périphériques découverts sur les périphériques clients.
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 sélectionné et génère un événement relatif à la détection d'une tentative d'accès à l'appareil. • **Bloquer** (valeur par défaut). Lorsque cette option est sélectionnée, Kaspersky Endpoint Security applique le mode d'accès spécifié pour l'appareil ou le bus.
Paramètres du Contrôle des périphériques	Le bloc 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.

Fenêtre Périphériques de confiance

Le tableau contient la liste des périphériques de confiance. Par défaut, le tableau est vide.

Paramètres du périphérique de confiance.

Paramètre	Description
ID du périphérique	ID d'un périphérique de confiance.
Nom du périphérique	Nom d'un périphérique de confiance.
Type de périphérique	Type d'un périphérique de confiance (par exemple, Disque dur ou Lecteur de carte intelligente).
Nom du périphérique client	Nom du périphérique client auquel se connecte un périphérique de confiance.
Commentaire	Commentaire lié à un périphérique de confiance.

Vous pouvez ajouter un appareil à une liste des appareils de confiance par l'identifiant ou le masque ou en sélectionnant l'appareil requis dans une liste des appareils détectés sur l'appareil de l'utilisateur.

Vous pouvez modifier et supprimer des périphériques de confiance dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

Vous pouvez également importer une liste d'appareils à partir d'un fichier à l'aide du bouton **Additionnel** -> **Importer** et exporter une liste d'appareils ajoutés vers un fichier à l'aide du bouton **Additionnel** -> **Exporter les éléments sélectionnés** ou **Additionnel** -> **Tout exporter**. Lors de l'importation, vous serez invité à remplacer la liste des appareils de confiance ou à ajouter des appareils à une liste existante.

Fenêtre Périphérique de confiance

Cette fenêtre permet d'ajouter un périphérique à la liste des périphériques de confiance sur la base de son ID.

Ajout d'un périphérique par ID

Paramètre	Description
ID du périphérique	Champ de saisie d'ID ou de masque d'ID du périphérique que vous souhaitez ajouter à la liste des périphériques 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 périphériques	Un clic sur le bouton affiche les périphériques trouvés par l'identifiant ou le masque spécifié sur les appareils clients connectés. Le bouton est disponible quand le champ **ID du périphérique** contient une valeur.
Périphériques 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 du périphérique que vous souhaitez ajouter à la liste des périphériques de confiance (facultatif).

Fenêtre Périphériques sur les périphériques clients

Dans cette fenêtre, vous pouvez ajouter un périphérique à une liste de périphériques en sélectionnant dans une liste de périphériques clients.

Les informations sur les périphériques existants sont disponibles uniquement 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). Si vous créez une stratégie et qu'aucune autre n'est active, la liste sera vide.

Ajout d'un périphérique à partir de la liste

Paramètre	Description
Nom du périphérique client	Champ de saisie du nom ou du masque du nom du périphérique administré pour lequel vous souhaitez trouver les périphériques connectés. Le masque par défaut est *, qui représente tous les périphériques administrés.
Type de périphérique	Cette liste déroulante permet de définir le type de périphérique connecté à rechercher (par exemple, Disques durs ou Lecteurs de carte intelligente). L'option sélectionnée par défaut est **Tous les périphériques**.
ID du périphérique	Champ de saisie de l'ID ou du masque d'ID du périphérique que vous souhaitez trouver. Le masque par défaut est *, qui représente tous les périphériques.
Recherche sur les périphériques	Cliquez sur ce bouton pour que l'application lance une recherche de périphériques selon les paramètres indiqués. Les résultats de la recherche sont repris dans le tableau inférieur.

Fenêtre Type de périphérique

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 de périphérique	Types de périphérique (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'un des éléments suivants : • **Autoriser** pour octroyer l'accès aux périphériques du type sélectionné. • **Bloquer** pour interdire l'accès aux périphériques du type sélectionné. • **Dépend du bus** (valeur par défaut) pour autoriser ou bloquer l'accès aux appareils en fonction d'un mode d'accès pour un bus de connexion. • **En fonction des règles** : autoriser ou bloquer l'accès aux appareils, selon une règle d'accès et sa planification.

Vous pouvez configurer les règles et les horaires d'accès dans la fenêtre **Configuration des règles 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 périphériques

Cette fenêtre permet configurer les règles d'accès et la planification pour les types de périphérique sélectionnés.

Pour ouvrir cette fenêtre, double-cliquez sur le nom du type de périphérique dans la fenêtre **Type de périphérique**.

Règles et planifications d'accès aux périphériques

Paramètre	Description
Utilisateurs	Liste des utilisateurs et des groupes pour lesquels vous pouvez configurer des

et/ou groupes d'utilisateurs	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 du groupe d'utilisateurs sélectionné par planifications d'accès	Le tableau contient les planifications d'accès pour les utilisateurs et les groupes. Il contient 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 composant. • **Accès** : type d'accès pour la planification : **Autoriser** (octroyer l'accès aux périphériques du type sélectionné) ou **Bloquer** (interdire l'accès aux périphériques 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 périphériques 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 de périphérique. 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**. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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 périphériques

Paramètre	Description
Type	**Utilisateur** ou **Groupe** auquel la règle s'applique.
Nom d'utilisateur ou de groupe	Nom d'utilisateur ou nom du groupe d'utilisateurs auxquels la règle s'applique.

Fenêtre Planification d'accès

Cette fenêtre permet de configurer les planifications d'accès aux périphériques.

Planifier l'accès aux périphériques

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'un des éléments suivants : • **Autoriser** (valeur par défaut) permet d'accéder aux appareils connectés à l'aide de ce bus de connexion. • **Bloquer** : interdire l'accès aux appareils connectés via ce bus de connexion.

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 est exécutée 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.

Vous pouvez également afficher la liste des appareils connectés à l'aide des commandes de gestion du Contrôle des appareils.

Paramètres du Contrôle des périphériques

Le tableau décrit toutes les valeurs disponibles et les valeurs par défaut pour tous les paramètres que vous pouvez définir pour la tâche Contrôle des périphériques.

Paramètres du Contrôle des périphériques

Paramètre	Description	Valeurs
OperationMode	Mode de fonctionnement de	`Block` (valeur par défaut) : l'a le mode d'accès spécifié pour

	l'application lors de la tentative d'accès à un appareil dont l'accès est interdit conformément aux paramètres du Contrôle des appareils.	`Notify` : l'application teste le sélectionné et génère un évér détection d'une tentative d'ac
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 disc autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé disque dur dépend du mode c connexion sur lequel le disque `Block` : l'accès à tous les disc l'exclusion des disques durs sy jamais bloqués par le Contrôle est bloqué pour les utilisateur `ByRule` : l'accès aux disques règles d'accès.
RemovableDrive	Spécifie le mode d'accès aux disques amovibles connectés à l'appareil client.	`Allow` : l'accès à tous les disc autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé disque amovible dépend du m de connexion sur lequel le disc `Block` : l'accès à tous les disc bloqué pour les utilisateurs. `ByRule` : l'accès aux disques a des règles d'accès.
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 périphérique client via le bus ISA.	`Allow` : l'accès à tous les lect est autorisé pour les utilisateu `DependsOnBus` (valeur par dé disquette dépend du mode d' connexion sur lequel la disque `Block` : l'accès à tous les lect est bloqué pour les utilisateur `ByRule` : l'accès aux lecteurs dépend des règles d'accès.
OpticalDrive	Spécifie le mode d'accès pour les lecteurs CD/DVD connectés à l'appareil client.	`Allow` : l'accès à tous les lect autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé lecteur de CD/DVD dépend d bus de connexion via lequel le est connecté. `Block` : l'accès à tous les lect est bloqué pour les utilisateur `ByRule` : l'accès aux lecteurs des règles d'accès.

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 au périphérique client via un port série via le bus ISA.	`Allow` : l'accès aux périphéric un port série est autorisé pou `DependsOnBus` (valeur par dé l'appareil connecté via un port mode d'accès pour le bus de `Block` : l'accès aux périphéric un port série est bloqué pour
ParallelPortDevice	Spécifie le mode d'accès aux appareils connectés à l'appareil client via un port parallèle.	`Allow` : l'accès aux périphéric un port parallèle est autorisé `DependsOnBus` (valeur par dé l'appareil connecté via un port du mode d'accès pour le bus `Block` : l'accès aux périphéric un port parallèle est bloqué p
Printer	Spécifie le mode d'accès aux imprimantes connectées à l'appareil client.	`Allow` : l'accès à toutes les im autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé l'imprimante dépend du mode connexion via lequel l'imprima `Block` : l'accès à toutes les im bloqué pour les utilisateurs.
Modem	Spécifie le mode d'accès aux modems connectés à l'appareil client.	`Allow` : l'accès à tous les mod pour les utilisateurs. `DependsOnBus` (valeur par dé modem dépend du mode d'ac connexion via lequel le moden `Block` : l'accès à tous les mod pour les utilisateurs.
TapeDrive	Spécifie le mode d'accès aux lecteurs de bande connectés à l'appareil client.	`Allow` : l'accès à tous les lect autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé streamer dépend du mode d'a connexion via lequel le stream `Block` : l'accès à tous les lect bloqué pour les utilisateurs.
MultifuncDevice	Spécifie le mode d'accès aux dispositifs multifonctions connectés à l'appareil client.	`Allow` : l'accès à tous les péri multifonctions est autorisé po `DependsOnBus` (valeur par dé l'appareil multifonction dépen du bus de connexion sur leque connecté. `Block` : l'accès à tous les péri multifonctions est bloqué pou
SmartCardReader	Spécifie le mode d'accès aux lecteurs de cartes à	`Allow` : l'accès à tous les lect puce est autorisé pour les util

	puce connectés à l'appareil client.	`DependsOnBus` (valeur par dé lecteur de carte à puce dépen au bus de connexion sur leque connecté. `Block` : l'accès à tous les lect puce est bloqué pour les utilis
WiFiAdapter	Spécifie le mode d'accès aux adaptateurs Wi-Fi connectés à l'appareil client.	`Allow` : l'accès à tous les ada autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé l'adaptateur Wi-Fi dépend du le bus de connexion. `Block` : l'accès à tous les ada bloqué pour les utilisateurs.
NetworkAdapter	Spécifie le mode d'accès aux adaptateurs réseau connectés à l'appareil client.	`Allow` : l'accès à toutes les ca autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé l'adaptateur réseau externe d d'accès au bus de connexion s l'adaptateur est connecté. Le Contrôle des périphériqu permet pas de refuser l'acc adaptateurs réseau externe déconnecter votre périphé réseau.
PortableDevice	Spécifie le mode d'accès aux appareils mobiles connectés à l'appareil client.	`Allow` : l'accès à tous les péri est autorisé pour les utilisateu `DependsOnBus` (valeur par dé l'appareil portable dépend du bus de connexion sur lequel l'a connecté. `Block` : l'accès à tous les péri est bloqué pour les utilisateur
BluetoothDevice	Spécifie le mode d'accès aux dispositifs Bluetooth connectés à l'appareil client.	`Allow` : l'accès à tous les péri Bluetooth est autorisé pour le `DependsOnBus` (valeur par dé l'appareil Bluetooth dépend d bus de connexion sur lequel l'a connecté. `Block` : l'accès à tous les péri Bluetooth est bloqué pour les
ImagingDevice	Spécifie le mode d'accès aux appareils d'imagerie connectés à l'appareil client.	`Allow` : l'accès à tous les péri traitement d'images est autor utilisateurs. `DependsOnBus` (valeur par dé l'appareil d'imagerie dépend d bus de connexion sur lequel l'a connecté.

		`Block` : l'accès à tous les péri traitement d'images est bloqu utilisateurs.
SoundAdapter	Spécifie le mode d'accès aux cartes sons connectées à l'appareil client.	`Allow` : l'accès à toutes les ca autorisé pour les utilisateurs. `DependsOnBus` (valeur par dé l'adaptateur audio dépend du bus de connexion sur lequel l'a connecté. `Block` : l'accès à toutes les ca 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 péri est autorisé pour les utilisateu `DependsOnBus` (valeur par dé l'appareil de saisie dépend du bus de connexion sur lequel l'a connecté. `Block` : l'accès à tous les péri est bloqué pour les utilisateur
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'a périphériques USB est autoris utilisateurs. `Block` : l'accès à tous les péri bloqué pour les utilisateurs.
FireWire	Mode d'accès pour les appareils connectés à l'appareil client via l'interface FireWire.	`Allow` (valeur par défaut) : l'a périphériques connectés via l' est autorisé pour les utilisateu `Block` : l'accès aux périphéric l'interface FireWire est bloqué utilisateurs.
La section **[TrustedDevices.item_#]** contient les appareils de confiance.		
DeviceId	Spécifie l'ID ou le masque d'ID d'un périphérique de confiance.	Vous pouvez utiliser le caract (n'importe quelle séquence de (n'importe quel caractère) pou périphérique. Exemples : *Pour refuser l'accès à tous USB à l'exception de celui q définissez, indiquez les para* Dans la section `[DeviceBu USB=Block` Dans la section `[TrustedDevices.item_ DeviceId=<identifiant périphérique>`

		Pour refuser l'accès à tous USB, mais autoriser l'accès USB, indiquez les paramètr Dans la section `[DeviceBu` `USB=Block` Dans la section `[TrustedDevices.item_` `DeviceId=USBSTOR*`
Comment	Commentaire sur le périphérique de confiance spécifié.	—
La section **[Schedules.item_#]** contient les planifications d'accès pour les périphériques. Vous pouvez configure programmation uniquement pour les disques durs, les disques amovibles, les lecteurs de disquette et les lecteurs		
ScheduleName	Spécifie un nom de planification. Le nom de l'horaire doit être unique.	Valeur par défaut : `Default`. La planification `Par défaut` complet aux périphériques à t tout moment si l'accès par le l est autorisé pour le type de p question. Vous ne pouvez pas supprime `Par défaut`.

DaysHours	Spécifie des intervalles de temps pour une planification.	`All` (valeur par défaut) : la pla 24/7 (aucune limite de temps)
		
		`< jour de la semaine >` : jo Vous pouvez utiliser les noms ou les abréviations des jours d exemple, pour lundi, vous pouv `Lun` ou `lundi`). Pour les jours pouvez spécifier des intervalle spécifiques. La semaine comr
		
		`< heure >` : heures [0:24]. Pou ne pouvez spécifier que des ir
		
		Exemples :
		Spécifiez la planification Sc couvre les jours du dimanch à 11, de 12 à 15 et de 16 à 24 :
		`[Schedules.item_0001]` `ScheduleName=schedule` `DaysHours=Su-Sa:0..11`
		Spécifiez la planification sc couvre les intervalles suivar 12 à 14 et les vendredis de 2
		`[Schedules.item_0002]` `ScheduleName=schedule` `DaysHours=Th:12..14;F`
		Spécifiez la planification sc couvre 24 heures/24 et 7 jo
		`[Schedules.item_0003]` `ScheduleName=schedule` `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 disque dur. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisateurs. 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 défau s'applique à tous les utilisateu `<nom d'utilisateur>` : no auquel la règle d'accès est ap `@<nom de groupe>` : nom d d'utilisateurs auquel la règle d' appliquée.
[HardDrivePrincipals.item_#.AccessRules.item_#]	Paramètres des règles d'accès.	—
UseRule	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'ac `No` : la règle d'accès est désac
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'a durs est autorisé. `Block` : l'accès aux disques d
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 disque amovible. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisa 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 défau s'applique à tous les utilisateu `<nom d'utilisateur>` : no auquel la règle d'accès est ap `@<nom de groupe>` : nom d d'utilisateurs auquel la règle d' appliquée.
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	Paramètres des règles d'accès.	—
UseRule	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'ac `No` : la règle d'accès est désac
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'a amovibles est autorisé. `Block` : l'accès aux disques a

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 plusieu un lecteur de disquette. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe 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 défau s'applique à tous les utilisateu `< nom d'utilisateur >` : no auquel la règle d'accès est ap `@< nom de groupe >` : nom d d'utilisateurs auquel la règle d' appliquée.
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	Paramètres des règles d'accès.	—
UseRule	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'ac `No` : la règle d'accès est désac
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 a disquette est autorisé. `Block` : l'accès aux lecteurs d 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 r lecteur CD/DVD. De plus, plusieurs planifications peuvent être spécifiées pour un utilisateur ou un groupe d'utilisa 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 défau s'applique à tous les utilisateu `< nom d'utilisateur >` : no auquel la règle d'accès est ap `@< nom de groupe >` : nom d d'utilisateurs auquel la règle d' appliquée.
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	Paramètres des règles d'accès.	—
UseRule	Spécifie si la règle est activée ou désactivée.	`Yes` (par défaut) : la règle d'ac `No` : la règle d'accès est désac
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'a CD/DVD est autorisé. `Block` : l'accès à tous les lect bloqué.

Afficher une liste des appareils connectés dans la ligne de commande

Seuls les utilisateurs ayant des rôles d'admin et d'audit sont autorisés à afficher la liste des périphériques connectés.

Pour consulter la liste des périphériques connectés, exécutez la commande suivante :

```
kesl-control [-D] --get-device-list
```

Kaspersky Endpoint Security affiche les informations suivantes sur les périphériques connectés :

- **Type de périphérique**. Type d'un appareil connecté. Par exemple, `OpticalDrive` ou `HardDrive`.
- **ID**. ID du périphérique connecté.
- **Nom**. Nom du périphérique connecté.
- **Chemin**. Chemin d'accès au périphérique dans le système d'exploitation virtuel sysfs.
- **Disque système**. Paramètre qui indique si le périphérique 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.

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, l'application Kaspersky Endpoint Security bloque l'accès ou affiche un avertissement.

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 catégorie du 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 des 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.

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 restreindre l'accès à Internet via un navigateur à tous les utilisateurs de l'organisation, à l'exception du service informatique.

- **Horaire des règles**. 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 votre navigateur uniquement pendant les heures de bureau.

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.

- *Informer.* Le Contrôle Internet affiche un avertissement indiquant que la visite de la ressource Web n'est pas recommandée. À l'aide des liens contenus dans le message d'avertissement, l'utilisateur peut accéder à la ressource Web demandée.

Chaque règle est prioritaire. 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** → **Contrôle de sécurité** → **Contrôle Internet**).

Paramètres du module Contrôle Internet

Paramètre	Description

Contrôle Internet activé/désactivé	Le commutateur active ou désactive le module Contrôle Internet. Le bouton bascule est désactivé par défaut.

Liste des règles	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 :
	• **Nom de la règle**. Le nom de la règle d'accès aux ressources Web.
	• **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 activer ou désactiver un commutateur dans le tableau, ou 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.
	Vous pouvez ajouter, modifier, supprimer, déplacer vers le haut ou déplacer vers le bas les éléments 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.
	Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.
	Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.
	Vous pouvez également importer une liste de règles à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste de règles ajoutées à un fichier à l'aide du bouton **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	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 tout ce qui n'est pas spécifié dans la liste des règles** (valeur par défaut) : autoriser l'accès aux ressources Web.

	• **Bloquer tout ce qui n'est pas précisé dans la liste des règles** : bloquer l'accès aux ressources Web.
Modèles	**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 apparaît lorsqu'une règle est déclenchée et bloque l'accès à une ressource Web. **Message à 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.

Fenêtre Règle du Contrôle Internet

Dans cette fenêtre, vous pouvez configurer les paramètres de la règle d'accès aux ressources Web.

Ajout d'une 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.
État	Vous pouvez sélectionner l'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.
Action	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.
Filtrer par catégories de contenu	La case active ou désactive l'utilisation d'un filtre par catégorie de contenu. Si la case est cochée, le lien **Catégories de contenu** est disponible. Ce lien ouvre une fenêtre dans laquelle vous pouvez sélectionner les catégories de contenu souhaitées. La case est décochée par défaut.

Filtrer par catégories de types de données	La case active ou désactive l'utilisation d'un filtre par catégorie de contenu. Si la case est cochée, le lien **Catégories de type de données** est disponible. Ce lien ouvre une fenêtre dans laquelle vous pouvez sélectionner les catégories de types de données souhaitées. La case est décochée par défaut.
Adresses	Vous pouvez choisir d'utiliser un filtre d'adresse de ressource Web : • **Appliquer à toutes les adresses** (valeur par défaut). Lorsque cette option est sélectionnée, 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. • **Appliquer aux adresses et/ou groupes spécifiés**. Lorsque vous sélectionnez cette option, un tableau des adresses des ressources Web soumises à la règle devient disponible, ainsi que le bouton **Ajouter une adresse**, qui ouvre une fenêtre dans laquelle vous pouvez ajouter l'adresse souhaitée d'une ressource Web et le bouton **Ajouter un groupe**, qui ouvre une fenêtre Groupes d'adresses dans laquelle vous pouvez ajouter des groupes d'adresses des ressources Web.
Utilisateurs	Vous pouvez choisir d'utiliser un filtre pour les utilisateurs soumis à la règle d'accès aux ressources Web : • **Appliquer à tous les utilisateurs** (valeur par défaut). Lorsque cette option est sélectionnée, le filtre des utilisateurs n'est pas utilisé et la règle Contrôle Internet est appliquée à tous les utilisateurs. • **Appliquer aux utilisateurs et/ou groupes spécifiés**. Lorsque vous sélectionnez cette option, un tableau des utilisateurs et des groupes d'utilisateurs concernés par la règle et le bouton **Ajouter** deviennent disponibles. Ce bouton ouvre la fenêtre **Sélectionner un utilisateur ou un groupe** dans laquelle vous pouvez ajouter les utilisateurs et/ou groupes d'utilisateurs souhaités.
Horaire des règles	Calendrier de fonctionnement des règles du Contrôle Internet. La planification par défaut est **Toujours**. Le lien **Toujours** ouvre la fenêtre **Planifications**, dans laquelle vous pouvez configurer un autre calendrier pour la règle.

Fenêtre Groupes d'adresses

Le tableau contient des groupes d'adresses de ressources Web auxquelles l'accès des utilisateurs est contrôlé par le module Contrôle Internet. Par défaut, le tableau est vide.

Configuration des règles d'accès aux ressources Web

Paramètre	Description
Nom du groupe	Nom du groupe d'adresses des ressources Web auquel la règle s'applique.
Nombre d'adresses dans un groupe	Nombre d'adresses dans le groupe d'adresses.

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 Groupe en cliquant sur le bouton **Ajouter** situé au-dessus du tableau.

Si vous souhaitez ajouter un groupe d'adresses à la liste des groupes dans la fenêtre **Règle du Contrôle Internet**, cochez la case en regard du nom du groupe dans le tableau et cliquez sur le bouton **Ajouter des groupes à une règle** situé sous le tableau.

Groupe Fenêtre

Dans cette fenêtre, vous pouvez ajouter un groupe d'adresses des ressources Web.

Configuration des règles d'accès aux ressources Web

Paramètre	Description
Nom du groupe	Le nom du nouveau groupe d'adresses des ressources Web.
Adresses	Tableau des adresses incluses dans le groupe d'adresses des ressources Web.

Vous pouvez ajouter, modifier et supprimer des éléments 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.

Sélectionner un utilisateur ou un groupe

Cette fenêtre permet d'indiquer l'utilisateur local ou de domaine ou le groupe d'utilisateurs pour lequel vous souhaitez configurer la règle d'accès aux ressources Web.

Configuration des règles d'accès aux ressources Web

Paramètre	Description
Manuel	Si cette option est sélectionnée, dans le champ ci-dessous, vous devez saisir le nom de l'utilisateur local ou de domaine ou le nom du groupe d'utilisateurs qui sera soumis à la règle d'accès aux ressources Web.
Liste des groupes ou des utilisateurs	Si cette option est sélectionnée, dans la zone de recherche, vous pouvez saisir des critères de recherche pour le nom d'utilisateur ou le nom du groupe d'utilisateurs auquel la règle d'accès aux ressources Web s'appliquera, ou sélectionner le nom du groupe d'utilisateurs dans la liste ci-dessous.

Fenêtre Planifications

Cette fenêtre permet d'indiquer la planification de la règle d'accès au périphérique sélectionnée.

Vous pouvez ajouter, modifier et supprimer des planifications d'accès.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Le calendrier par défaut **Toujours** ne peut pas être supprimé ou modifié.

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. Le nom de l'horaire doit être unique.
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 du Contrôle Internet dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres du Contrôle Internet dans les propriétés de la stratégie (**Contrôle 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 ou déplacer vers le bas les éléments 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 des messages	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre Modèles des messages.

Fenêtre Règle du Contrôle Internet

Dans cette fenêtre, vous pouvez configurer les paramètres de la règle d'accès aux ressources Web.

Ajout d'une règle du Contrôle Internet

Paramètre	Description
Nom de la règle	Champ de saisie du nom de la règle d'accès aux ressources Web.
Utiliser la 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.

	Cette 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 catégorie du contenu**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton ouvre la fenêtre **Sélectionner les catégories de contenu**. • **Par catégories des types de données**. Lorsque vous sélectionnez cet élément de liste, le bouton **Sélectionner** devient disponible. Ce bouton ouvre la fenêtre **Sélectionner une catégorie de type de données**. • **Par catégorie du contenu et types de données**. Lorsque vous sélectionnez cet élément de liste, les boutons **Sélectionner** deviennent disponibles. Ces boutons ouvrent les fenêtres dans lesquelles vous pouvez sélectionner les catégories souhaitées.
Filtrer une adresse	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 les adresses** devient disponible, en cliquant sur ce qui ouvre la fenêtre **Sélectionner les adresses** dans laquelle vous pouvez sélectionner les adresses souhaitées des ressources Web.
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, en cliquant sur ce qui ouvre la fenêtre **Sélection des 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 nouvel horaire**. 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.

Sélectionner une catégorie de contenu

Dans cette fenêtre, vous pouvez sélectionner les catégories de contenu dont vous souhaitez contrôler l'accès.

Pour cela, 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.

Sélectionner une catégorie de type de données

Cette fenêtre vous permet de sélectionner les catégories de types dont vous souhaitez contrôler l'accès.

Pour cela, cochez les cases à côté des catégories souhaitées.

Toutes les cases sont décochées par défaut.

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'adresse**.

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 **Sélection d'adresse**, 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Si vous souhaitez ajouter un nouveau groupe d'adresses à la liste des groupes de cette fenêtre, ouvrez la fenêtre **Ajouter un groupe d'adresses** en cliquant sur le bouton **Ajouter** situé au-dessus du tableau.

Par défaut, le tableau est vide.

Ajouter 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.

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 et supprimer des éléments dans le tableau

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.
Nom d'utilisateur ou de 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 les utilisateurs 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 concernant le blocage d'une ressource Web. L'application affiche un message de blocage d'une ressource Web (voir figure ci-dessous) 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** → **Contrôle de sécurité** → **Contrôle Internet**.

5. Dans le groupe **Modèles**, 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 apparaît lorsqu'une règle est déclenchée et bloque l'accès à une ressource Web.

   - **Message à 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.

6. Cliquez sur **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 l'espace de travail, sélectionnez 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 bloc 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 apparaît lorsqu'une règle est déclenchée et bloque l'accès à une ressource Web.

   - **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 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.

7. Cliquez sur **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 préinstallée 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 préinstallée 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) : auto l'accès aux ressources Web. `Block` : interdire 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.	

`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) : auto l'accès à la ressource Web. `Block` : interdire l'accès à une ressource Web. `Notify` : afficher un avertissem indiquant que la ressource Web pas recommandée à la visite. À des liens contenus dans le mess d'avertissement, l'utilisateur peu accéder à la ressource Web demandée.
`Enabled`	État de fonctionnement de la règle d'accès aux ressources Web.	`Yes` : la règle est activée, le Cor Internet applique cette règle pendant son fonctionnement. `No` (valeur par défaut) : la règle désactivée et n'est pas prise en compte lors du fonctionnement Contrôle Internet.
`ScheduleId`	Identifiant de planification, 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 une règle. `No` (valeur par défaut) : ne pas u le filtre pour les adresses des ressource Web, appliquer la règ toutes les adresses des ressour Web.
`Urls.item_#`	L'adresse de la ressource Web, dont l'accès est réglementé par la règle.	Vous pouvez utiliser des masqu pour spécifier l'adresse d'une ressource Web.
`UseCategories`	Utilisation de filtres dans une règle par catégories de contenu et par catégories de types de données.	`None` (valeur par défaut) : ne pa utiliser le filtre de contenu des ressources Web. `ContentOnly` : utiliser un filtre catégories de contenu dans la r `FormatOnly` : utiliser un filtre p les catégories de types de donr dans la règle. `ContentAndFormat` : utiliser ur dans la règle par catégories de contenu et catégories de types données.
`[Rules.item_#.ContentCategories.item_#]`	Section pour indiquer la catégorie de contenu.	–
`ContentCategory`	Catégorie de contenu.	`AdultContent, AlcoholTobaccoNarcotics,` `Violence, Profanity, Weap`

		ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepsta InternetCommunicationMedi CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileShari AudioAndVideo, BankSites, Blogs, DatingSites, LegislationR LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITo
[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 exécutab 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 la règle. No (valeur par défaut) : ne pas u le filtre utilisateur, appliquer la rè tous les utilisateurs.
[Rules.item_#.Principals.item_#]	Section permettant de spécifier les utilisateurs soumis à la règle d'accès aux ressources Web.	
isGroup	Le paramètre spécifie si le nom spécifié dans le champ Name est un nom d'utilisateur ou un	Yes : le nom spécifié est un nom groupe. No : le nom spécifié est le nom d'utilisateur.

	nom de groupe d'utilisateurs.	
`Name`	Utilisateur ou groupe d'utilisateurs soumis à une règle d'accès aux ressources Web.	`< nom d'utilisateur >` : nom utilisateur auquel la règle est appliquée. `@< nom de groupe >` : nom d'u groupe d'utilisateurs auquel la r est appliquée.
`Sid`	Identifiant de l'utilisateur ou du groupe d'utilisateurs.	
La section **[UrlCategories.item_#]** contient les paramètres suivants :		
`Name`	Nom du groupe d'adresses des ressources Web auquel la règle régule l'accès.	
`Urls.item_#`	L'adresse d'une ressource Web incluse dans le groupe.	Vous pouvez utiliser des masqu 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 garan que la règle s'exécute sans restr 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 >` : jou la semaine. Vous pouvez utiliser noms complets des jours ou les abréviations des jours de la sem (par exemple, pour lundi, vous p spécifier `Lu`, `Lun` ou `lundi`). P les jours de la semaine, vous pou spécifier des intervalles ou des spécifiques. La semaine comme le dimanche. `< heure >` : heures [0:24]. Pour l heures, vous ne pouvez spécifie 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>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres seront affichés.

`--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>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être 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.exemple.fr/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 `*.exemple.fr` :

   - `http://pictures.exemple.fr` : masque de domaine `*.` appliqué pour `pictures.`.
   - `http://user.pictures.exemple.fr` : masque de domaine `*.` appliqué pour `pictures.` et `user.`.
   - `http://exemple.fr` : 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.exemple.fr` est interprété comme `*.exemple.fr`. Le masque couvre les adresses `www2.exemple.fr` et `www.pictures.exemple.fr`.

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.exemple.fr` comprend des adresses de la forme `http://www.exemple.fr/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 de caractères `/*` à la fin du masque d'adresse est traitée comme `/*` ou une chaîne 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 `exemple.fr` comprend les adresses `http://exemple.fr` et `https://exemple.fr`.

   - 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://*.exemple.fr` est soumis à l'adresse `http://www.exemple.fr`, mais pas à l'adresse `https://www.exemple.fr`.

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

№	Masque d'adresse	Adresse vérifiée de la ressource Web	L'adresse vérifiée satisfait-elle au masque d'adresse ?	Commentaire
1	*.exemple.fr	http://www.123exemple.fr	Non	Voir règle 1.
2	*.exemple.fr	http://www.123.exemple.fr	Oui	Voir règle 2.
3	*exemple.fr	http://www.123exemple.fr	Oui	Voir règle 1.
4	*exemple.fr	http://www.123.exemple.fr	Oui	Voir règle 1.
5	http://www.*.exemple.fr	http://www.123exemple.fr	Non	Voir règle 1.
6	www.exemple.fr	http://www.exemple.fr	Oui	Voir règles 3, 2, 1.

7	www.exemple.fr	https://www.exemple.fr	Oui	Voir règles 3, 2, 1.
8	http://www.*.exemple.fr	http://123.exemple.fr	Oui	Voir règles 3, 4, 1.
9	www.exemple.fr	http://www.exemple.fr/abc	Oui	Voir règles 3, 5, 1.
10	exemple.fr	http://www.exemple.fr	Oui	Voir règles 3, 1.
11	http://exemple.fr/	http://exemple.fr/abc	Oui	Voir règles 6.
12	http://exemple.fr/*	http://exemple.fr	Oui	Voir règle 7.
13	http://exemple.fr	https://exemple.fr	Non	Voir règle 8.
14	"exemple.fr"	http://www.exemple.fr	Non	Voir règle 9.
15	"http://www.exemple.fr"	http://www.exemple.fr/abc	Non	Voir règle 9.
16	"*.exemple.fr"	http://www.exemple.fr	Oui	Voir règles 1, 9.
17	"http://www.exemple.fr/*"	http://www.exemple.fr/abc	Oui	Voir règles 1, 9.
18	"www.exemple.fr"	http://www.exemple.fr; https://www.exemple.fr	Oui	Voir règles 9, 8.
19	www.exemple.fr/abc/123	http://www.exemple.fr/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.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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 :

- Configurez les zones de surveillance pour surveiller 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** → **Contrôle de sécurité** → **Contrôle des applications**).

Paramètres du module Contrôle de l'intégrité du système

Paramètre	Description
Contrôle de l'intégrité du système activé / désactivé	Le commutateur active ou désactive le module Contrôle de l'intégrité du système. Le bouton bascule est désactivé par défaut.
Zones de contrôle	Cliquez sur le lien **Configurer les zones de surveillance** pour ouvrir la fenêtre **Zones de contrôle**.
Zones d'exclusion	Cliquez sur le lien **Configurer les zones d'exclusion de surveillance** pour ouvrir la fenêtre **Zones d'exclusion**.
Exclusions d'après le masque	Cliquez sur le lien **Configurer les exclusions par masque** pour ouvrir la fenêtre **Exclusions d'après le masque**.

Fenêtre Zones de contrôle

Le tableau contient les zones de contrôle pour le composant 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** (/opt/kaspersky/kesl/).

Paramètres de la zone de contrôle pour le Contrôle de l'intégrité du système

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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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 d'ajout d'une zone de surveillance

Cette fenêtre permet d'ajouter ou de modifier une zone de contrôle pour le composant du Contrôle 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 fenêtre **Zones de contrôle**. 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 son fonctionnement.

	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. Cette 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. 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.
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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Zones d'exclusion

Le tableau 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. 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 le module fonctionne.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre d'ajout d'une 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 composant. Si cette case est décochée, l'application ne contrôle pas cette zone pendant le fonctionnement du composant. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. Cette 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. 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 **/** est renseigné 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 **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

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 **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

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).

Configuration du contrôle de l'intégrité du système dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de contrôle de l'intégrité du système dans les propriétés de la stratégie (**Contrôle de sécurité** → **Contrôle de l'intégrité du système**).

Paramètres du module 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	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour ouvrir la fenêtre **Zone d'analyse**.
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour 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 composant 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

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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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 composant 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. Cette 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

Fenêtre Zones d'exclusion

Le tableau 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. 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 le module fonctionne.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

Fenêtre <Nom de la 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 composant. Si cette case est décochée, l'application ne contrôle pas cette zone pendant le fonctionnement du composant. Par la suite, vous pouvez exclure cette zone de contrôle après avoir coché la case. Cette 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 **/** est renseigné 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 **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre. 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 **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

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).

Configuration du contrôle de l'intégrité du système dans la 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.

Paramètres de la tâche de contrôle de l'intégrité du système à l'accès

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 la valeur de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez définir 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/*/fichier ou /dir/*/*/fichier. 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/**/fichier*/ ou /dir/fichier**/. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/fichier 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 que vous souhaitez exclure de toutes les sections [ScanScope.item_#]. Vous pouvez spécifier 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.
`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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 :

- hachage de 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 du système est mis à jour lorsque les paramètres de la tâche changent, par exemple, lorsqu'une nouvelle zone de surveillance est ajoutée.

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.

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.
Vérifier les répertoires dans les zones de surveillance	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.
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, configurer, supprimer, déplacer vers le haut ou déplacer vers le bas les zones de contrôle dans le tableau. Cliquez sur le bouton **Descendre** pour déplacer l'élément sélectionné vers le bas du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone dans le tableau. Cliquez sur le bouton **Monter** pour déplacer l'élément sélectionné vers le haut du tableau. Kaspersky Endpoint Security analyse les objets dans les zones indiquées dans l'ordre où elles apparaissent dans le tableau des zones d'analyse. Si vous voulez spécifier des paramètres de sécurité pour le répertoire enfant différents des paramètres de sécurité du répertoire parent, vous devez placer le répertoire enfant plus haut que le répertoire parent dans le tableau. Le bouton est accessible dès que vous sélectionnez une zone 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.

Cliquez sur le nom de la zone d'analyse pour ouvrir la fenêtre **<Nom de la zone d'analyse>**. Dans cette fenêtre, vous pouvez modifier les paramètres de la zone d'analyse choisie.

Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **<Nouvelle zone d'analyse>**. Cette fenêtre permet d'indiquer une nouvelle zone d'analyse.

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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 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 **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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.

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 **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

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).

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.
Vérifier les répertoires dans les zones de surveillance	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.
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	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-

	ci pour ouvrir la fenêtre **Zone 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.

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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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 la tâche Vérification de l'intégrité du système.

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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau. Le bouton est disponible si au moins un élément dans le tableau a été sélectionné. 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 Zones d'exclusion

Paramètres des exclusions de l'analyse

Groupe de paramètres	Description
Exclusions du contrôle	Ce groupe de paramètres contient le bouton **Configurer**. Cliquez sur celui-ci pour 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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.

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. Cette 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 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 **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

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 **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

La modification des paramètres de l'élément sélectionné s'effectue dans une nouvelle fenêtre.

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).

Contrôle de l'intégrité du système dans la ligne de commande

À partir de la ligne de commande, vous pouvez effectuer des vérifications de l'intégrité du système sur l'appareil à l'aide des tâches personnalisées de la *Vérification de l'intégrité du système* (tâches de type *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 (SHAé56) 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. `Non` (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	La valeur par défaut n'est pas définie.

	plusieurs fichiers à l'aide de masques au format shell. Avant d'indiquer la valeur de ce paramètre, assurez-vous que le paramètre `UseExcludeMasks` est activé. Vous pouvez définir plusieurs masques, chaque masque doit figurer sur sa propre ligne et il faut définir un nouvel index.	
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.
`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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.
`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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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, Kaspersky Endpoint Security peut arrêter le processus de l'application qui exécute l'activité malveillante.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

Le module Détection comportementale est activé automatiquement avec les paramètres par défaut lorsque vous lancez l'application Kaspersky Endpoint Security.

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.
- Excluez l'activité du processus de l'analyse.

Si l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée, les exclusions de processus ne sont pas appliquées lors de l'analyse du comportement des applications dans le système d'exploitation.

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.

Configuration de la détection comportementale dans Web Console

Dans Web Console, vous pouvez configurer les paramètres d'analyse du comportement des applications dans les propriétés de la stratégie (**Paramètres de l'application** → **Protection avancée** → **Détection comportementale**).

Paramètre du module Détection comportementale

Paramètre	Description
Détection comportementale activée / désactivée	Le bouton bascule active ou désactive le module Détection comportementale. Le bouton bascule est activé 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 : • **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. • **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.
Exclusions par processus	Cliquez sur le lien **Configurer les exclusions par processus** 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

Le tableau 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 et des fichiers modifiés par le processus spécifié. Par défaut, le tableau est vide.

Si l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée, les exceptions de processus ne sont pas appliquées.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
Exclure/Ne pas exclure les processus de confiance des analyses	Le commutateur active ou désactive l'utilisation des exclusions configurées en fonction des processus dans le fonctionnement du composant Détection comportementale. Le bouton bascule est désactivé 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.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Vous pouvez également importer une liste d'exceptions à partir d'un fichier à l'aide du bouton **Importer** et exporter la liste des exceptions ajoutées vers un fichier 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 de zone d'exclusion en fonction des processus

Cette fenêtre permet d'ajouter ou de configurer une zone d'exclusion en fonction des processus.

Paramètres de zone d'exclusion

Paramètre	Description
Nom de la zone d'exclusion	Champ de saisie du nom de la zone d'exclusion basée sur le processus. Ce nom sera affiché dans le tableau de la fenêtre Exclusions par processus. Le champ de saisie ne peut être vide.

basée sur le processus	
Utiliser cette exclusion	Ce commutateur active ou désactive l'exclusion de cette zone pendant le fonctionnement de l'application. Cette case est cochée par défaut.
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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.

Configuration de la détection comportementale dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres d'analyse du comportement des applications dans les propriétés de la stratégie (**Protection avancée** → **Détection comportementale**).

Paramètre du module Détection comportementale

Paramètre	Description
Activer la Détection comportementale	La case active ou désactive le module Détection comportementale. Cette 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 composant 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

Le tableau 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. Par défaut, le tableau est vide.

Si l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée, les exceptions de processus ne sont pas appliquées.

Paramètres de la zone d'exclusion en fonction des processus

Paramètre	Description
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.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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**. Lors de l'importation, vous serez invité à remplacer la liste d'exclusions ou à ajouter des exclusions à une liste existante.

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	Champ de saisie du nom de la zone d'exclusion. Ce nom sera affiché dans le tableau de la fenêtre **Exclusions par processus**.

d'exclusion	
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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. Cette case est cochée par défaut.

Configuration de la détection comportementale dans 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 Détection comportementale

Paramètre	Description	Valeurs
`TaskMode`	Action exécutée par l'application suite à la détection d'une	`Block` (valeur par défaut) : termine le processus de l'application qui exécute une activité malveillante.

	activité malveillante dans le système d'exploitation.	`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.
`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.
La section **[TrustedPrograms.item_#]** contient les processus exclus de la vérification. 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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`	Activer l'exclusion du processus spécifié de l'analyse.	`Yes` (valeur par défaut) : activer l'exclusion de l'activité du processus spécifié de l'analyse. `No` : ne pas activer l'exclusion de l'activité du processus spécifié de l'analyse.

Utilisation de Kaspersky Security Network

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 composants de protection et une réduction des risques de faux positifs.

L'utilisation de Kaspersky Security Network est volontaire. Vous pouvez activer ou désactiver l'utilisation de KSN à tout moment.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

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 périphériques 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 de périphériques 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 périphériques. 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 au périphérique et aux données.
- **Mode standard KSN** : 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 à tout moment choisir une autre option pour utiliser Kaspersky Security Network.

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 Internet 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 vous permet de réduire la charge sur la mémoire vive de l'appareil.

L'application fonctionne avec des bases de données de logiciels malveillants légers via Kaspersky Security Network.

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.

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. L'interaction 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 :

- Le périphérique 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.

Configuration de l'utilisation de Kaspersky Security Network dans Web Console

Dans Web Console, vous pouvez configurer l'utilisation de Kaspersky Security Network dans le fonctionnement de l'application Kaspersky Endpoint Security dans les propriétés de la stratégie (**Paramètres de l'application** → **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 **Actifs (Appareils)**.

Paramètres d'utilisation de Kaspersky Security Network

Paramètre	Description
Ne pas utiliser KSN	En sélectionnant cette option, vous refusez d'utiliser Kaspersky Security Network.
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.
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.
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 les serveurs KSN si le proxy KSN	La case active ou désactive la possibilité de communiquer directement avec les serveurs KSN lorsque le service proxy KSN n'est pas disponible. Cette case est cochée par défaut.

n'est pas disponible	Le paramètre s'applique uniquement si l'application est utilisée en mode standard.
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 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.
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

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.

Paramètres 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 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 dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer l'utilisation de Kaspersky Security Network dans le fonctionnement de l'application Kaspersky Endpoint Security dans les propriétés de la stratégie (**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 d'utilisation 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 les serveurs KSN si le proxy KSN n'est pas disponible	La case active ou désactive la possibilité de communiquer directement avec les serveurs KSN lorsque le service proxy KSN n'est pas disponible. Cette case est cochée par défaut. Le paramètre s'applique uniquement si l'application est utilisée en mode standard.

Paramètres Kaspersky Security Network

Cette fenêtre permet de configurer les paramètres d'utilisation de Kaspersky Security Network.

Paramètres Kaspersky Security Network

Paramètre	Description
En savoir plus...	Cliquez sur ce lien pour accéder au site Internet de Kaspersky.
Ne pas	En sélectionnant cette option, vous refusez d'utiliser Kaspersky Security Network.

utiliser Kaspersky Security Network	
Mode standard 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.
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 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 standard KSN** ou **Mode avancé 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.

Paramètres Kaspersky Security Network

Paramètre	Description
Je confirme avoir entièrement lu,	En sélectionnant cette option, vous confirmez que vous souhaitez

compris et accepté les conditions générales de la Déclaration de Kaspersky Security Network	utiliser 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 dans 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 d'utilisation de Kaspersky Security Network.
- `--accept-ksn` : une clé signifiant que vous acceptez les conditions énoncées dans 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 <nom du fichier de configuration> [--json] [--accept-ksn]
```

où :

- `--file <chemin d'accès au fichier de configuration>` : chemin complet vers le fichier de configuration avec les paramètres généraux de l'application, dans lequel la valeur souhaitée du paramètre `UseKSN` est configurée.
- `--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` : une clé signifiant que vous acceptez les conditions énoncées dans 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 périphérique client, fonctionne sous une stratégie définie dans 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 périphérique 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 standard KSN` 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 :

- Le périphérique 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 d'un fichier de configuration contenant tous les paramètres généraux de l'application ou à l'aide de 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 :

- Utilisation d'un serveur proxy dans l'application.
- Exclusions globales : exclusion des points de montage de l'interception des opérations sur les fichiers pour les modules Protection contre les menaces sur les fichiers, Protection contre le chiffrement, Surveillance du conteneur et des tâches Analyse des logiciels malveillants, Analyse des zones critiques, Analyse des conteneurs et Analyse des disques amovibles.
- Exclure la mémoire de processus des analyses.
- 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.

Configuration du serveur proxy

Vous pouvez configurer les paramètres du serveur proxy si les utilisateurs des périphériques clients accèdent à Internet via un serveur proxy. L'application Kaspersky Endpoint Security peut utiliser un serveur proxy pour se connecter aux serveurs de Kaspersky, par exemple, lors de la mise à jour des bases de données et des modules de l'application ou lors de l'interaction avec Kaspersky Security Network et Kaspersky Endpoint Detection and Response (KATA).

Par défaut, l'utilisation d'un serveur proxy est désactivée.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation d'un serveur proxy pour se connecter à Kaspersky Security Network, SVM et Serveur d'intégration n'est pas prise en charge.

Configuration des paramètres du serveur proxy dans Web Console

Dans Web Console, vous pouvez configurer l'utilisation d'un serveur proxy dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Paramètres du serveur proxy**).

Configuration 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 du serveur proxy spécifiés, par exemple pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
Adresse	Champ de saisie de l'adresse IP ou du nom de domaine du serveur proxy. Ces champs sont accessibles si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée.
Port	Champ de saisie du port du serveur proxy. Valeur par défaut : 3128. Ces champs sont accessibles si l'option **Utiliser les paramètres indiqués du serveur proxy** a été sélectionnée.
Utiliser l'authentification sur le serveur proxy	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 sécurisée 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 du serveur proxy** est cochée.
Modifier	Permet d'indiquer le mot de passe de l'utilisateur pour l'authentification sur le serveur proxy. Le contenu du champ **Mot de passe** n'est pas modifiable. Par défaut, le mot de passe est vide. Pour indiquer un mot de passe, cliquez sur le bouton **Modifier**, saisissez le mot de passe dans la fenêtre qui s'ouvre, puis 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. Quand vous cliquez sur le bouton **Afficher** dans la fenêtre de saisie du mot de passe, celui-ci s'affiche en clair. Le bouton est disponible si la case **Utiliser l'authentification du serveur proxy** est cochée.
Utiliser Kaspersky	Cette case active ou désactive l'utilisation de Kaspersky Security Center comme

Security Center en guise de serveur proxy pour l'activation	serveur proxy pour l'activation de l'application. Si cette case est cochée, Kaspersky Endpoint Security utilise Kaspersky Security Center comme serveur proxy pour l'activation de l'application. 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.

Configuration des paramètres du serveur proxy dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer l'utilisation d'un serveur proxy dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres du serveur proxy**).

Configuration 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 du serveur proxy spécifiés, par exemple pour l'intégration avec Kaspersky Endpoint Detection and Response (KATA).
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.
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 sécurisée 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 du 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 du serveur proxy** est cochée.
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation	Cette case active ou désactive l'utilisation de Kaspersky Security Center comme serveur proxy pour l'activation de l'application. Si cette case est cochée, Kaspersky Endpoint Security utilise Kaspersky Security Center comme serveur proxy pour l'activation de l'application. 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.

Configuration des paramètres de proxy dans la ligne de commande

À partir de la ligne de commande, vous pouvez activer ou désactiver l'utilisation d'un serveur proxy par les modules de l'application à l'aide des paramètres `UseProxy` et `ProxyServer` 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 `UseProxy` peut prendre les valeurs suivantes :

- `Yes` : active l'utilisation d'un serveur proxy.
- `No` : désactiver l'utilisation d'un serveur proxy.

Le paramètre `ProxyServer` vous permet de spécifier les paramètres du serveur proxy au format `[<utilisateur>[:<mot de passe>]@]<adresse du serveur proxy a>[:<port>]`, où :

- `<utilisateur>` : nom d'utilisateur pour l'authentification sur le serveur proxy.
- `<пароль>` : le mot de passe utilisateur pour l'autorisation sur le serveur proxy.
- `<adresse du serveur proxy a>` : adresse IP ou nom de domaine du serveur proxy.
- `<port>` : port du serveur proxy.

Si l'authentification n'est pas requise pour se connecter à un serveur proxy, vous n'avez pas besoin de spécifier le paramètre `ProxyServer`.

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 sécurisée et le compte utilisateur peut être compromis.

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 menaces sur les fichiers 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 des conteneurs. 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 exceptions globales affectent le fonctionnement du module Surveillance du conteneur 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** → **Paramètres généraux** → **Exclusions globales**).

Le tableau de la section **Exclusions globales** contient les points de montage qui seront exclus des opérations d'interception des fichiers.

Dans la colonne **Chemin**, les chemins vers les points de montage exclus apparaissent. Par défaut, le tableau est vide.

Vous pouvez ajouter, modifier et supprimer des éléments dans le tableau.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

Fenêtre d'ajout d'exclusion d'un point de montage

Paramètres de point de montage

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** : points de montage locaux. • **Monté** : répertoires distants montés sur le périphérique via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique via les protocoles Samba et NFS.
Protocole	Cette liste déroulante permet sélectionner le protocole d'accès à distance :

d'accès	• **NFS** : répertoires distants montés sur le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : les ressources de système de fichiers du périphérique 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.
Chemin	Champ de saisie du chemin d'accès au point de montage à 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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. 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 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 **Protocole d'accès**.

Configuration des exclusions globales dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer des exclusions globales dans les propriétés de la stratégie (**Paramètres généraux** → **Exclusions globales**).

Le groupe de paramètres **Points de montage exclus** contient le bouton **Configurer**. Cliquez sur celui-ci pour 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.

Cliquez sur le bouton **Supprimer** pour supprimer l'élément sélectionné du tableau.

Le bouton est disponible si au moins un élément dans le tableau a été sélectionné.

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 le périphérique via le protocole Samba ou NFS. • **Tous les systèmes montés distants** : tous les répertoires distants montés sur le périphérique 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 le périphérique via le protocole NFS. • **Samba** : répertoires distants montés sur le périphérique via le protocole Samba. • **Personnalisé** : tous les ressources de système de fichiers du périphérique 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/*/fichier` ou `/dir/*/*/fichier`. 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/**/fichier*/` ou `/dir/fichier**/`. Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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.
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 dans 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 le périphérique via les protocoles SMB et NFS.
- `Mounted:NFS` : exclut de l'interception des opérations de fichiers tous les répertoires distants montés sur le périphérique 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 de fichiers tous les répertoires montés avec le type de système de fichiers indiqué.

- `/Mnt` : exclut de l'interception les objets dans le point de montage /mnt (y compris les sous-répertoires) 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 les objets qui se trouvent dans les 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/*/fichier` ou `/dir/*/*/fichier`.

  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/**/fichier*/` ou `/dir/fichier**/`.

  Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 spécifier plusieurs points de montage que vous souhaitez exclure de l'analyse.

Les points doivent être spécifiés de la même manière qu'ils sont affichés dans la sortie de commande `mount`.

Exclure la mémoire de processus des analyses

Vous pouvez configurer des exclusions à partir de l'analyse de la mémoire de processus. L'application n'analysera pas la mémoire des processus spécifiés.

Configuration des exclusions dans Web Console

Dans Web Console, vous pouvez configurer les exclusions de mémoire de processus de l'analyse dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**).

Le lien **Configurer l'exclusion de l'analyse de la mémoire du processus** dans le groupe **Exclure la mémoire de processus des analyses** ouvre la fenêtre **Exclure la mémoire de processus des analyses**, 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/*/fichier` ou `/dir/*/*/fichier`.

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/**/fichier*/` ou `/dir/fichier**/`.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 ajouter, modifier et supprimer des éléments dans la liste.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime de la liste le chemin sélectionné d'accès au processus.

Le bouton est disponible si au moins un chemin d'accès au processus est sélectionné dans la liste.

Le bouton **Modifier** ouvre une fenêtre dans laquelle vous pouvez modifier le chemin d'accès au processus. Kaspersky Endpoint Security exclut de l'analyse la mémoire du processus spécifié.

Le bouton **Ajouter** ouvre une fenêtre dans laquelle vous pouvez saisir le chemin d'accès complet au processus. Kaspersky Endpoint Security exclut de l'analyse la mémoire du processus spécifié.

Configuration des exclusions dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les exclusions de la mémoire de processus de l'analyse dans les propriétés de la stratégie (**Paramètres généraux** → **Exclure la mémoire des processus**).

Cliquer sur le bouton **Configurer** dans le groupe **Exclure la mémoire de processus des analyses** 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/*/fichier` ou `/dir/*/*/fichier`.

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/**/fichier*/` ou `/dir/fichier**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 ajouter, modifier et supprimer des éléments dans la liste.

Si vous cliquez sur le bouton **Supprimer**, Kaspersky Endpoint Security supprime de la liste le chemin sélectionné d'accès au processus.

Le bouton est disponible si au moins un chemin d'accès au processus est sélectionné dans la liste.

Le bouton **Modifier** ouvre une fenêtre dans laquelle vous pouvez modifier le chemin d'accès au processus. Kaspersky Endpoint Security exclut de l'analyse la mémoire du processus spécifié.

Le bouton **Ajouter** ouvre une fenêtre dans laquelle vous pouvez saisir le chemin d'accès complet au processus. Kaspersky Endpoint Security exclut de l'analyse la mémoire du processus spécifié.

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/*/fichier` ou `/dir/*/*/fichier`.

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/**/fichier*/` ou `/dir/fichier**/`.

Le masque `**` ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, `/dir/**/**/fichier` 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 menaces sur les fichiers et Contrôle des appareils.

- Une application peut bloquer l'accès aux fichiers analysés par le module Protection contre les menaces sur les fichiers 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 les paramètres **Première action** (`FirstAction`) et **Deuxième action** (`SecondAction`) du module Protection contre les menaces sur les fichiers.

  Vous pouvez désactiver le blocage de l'accès aux fichiers analysés par le module Protection contre les menaces sur les fichiers. 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.

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 l'application**, groupe **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 menaces sur les fichiers et Contrôle des appareils.

Cette case est cochée par défaut.

Si la case est décochée, l'accès à n'importe quel fichier est autorisé pendant l'analyse et l'analyse est effectuée en mode asynchrone.

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer le mode d'interception de fichiers dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, groupe **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 menaces sur les fichiers et Contrôle des appareils.

Cette case est cochée par défaut.

Si la case est décochée, l'accès à n'importe quel fichier est autorisé pendant l'analyse et l'analyse est effectuée 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 menaces sur les fichiers 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.

Configuration dans Web Console

Dans Web Console, 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 (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, groupe **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 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 (**Paramètres généraux** → **Paramètres de l'application**, groupe **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

À partir de la ligne de commande, vous pouvez activer ou désactiver la détection des applications légitimes que les intrus pourraient utiliser pour endommager des appareils ou des 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.

Configuration dans Web Console

Dans Web Console, vous pouvez activer ou désactiver la surveillance de la stabilité des applications dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, groupe **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 le paramètre, vous devez redémarrer l'application.

Si l'application est instable, le message suivant s'affiche dans les propriétés de l'appareil sur lequel l'application est installée : *<Nombre> d'arrêts anormaux de l'application depuis <date et heure>*.

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver la surveillance de la stabilité des applications dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, groupe **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 le paramètre, vous devez redémarrer l'application.

Si l'application est instable, le message suivant s'affiche dans les propriétés de l'appareil sur lequel l'application est installée : *<Nombre> d'arrêts anormaux de l'application depuis <date et heure>*.

Configuration sur la ligne de commande

Dans la ligne de commande, vous pouvez configurer la surveillance de la stabilité des applications 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 ou de désactiver la surveillance de la stabilité des applications. Le paramètre peut prendre les valeurs suivantes :

- `Yes/true` : activer la surveillance de la stabilité de l'application.
- `No/false` : ne pas activer la surveillance de la stabilité des applications.

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 requis pour afficher une notification concernant le fonctionnement instable de l'application. 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 Web Console, vous pouvez configurer les paramètres de lancement de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, groupe **Paramètres de démarrage de l'application**).

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 Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de lancement de l'application dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, groupe **Paramètres de démarrage 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 et du processeur

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. Vous pouvez également configurer des limites d'utilisation de la mémoire pour les tâches d'analyse. La limite par défaut est de 8 192 mégaoctets.

Configuration d'une limite dans Web Console

Dans Web Console, vous pouvez activer ou désactiver la limite d'utilisation du processeur et configurer la limite d'utilisation de la mémoire pour les tâches d'analyse dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, groupe **Performances**).

Paramètres

Paramètre	Description
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.
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, Analyse de l'inventaire et Analyse du conteneur. Si la case est cochée, la charge maximale sur tous les noyaux du processeur lors de l'exécution de ces tâches ne dépasse pas la valeur spécifiée dans le champ **Valeur maximale (%)**. La case est décochée par défaut.

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 la limite d'utilisation de la mémoire pour les tâches d'analyse dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**, groupe **Performances**).

Dans le groupe **Performances**, cliquez sur le bouton **Configurer** pour ouvrir la fenêtre **Consommation du processeur et de la mémoire**, dans laquelle vous pouvez configurer des restrictions (cf. le tableau ci-dessous).

Paramètres

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, Analyse de l'inventaire et Analyse du conteneur.

	Si la case est cochée, la charge maximale sur tous les noyaux du processeur lors de l'exécution de ces tâches ne dépasse pas la valeur spécifiée dans le champ de droite (en pourcentage). 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

À partir de la ligne de commande, vous pouvez configurer la limite de ressources CPU pour les tâches de type *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` active 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*. Le paramètre peut prendre des valeurs de 10 à 100. Valeur par défaut : 100.

Dans la ligne de commande, vous pouvez configurer la limite d'utilisation de la mémoire pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan* à l'aide du paramètre `ScanMemoryLimit` dans le fichier de configuration kesl.ini. Valeur par défaut : 8192.

Limite d'utilisation de la mémoire résidente par une application

Vous pouvez configurer une limite sur l'utilisation de la mémoire résidente par l'application. Le réglage par défaut est automatique.

Configuration d'une limite dans Web Console

Dans Web Console, vous pouvez configurer la limite d'utilisation de la mémoire résidente par une application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, groupe **Paramètres avancés de l'application**).

Dans le groupe **Paramètres avancés de l'application**, cliquez sur le lien **Configurer l'utilisation de la mémoire** pour ouvrir une fenêtre dans laquelle vous pouvez configurer la limite d'utilisation de la mémoire résidente (cf. le tableau ci-dessous).

Paramètres

Paramètre	Description
Utilisation de	Dans la liste déroulante, vous pouvez sélectionner comment limiter l'utilisation de la

la mémoire résidente de l'application	mémoire résidente : • **Pas limitée**. Lorsque vous sélectionnez cet élément de la liste, l'utilisation de la mémoire résidente n'est pas limitée. • **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. • **Limitée automatiquement (recommandé)**. Lorsque vous sélectionnez cet élément de la liste, l'utilisation de la mémoire résidente est automatiquement limitée (par défaut).
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 Console d'administration

Dans la Console d'administration, vous pouvez configurer la limite d'utilisation de la mémoire résidente par une application dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**).

Dans le groupe **Paramètres avancés de l'application**, 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).

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**. Lorsque vous sélectionnez cet élément de la liste, 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

Dans la ligne de commande, vous pouvez configurer la limite d'utilisation de la mémoire résidente de l'application 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 de 1 à 100 en pourcentage de la taille de la mémoire.
- < `valeur` >`MB` : valeur en mégaoctets.
- `lowest/`< `valeur` >%/< `valeur` >`Mo` : valeur la plus basse entre la valeur en pourcentage et la valeur en mégaoctets.
- `highest/`< `valeur` >%/< `valeur` >`Mo` : valeur la plus élevée entre la valeur en pourcentage et la valeur 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 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.

Vous pouvez activer ou désactiver la limite du nombre de tâches d'analyse personnalisées exécutées simultanément sur la ligne de commande à l'aide du paramètre `LimitNumberOfScanFileTasks` 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 `LimitNumberOfScanFileTasks` peut prendre des valeurs comprises entre 0 et 4294967295. Valeur par défaut : 0.

Si la valeur 0 est attribuée, l'utilisateur non privilégié ne peut pas exécuter de tâches d'analyse personnalisée.

Si vous avez installé le paquet d'interface utilisateur graphique lors de l'installation de l'application, le paramètre `LimitNumberOfScanFileTasks` prend par défaut la valeur `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 non traités et les appareils connectés vers le stockage de Kaspersky Security Center.

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 (**Avancé → 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 (**Avancé → Stockages → Équipement**). Les informations sont transmises si le Contrôle des appareils est activé.

Activation ou désactivation de l'envoi d'informations à Web Console

Dans Web Console, vous pouvez activer ou désactiver l'envoi des informations dans les propriétés de la stratégie (**Paramètres de l'application → Paramètres généraux → Paramètres de stockage**).

Paramètres d'envoi d'informations vers le stockage de Kaspersky Security Center

Paramètre	Description
Information sur les fichiers non traités activée / désactivée	Ce bouton bascule active ou désactive l'envoi de notifications sur les fichiers non traités pendant l'analyse au Serveur d'administration. Le bouton bascule est activé par défaut.
Information sur les périphériques installés activée / désactivée	Le commutateur active ou désactive la transmission au Serveur d'administration des informations sur les appareils installés sur l'appareil client ou connectés à celui-ci. Le bouton bascule est activé par défaut.

Activation ou désactivation de l'envoi d'informations dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver l'envoi d'informations dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de stockage**).

Paramètres d'envoi d'informations vers le stockage de Kaspersky Security Center

Paramètre	Description
Informer 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. Cette case est cochée par défaut.
Informer sur les périphériques 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. Cette 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'afficher les tâches créées dans l'application Kaspersky Endpoint Security ;
- autorisation d'afficher les tâches créées dans Kaspersky Security Center sur les appareils clients.

Configuration dans Web Console

Dans Web Console, vous pouvez configurer l'autorisation d'afficher les tâches dans les propriétés de la stratégie (**Paramètres de l'application** → **Tâches locales** → **Gestion des tâches**).

Paramètres Gestion des tâches

Paramètre	Description
Autoriser les utilisateurs à consulter et à administrer les 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 périphériques clients administrés. La case est décochée par défaut.
Autoriser les utilisateurs à consulter et à administrer les tâches créées via KSC	Cette case autorise ou interdit pour les utilisateurs la consultation et l'administration des tâches créées via Kaspersky Security Center Web Console et l'administration de ces tâches sur les appareils administrés. La case est décochée par défaut.

Configuration dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer l'autorisation d'afficher les tâches dans les propriétés de la stratégie (**Tâches locales** → **Gestion des tâches**).

Paramètres Gestion des tâches

Paramètre	Description
Autoriser les utilisateurs à consulter et à administrer les 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 périphériques clients administrés.

	La case est décochée par défaut.
Autoriser les utilisateurs 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 périphériques clients administrés. La case est décochée par défaut.

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*, en 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 conservées dans un format spécial et ne représentent aucun danger.

Si le fichier peut être désinfecté, l'état de la copie de sauvegarde du fichier passe à *Désinfecté*. Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations critiques partiellement ou complètement perdues suite à la désinfection, vous pouvez tenter de restaurer le fichier au départ de sa copie désinfectée dans son répertoire d'origine.

Il est recommandé de restaurer les fichiers à partir des copies de sauvegarde uniquement s'ils ont reçu l'état *Désactivé*. La restauration d'objets infectés peut infecter le périphérique.

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 suivants de la sauvegarde :

- Durée de stockage des objets dans la sauvegarde. Par défaut, les objets sont stockés pendant 90 jours.
- Taille maximale de la sauvegarde. Par défaut, la taille de la sauvegarde est illimitée.
- Chemin d'accès à la sauvegarde. Par défaut, la sauvegarde se trouve dans /var/opt/kaspersky/kesl/common/objects-backup/.

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 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 (**Avancé** → **Stockages** → **Sauvegarde**) et dans Web Console (**Opérations** → **Stockages** → **Sauvegarde**). Vous pouvez afficher les propriétés des fichiers situés dans la sauvegarde sur les appareils protégés, exécuter une analyse des logiciels malveillants dans la sauvegarde 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.

Configuration des paramètres de la sauvegarde dans Web Console

Dans Web Console, vous pouvez configurer les paramètres de la sauvegarde dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres réseau**).

Paramètres de la sauvegarde

Paramètre	Description
Les informations sur les fichiers dans la	Ce bouton bascule active ou désactive l'envoi de notifications

sauvegarde sont activées/désactivées	au Serveur d'administration sur les fichiers dans la sauvegarde. Le bouton bascule est activé par défaut.
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 : 0 à 3653. Valeur par défaut : 90. Si la valeur définie est 0, les objets sont conservés dans la sauvegarde pour une période indéterminée.
Limiter la taille de la sauvegarde à (Mo)	Champ de saisie pour spécifier la taille maximale de la sauvegarde (en mégaoctets). Valeurs admises : 0 à 999999. Valeur par défaut : 0 (La taille de la sauvegarde est illimitée).

Configuration des paramètres de la sauvegarde dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de la sauvegarde dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de stockage**).

Paramètres de la sauvegarde

Paramètre	Description
Informer sur les fichiers dans la sauvegarde	La case active ou désactive l'envoi de notifications au Serveur d'administration sur les fichiers dans la sauvegarde. Cette case est cochée par défaut.
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 3653. Valeur par défaut : 90. Si la valeur définie est 0, les objets sont conservés dans la sauvegarde pour une période indéterminée.
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 : 0 à 999999. Valeur par défaut : 0 (La taille de la sauvegarde est illimitée).

Configuration des paramètres de la sauvegarde dans la ligne de commande

Sur la ligne de commande, vous pouvez configurer les paramètres de la sauvegarde à l'aide de la tâche prédéfinie Gestion de la sauvegarde (*Backup*).

La tâche Gestion de la sauvegarde est exécutée par défaut. Vous ne pouvez pas démarrer et arrêter une tâche manuellement.

Vous pouvez configurer les paramètres de la sauvegarde en modifiant les paramètres de la tâche prédéfinie Gestion de la sauvegarde.

Paramètres de la tâche Gestion de la sauvegarde

Paramètre	Description	Valeur

`DaysToLive`	Durée de conservation des objets dans la sauvegarde (en jours). Pour supprimer la limite de durée de conservation des objets dans la sauvegarde, spécifiez la valeur 0.	0 : la durée de conservation des objets dans la sauvegarde n'est pas limitée. Valeur par défaut : 90.
`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.
`BackupFolder`	Chemin d'accès au répertoire de la copie de sauvegarde. Vous pouvez définir un répertoire de la sauvegarde autre que celui défini par défaut. En guise de répertoire de la sauvegarde, vous pouvez utiliser des répertoires sur n'importe quel appareil. Il est déconseillé de désigner des répertoires qui se trouvent sur des périphériques distants, par exemple des répertoires montés via les protocoles Samba et NFS. Kaspersky Endpoint Security commence à placer les objets dans le répertoire indiqué après la modification des paramètres et le relancement de l'application. 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 de la sauvegarde par défaut requiert les privilèges root.

Utilisation des objets de stockage 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 le périphérique.

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 filtre >"] [-n < nombre >] [--json]
```

où :

- `< conditions du filtre >` : 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.
- `< numéro >` : le nombre d'objets récents du stockage qui doivent être affichés. 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.

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 --restore < identifiant de l'objet >
```

où `< identifiant d'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 --restore < identifiant de l'objet > --file < nom et chemin d'accès au fichier >
```

où `--file < nom et chemin du fichier >` est le nouveau nom de 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.

Suppression des objets de la sauvegarde

Pour supprimer les objets sélectionnés de la sauvegarde, exécutez la commande suivante :

```
kesl-control --mass-remove --query "< conditions du filtre >"
```

où `< conditions du filtre >` : 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.

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 de détection et de réponse de Kaspersky sont des systèmes de sécurité conçus pour détecter les menaces complexes et les signes d'attaques à différents niveaux de l'infrastructure d'une organisation. Les solutions de détection et de réponse 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 Anti Targeted Attack Platform (module Kaspersky Endpoint Detection and Response). L'intégration avec Kaspersky Endpoint Detection and Response (KATA) est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (ci-après également EDR (KATA)).

- 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).

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.

À propos de la réponse aux commandes des solutions Detection and Response

L'application Kaspersky Endpoint Security peut effectuer des actions de réponse visant à fournir des fonctions de sécurité :

- Lors de l'interaction avec le module de la solution Kaspersky Anti Targeted Attack Platform – Kaspersky Endpoint Detection and Response (KATA).

- Lors de l'interaction avec la solution Kaspersky Endpoint Detection and Response Optimum.

Les paramètres d'action de réponse de Kaspersky Anti Targeted Attack Platform et de Kaspersky Endpoint Detection and Response Optimum sont différents.

L'application Kaspersky Endpoint Security peut effectuer les actions de réponse suivantes :

- Recevoir les fichiers depuis des appareils.

  L'action est effectuée à l'aide de la tâche *Obtenir un fichier* (Get file task). Par exemple, vous pouvez configurer pour recevoir un fichier journal des événements généré par un logiciel tiers.

- Supprimer les fichiers des appareils.

  L'action est effectuée à l'aide de la tâche *Supprimer le fichier* (Delete file task).

- Lancer les processus à distance sur les appareils.

  L'action est effectuée à l'aide de la tâche *Exécuter le processus* (Run process).

  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 *Obtenir un fichier*.

- Terminer à distance les processus sur les appareils.

  L'action est effectuée à l'aide de la tâche *Terminer le processus* (Terminate 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.

- Détecter les *indicateurs de compromission* sur les appareils et prendre les mesures pour répondre aux menaces.

  L'action est effectuée à l'aide de la tâche *Analyse IOC* (IOC Scan).

  Lors de l'exécution de la tâche *Analyse IOC*, la vérification 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 pour les fichiers de plus de 200 Mo.

- Activer ou désactiver l'isolation réseau de l'appareil.

  Lorsque Kaspersky Endpoint Security interagit avec Kaspersky Endpoint Detection and Response Optimum, vous pouvez :

  - Activer ou désactiver l'isolation réseau dans Web Console ou Kaspersky Security Center Cloud Console.
  - Désactiver l'isolation réseau dans la ligne de commande.
  - Configurer la désactivation automatique de l'isolation réseau dans Web Console ou Kaspersky Security Center Cloud Console.

  Lorsque Kaspersky Endpoint Security interagit avec Kaspersky Endpoint Detection and Response (KATA), vous pouvez :

  - Désactiver l'isolation réseau dans la ligne de commande.
  - Activer ou désactiver l'isolation réseau du côté de la solution Kaspersky Endpoint Detection and Response (KATA).

    Pour en savoir plus, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

Limites de l'isolation du réseau

Lorsque vous utilisez l'isolation réseau, il est fortement recommandé de vous familiariser avec les limitations décrites ci-dessous.

Pour que l'isolation du 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'isolation réseau est activée par la solution Kaspersky Anti Targeted Attack Platform ou Kaspersky Endpoint Detection and Response Optimum n'est pas garanti.

Le trafic de transit avec l'isolation du réseau activée est pris en charge avec des restrictions et peut être filtré.

DHCP et DNS ne sont pas automatiquement ajoutés aux exceptions d'isolement du réseau. Par conséquent, si l'adresse réseau d'une ressource a été modifiée pendant l'isolement du réseau, 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 exceptions d'isolement du réseau, vous devez donc l'ajouter manuellement aux exceptions afin que l'application Kaspersky Endpoint Security ne perde pas la connexion avec le serveur KATA.

L'ajout d'un processus à l'isolation réseau et l'exclusion d'un processus de l'isolation réseau par son nom ne sont pas pris en charge.

Si Kaspersky Endpoint Security est utilisé en mode standard, lors de l'utilisation de l'isolation 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, configurez les paramètres du serveur proxy requis et ajoutez-le aux exclusions.
- Spécifier Kaspersky Security Center comme source des mises à jour des bases de données.

Ces recommandations ne s'appliquent pas si Kaspersky Endpoint Security est utilisé en mode Light Agent.

Intégration à Kaspersky Endpoint Detection and Response (KATA)

Kaspersky Endpoint Detection and Response (KATA) est un module de la solution Kaspersky Anti Targeted Attack Platform. L'intégration avec le module Kaspersky Endpoint Detection and Response (KATA) est assurée par le module de l'application Kaspersky Endpoint Security – Endpoint Detection and Response (KATA) (ci-après également EDR (KATA)).

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, consultez l'aide de Kaspersky Anti Targeted Attack Platform.

Cette fonctionnalité n'est pas prise en charge dans le conteneur KESL.

En interagissant avec Kaspersky Endpoint Detection and Response (KATA), l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

- Envoyer des données sur les événements survenus sur les appareils (télémétrie) au serveur Kaspersky Anti Targeted Attack Platform avec le composant Central Node (ci-après dénommé serveur KATA). Kaspersky Endpoint Security envoie au serveur KATA 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 :

Pour intégrer Kaspersky Endpoint Detection and Response (KATA), le module Détection comportementale doit être activé.

L'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA) n'est possible que si le module Détection comportementale est activé. Sinon, les données télémétriques nécessaires ne sont pas transmises.

De plus, Kaspersky Endpoint Detection and Response (KATA) peut utiliser les données reçues des modules suivants :

- Protection contre les menaces sur les fichiers.

- Protection contre les menaces réseau.

- Protection contre les menaces Internet.

Lors de l'intégration avec Kaspersky Endpoint Detection and Response (KATA), les appareils dotés de Kaspersky Endpoint Security établissent des connexions sécurisées avec le serveur KATA via HTTPS. Les certificats suivants émis par le serveur KATA sont utilisés pour sécuriser la connexion :

- Certificat du serveur KATA. 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 d'intégration avant d'activer l'intégration avec Kaspersky Endpoint Detection and Response (KATA).

- Certificat client. Ce certificat est utilisé pour sécuriser davantage la connexion avec une authentification bidirectionnelle (analyse des périphériques avec Kaspersky Endpoint Security par le serveur KATA). Le même certificat client peut être utilisé par plusieurs périphériques. Par défaut, le serveur KATA 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 de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) et ajouter un certificat client (cryptoconteneur avec le certificat et la clé privée).

Les certificats destinés à protéger la connexion au serveur KATA sont fournis par l'administrateur de Kaspersky Anti Targeted Attack Platform.

Un serveur proxy est utilisé pour se connecter au serveur KATA 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 Endpoint Detection and Response (KATA) 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 la Web Console et de la Console d'administration :

- Configurer les paramètres généraux de connexion aux serveurs KATA.

- Ajouter et supprimer des certificats de serveur KATA.
- Configurer l'authentification bidirectionnelle lors de la connexion aux serveurs KATA et ajoutez des certificats clients.
- Configurer les paramètres d'envoi des événements.
- Activer ou désactiver l'envoi de la télémétrie.

  Si l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response est activée, les exclusions de processus ne sont pas appliquées lors de l'envoi de télémétrie.

L'administration des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) via Kaspersky Security Center Cloud Console n'est pas prise en charge.

Configuration de l'intégration avec Kaspersky Endpoint Detection and Response (KATA) dans Web Console

Dans Web Console, vous pouvez activer ou désactiver l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA) et configurer les paramètres d'intégration dans les propriétés de la stratégie (**Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response (KATA)**).

L'administration des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) via Kaspersky Security Center Cloud Console n'est pas prise en charge.

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description
Endpoint Detection and Response (KATA) activé/désactivé	Active ou de désactive l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA). L'intégration est désactivée par défaut.
Paramètres de connexion aux serveurs	Cliquez sur le lien **Configurer** pour ouvrir une fenêtre dans laquelle vous pouvez configurer les paramètres généraux de connexion aux serveurs KATA, ajouter un certificat de serveur et configurer l'authentification bidirectionnelle lors de la connexion aux serveurs KATA.
Serveurs KATA	Le tableau contient une liste des serveurs KATA auxquels la connexion est configurée. Le bouton **Ajouter** ouvre une fenêtre dans laquelle vous pouvez établir la connexion au serveur KATA. Les boutons situés au-dessus du tableau permettent de modifier et de supprimer les paramètres de connexion précédemment configurés.
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 de dépassement de la limite d'événements	Pourcentage de dépassement de la limite d'événements. 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`.

Fenêtre de configuration de la connexion aux serveurs

Cette fenêtre permet de configurer les paramètres généraux de connexion aux serveurs KATA, d'ajouter un certificat de serveur et de configurer l'authentification bidirectionnelle lors de la connexion 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 périphériques (télémétrie) au serveur KATA. La télémétrie est activée par défaut.
Certificat de serveur	Après avoir ajouté le certificat du serveur, les informations sur le certificat s'affichent : • 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.
Sélectionner	Ouvre une fenêtre de sélection de fichiers standard dans laquelle vous pouvez spécifier le chemin d'accès au certificat du serveur KATA.

	Si un certificat du serveur est ajouté, celui-ci est vérifié du côté de Kaspersky Endpoint Security, ce qui permet d'augmenter le niveau de sécurité de la connexion.
Supprimer	Supprime un certificat de serveur ajouté précédemment. Le bouton s'affiche uniquement si le certificat du serveur a été ajouté.
Paramètres de protection avancée	Ce groupe de paramètres vous permet d'activer ou de désactiver l'authentification bidirectionnelle lors de la connexion au serveur KATA et d'ajouter un certificat client.
Utiliser la vérification en deux étapes	Active ou désactive l'utilisation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur KATA. L'authentification bidirectionnelle doit être activée du côté du serveur KATA. Pour utiliser la vérification en deux étapes, vous devez ajouter un certificat client.
Ajouter un certificat client	Ouvre une fenêtre de sélection de fichiers standard dans laquelle vous pouvez spécifier le chemin d'accès au cryptocontainer (archive au format PFX) contenant le certificat client et la clé privée. Le bouton est disponible si la case **Utiliser la vérification en deux étapes** est cochée.
Modifier	Permet d'indiquer le mot de passe pour le cryptocontainer contenant le certificat client. Le contenu du champ **Mot de passe de conteneur de chiffrement** n'est pas modifiable. Par défaut, le mot de passe est vide. Pour indiquer un mot de passe, cliquez sur le bouton **Modifier**, saisissez le mot de passe dans la fenêtre qui s'ouvre, puis cliquez sur le bouton **OK**. Quand vous cliquez sur le bouton **Afficher** dans la fenêtre de saisie du mot de passe, celui-ci s'affiche en clair. 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. Le bouton est disponible si la case **Utiliser la vérification en deux étapes** est cochée.

Fenêtre d'ajout de paramètres pour la connexion au serveur KATA

Dans cette fenêtre, vous pouvez spécifier les paramètres de connexion au serveur KATA.

Paramètres de connexion au serveur KATA

Paramètre	Description
Adresse	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'isolation réseau de l'appareil est activée, 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 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 l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA) et configurer les paramètres d'intégration dans les propriétés de la stratégie (**Detection and Response** → **Endpoint Detection and Response (KATA)**).

Paramètres d'intégration à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description
Intégration à Endpoint Detection and Response (KATA)	Active ou de désactive l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA). L'intégration est désactivée par défaut.
Serveurs KATA	Le bouton **Configurer** ouvre la fenêtre **Serveurs KATA**. Cette fenêtre permet de configurer la connexion aux serveurs KATA, ainsi que visualiser la liste des serveurs auxquels la connexion est configurée.
Paramètres de connexion aux serveurs	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 de serveur et configurer l'authentification bidirectionnelle 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.

Fenêtre Serveurs KATA.

Cette fenêtre affiche le tableau contenant les 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.

Fenêtre d'ajout de paramètres pour la connexion au serveur KATA

Dans cette fenêtre, vous pouvez spécifier les paramètres de connexion au serveur KATA.

Paramètres de connexion au serveur KATA

Paramètre	Description
Adresse	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'isolation réseau de l'appareil est activée, 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`.

Fenêtre de configuration de la connexion aux serveurs

Cette fenêtre permet de spécifier les paramètres de connexion généraux aux serveurs KATA.

Paramètres de connexion aux serveurs 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 périphériques (télémétrie) au serveur KATA. La télémétrie est activée par défaut.
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 (certificat client)	Ouvre la fenêtre d'ajout de certificat client pour sécuriser davantage la connexion au serveur KATA. 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 KATA 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.
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 si le certificat du serveur a été ajouté.

Fenêtre d'ajout d'un certificat de serveur

Cette fenêtre permet d'ajouter un certificat de serveur KATA de l'une des manières suivantes :

- Indiquer le chemin d'accès au fichier du 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 du serveur est ajouté, celui-ci est vérifié du côté de Kaspersky Endpoint Security, ce qui permet d'augmenter le niveau de 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 KATA.

Si vous souhaitez renforcer la sécurité de connexion, vous devez activer la validation des certificats client du côté du serveur KATA et cocher la case **Utiliser la vérification en deux étapes** dans la fenêtre des paramètres de connexion aux serveurs.

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**.

Fenêtre Paramètres de transfert de données

Cette fenêtre permet de configurer les paramètres de connexion au serveur KATA.

Paramètres de transfert de données aux serveurs KATA

Paramètre	Description
Durée d'attente	Délai maximum en secondes pour l'envoi des événements au serveur KATA.

maximale pour l'envoi des événements (en secondes)	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 de dépassement de la limite d'événements	Pourcentage de dépassement de la limite d'événements. 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 Kaspersky Endpoint Detection and Response (KATA) à l'aide de la tâche prédéfinie Intégration avec Kaspersky Endpoint Detection and Response (KATA) (*KATAEDR*).

Par défaut, la tâche d'intégration avec Kaspersky Endpoint Detection and Response (KATA) n'est pas en cours d'exécution. Vous pouvez démarrer et arrêter cette tâche manuellement.

Vous pouvez configurer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) en modifiant les paramètres d'une tâche prédéfinie.

À l'aide des commandes de gestion des paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA), vous pouvez gérer les certificats utilisés pour se connecter aux serveurs KATA.

Paramètres de la tâche Intégration à Kaspersky Endpoint Detection and Response (KATA)

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 à Kaspersky Endpoint Detection and Response (KATA)

Paramètre	Description	Valeur
`Adresse`	Adresse du serveur KATA. 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`.

	Pour garantir que la communication avec le serveur KATA ne soit pas interrompue en cas d'échec de l'application lorsque l'isolation réseau de l'appareil est activée, il est recommandé de spécifier l'adresse IP du serveur.	
`Port`	Port de connexion au serveur KATA.	Valeur par défaut : `443`.
`UseClientPinnedCertificate`	Activation et désactivation de l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur KATA. Si l'authentification bidirectionnelle est activée du côté du serveur KATA, vous devez activer l'authentification bidirectionnelle dans les paramètres de la tâche Intégration à Kaspersky Endpoint Detection and Response (KATA) et ajouter un certificat client avant d'exécuter la tâche.	`Yes` : utiliser l'authentification bidirectionnelle pour sécuriser davantage la connexion au serveur KATA. `No` (valeur par défaut) : ne pas utiliser l'authentification bidirectionnelle.
`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`.
`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. `Non` - 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`.
`EnableTelemetry`	Activation et désactivation de l'envoi de données sur les événements sur les périphériques (télémétrie) au serveur KATA.	`Oui` (valeur par défaut) : envoie la télémétrie au serveur KATA. `Non` : n'envoie pas la télémétrie.

Gestion des certificats pour la connexion aux serveurs KATA

Les privilèges root sont nécessaires pour gérer les certificats.

Vous pouvez gérer les certificats qui sont utilisés pour se connecter aux serveurs KATA à l'aide de commandes. Vous pouvez effectuer les actions suivantes avec les certificats :

- ajouter ou remplacer un certificat de 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 [-R] --add-kataedr-server-certificate <nom et chemin d'accès au fichier>
```

où `<nom et chemin d'accès au fichier>` : nom et 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 <nom et chemin d'accès au fichier>
   ```

   où `<nom et chemin d'accès au fichier>` : est le nom et le chemin d'accès au cryptocontainer (archive au format 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 sécuriser la connexion au serveur KATA si la validation du certificat client est activée dans les paramètres du serveur KATA et si le paramètre `UseClientPinnedCertificate` dans les paramètres de la tâche Intégration avec Kaspersky Endpoint Detection and Response (KATA) est défini sur `yes`.

Pour afficher les informations relatives au certificat, exécutez la commande suivante :

- pour le certificat du serveur :

  ```
  kesl-control [-R] --query-kataedr-server-certificate
  ```

- pour le certificat client :

  ```
  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
```

Si l'utilisation d'un certificat est configurée dans les paramètres de la tâche Intégration à Kaspersky Endpoint Detection and Response (KATA) et que la tâche est lancée, la suppression de ce certificat se terminera par une erreur.

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.

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).

L'application Kaspersky Endpoint Security 12.1 for Linux est compatible avec Kaspersky Endpoint Detection and Response Optimum version 3.0.

Les versions de Kaspersky Endpoint Security for Linux inférieures à 12.1 ne contiennent pas le module EDR Optimum.

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 Kaspersky Threats.

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.
- Effectuez les actions de réponse visant à garantir les fonctions de sécurité sur la base des commandes reçues de Kaspersky Security Center.

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 Kaspersky Endpoint Security sont activés et fonctionnent :

   - Protection contre les menaces sur les fichiers.
   - Protection contre les menaces Internet.
   - Détection comportementale.

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 supplémentaire.

4. **Activation de l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum**

   Par défaut, l'intégration de Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum est désactivée. Vous pouvez activer et désactiver l'intégration et configurer les paramètres d'intégration :

   - à l'aide de Web Console ou de Kaspersky Security Center Cloud 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 ou Kaspersky Security Center Cloud 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 ou dans Kaspersky Security Center Cloud Console.

- À l'aide de la ligne de commande.

5. **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 activer les paramètres suivants :

   - Les **informations sur les fichiers dans la sauvegarde sont activées/désactivées**.

     Vous pouvez activer ce paramètre dans les propriétés de la stratégie dans la section **Paramètres de l'application → Paramètres généraux → Paramètres du stockage**.

     En activant ce paramètre, vous autorisez Kaspersky Security Center à transférer des informations sur les fichiers placés par l'application Kaspersky Endpoint Security dans la sauvegarde de l'appareil.

   - **Afficher les alertes EDR**.

     Vous pouvez activer ce paramètre dans la fenêtre principale de Web Console dans la section **Paramètres → Paramètres de l'interface**.

     En activant cette option, vous autoriserez l'affichage de la liste des alertes.

     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 ou désactiver l'intégration avec Kaspersky Endpoint Detection and Response Optimum :

- à l'aide de Web Console ou de Kaspersky Security Center Cloud 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 ou Kaspersky Security Center Cloud Console, vous pouvez activer ou désactiver l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum et configurer les paramètres d'intégration :

- dans les propriétés de la stratégie (**Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response Optimum**) ;
- dans les propriétés de l'appareil (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Application** → lien <nom de l'application Kaspersky Endpoint Security 12.1 for Linux> → **Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response Optimum**).

> L'activation ou la désactivation de l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum dans les propriétés de l'appareil n'est pas disponible si l'appareil est couvert par la stratégie.

Paramètres d'intégration avec Kaspersky Endpoint Detection and Response Optimum

Paramètre	Description
Endpoint Detection and Response Optimum activé/désactivé	Le bouton bascule permet d'activer ou de désactiver l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response Optimum. L'intégration est désactivée par défaut.
Isolation réseau	Cliquer sur le lien **Configurer le déverrouillage de l'appareil** ouvre la fenêtre **Configurer le déverrouillage de l'appareil** dans laquelle vous pouvez configurer la durée de verrouillage de l'appareil.
Exclusions	Le lien **Exclusions** ouvre la fenêtre **Exclusions**, dans laquelle vous pouvez configurer des exclusions de l'isolation réseau.

Activation et désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans la ligne de commande

Depuis la ligne de commande, vous pouvez activer ou désactiver l'intégration avec Kaspersky Endpoint Detection and Response 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 l'intégration avec Kaspersky Endpoint Detection and Response Optimum à l'aide des clés de la ligne de commande, exécutez la commande suivante :

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

Pour désactiver l'intégration avec Kaspersky Endpoint Detection and Response 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)

Affichage de l'état de l'intégration dans Web Console ou Kaspersky Security Center Cloud Console

Vous pouvez consulter l'état de l'intégration avec Kaspersky Endpoint Detection and Response Optimum dans Web Console ou dans Kaspersky Security Center Cloud Console en sélectionnant la section **Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Applications** → lien <nom de l'application Kaspersky Endpoint Security 12.1 for Linux> → **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*.

  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.

- *Erreur*.

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.

Pour plus d'informations sur l'utilisation des détails de l'alerte, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

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

Vous pouvez rechercher des indicateurs de compromission sur votre appareil et prendre des mesures pour répondre aux menaces à l'aide de la tâche *Analyse IOC*.

Pour rechercher des indicateurs de compromission, Kaspersky Endpoint Security utilise les fichiers IOC préparés par l'utilisateur. Les fichiers IOC doivent être conformes aux exigences relatives aux fichiers IOC.

Vous pouvez créer et lancer la tâche *Analyse IOC*, ainsi que modifier ses paramètres dans Web Console ou Kaspersky Security Center Cloud Console :

- dans la section **Actifs (Appareils)** → **Tâches** ;
- dans la section **Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → **Tâche** ;
- dans la fenêtre des détails de l'alerte.

Vous ne pouvez pas créer, lancer ou configurer la tâche *Analyse IOC* à l'aide de la ligne de commande. L'affichage de la tâche *Analyse IOC* créée dans Web Console ou Kaspersky Security Center Cloud Console n'est pas disponible à l'aide de la commande `kesl-control --get-task-list` dans la ligne de commande.

Pour cette tâche, 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.

Paramètres de la tâche *Analyse IOC*

Paramètre	Description
Redéfinir les fichiers IOC	Cliquer sur ce bouton ouvre le panneau **Redéfinir les fichiers IOC**. En cliquant sur le bouton **Ajouter des fichiers IOC** situé dans le panneau **Redéfinir les fichiers IOC**, une fenêtre s'ouvre qui vous permet de sélectionner et de télécharger les fichiers IOC nécessaires pour rechercher des indicateurs de compromission sur votre appareil. 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.
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 : • **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'isolement. • **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 et les secteurs de démarrage. Si la case n'est pas cochée, l'application ne prend aucune mesure de réponse 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.
Zones d'analyse	Les zones d'analyse des fichiers sont affichées : zones importantes des lecteurs système et le chemin depuis l'IOC.

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 d'analyse IOC pour les exécutions des tâches précédentes. Pour rechercher des indicateurs de compromission dans les nouveaux fichiers IOC, il est recommandé d'ajouter de nouvelles tâches.

Le résultat d'exécution de la tâche *Analyse IOC* peut être consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> → **Paramètres de l'application** → **Résultats d'analyse IOC**.

Le tableau de la section **Résultats d'analyse IOC** contient 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 sélectionner les résultats d'exécution des tâches pour tous les appareils administrés du groupe d'administration ou pour un appareil spécifique.

Ce tableau contient les colonnes suivantes :

- **État**.

  État de détection de compromission, affiché sous forme d'icône.

- **Appareil**.

  Nom de l'appareil sur lequel la tâche *Analyse IOC* a été effectuée.

- **Heure**.

  Date et heure d'exécution de la tâche *Analyse IOC*.

- **Résultats**.

  Informations sur le résultat de la tâche *Analyse IOC*. Suite à l'exécution de la tâche, l'un des statuts suivants peut être affiché :

  - *IOC détectés* ;

    Cet état est affiché sous forme de lien qui, lorsque vous cliquez dessus, ouvre une fenêtre avec les détails de l'alerte.

  - *Aucun IOC détecté*.

Le résultat de la tâche peut être aussi consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> sous l'onglet **Résultats** de la colonne **Description**.

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.

Exigences pour les fichiers IOC

Lors de la création de tâches d'analyse IOC, tenez compte des exigences et limitations suivantes associées 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. La présence de fichiers IOC avec les mêmes identifiants peut affecter l'exactitude des résultats de l'exécution des tâches.
- La taille d'un fichier IOC ne doit pas dépasser 2 Mo. L'utilisation des fichiers plus volumineux entraîne l'échec des tâches d'analyse IOC. La taille totale de tous les fichiers ajoutés à la collection IOC ne doit pas dépasser 10 Mo.

Si tous les fichiers font plus de 10 Mo, vous devez diviser la collection IOC et créer plusieurs tâches *Analyse IOC*.

- 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.

CHARGER 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` и `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`.

Activer ou désactiver l'isolation réseau des appareils

Vous pouvez activer l'isolation réseau des appareils des manières suivantes :

- Utilisation de la tâche *Analyse IOC* .

  Si, lors de la création et de la configuration des paramètres de la tâche Analyse IOC dans le groupe **Actions lorsqu'un IOC est détecté**, vous avez coché les cases **Appliquer les actions de réponse lorsqu'un IOC est détecté** et **Isoler l'appareil du réseau**, puis l'isolation réseau est activée automatiquement lorsque l'application détecte des indicateurs de compromission (IOC).

- Dans la fenêtre des détails de l'alerte.

- Dans les propriétés de l'appareil dans Web Console ou dans Kaspersky Security Center Cloud Console.

> L'activation de l'isolation réseau n'est disponible que si l'intégration avec la solution Kaspersky Endpoint Detection and Response Optimum est activée et que le module EDR Optimum est à l'état En cours d'exécution.

Vous pouvez désactiver l'isolation réseau d'un appareil des manières suivantes :

- Manuellement dans les propriétés de l'appareil dans Web Console ou Kaspersky Security Center Cloud Console.

- Manuellement dans la ligne de commande.

- Dans la fenêtre des détails de l'alerte.

- En configurant l'arrêt automatique dans les propriétés de l'appareil ou les propriétés de la stratégie.

> La désactivation de l'isolation réseau dans les propriétés de l'appareil et dans la ligne de commande est disponible, que l'intégration avec Kaspersky Endpoint Detection and Response Optimum soit activée et que le module EDR Optimum soit activé, et que l'appareil soit ou non couvert par la stratégie.

Vous pouvez configurer des exclusions pour les connexions réseau qui n'ont pas besoin d'être isolées lorsque l'isolation réseau est activée.

Vous pouvez vérifier l'état d'isolation réseau à partir de la ligne de commande.

Une fois l'isolation réseau activée, 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 excluions de l'isolation 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.

EDR Optimum attribue automatiquement le tag **ISOLATED FROM NETWORK** à l'appareil isolé. Une fois l'isolation réseau désactivée, ce tag est automatiquement supprimée.

Pour obtenir des informations générales sur l'obtention d'une liste des appareils isolés par balise, consultez l'aide de Kaspersky Endpoint Detection and Response Optimum.

Activer ou désactiver manuellement l'isolation réseau d'un appareil dans Web Console

Pour activer ou désactiver l'isolation réseau pour un appareil :

1. Dans la fenêtre principale de Web Console ou Kaspersky Security Center Cloud Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des périphériques 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 gérés, et dans la fenêtre qui s'ouvre, sélectionnez un groupe d'administration.

   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 12.1 for Linux**.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Accédez à l'onglet **Paramètres de l'application**.

7. Accédez à la section **Detection and Response → Endpoint Detection and Response Optimum**.

8. Dans le groupe de paramètres **Isolation réseau**, effectuez l'une des opérations suivantes :

   - pour activer l'isolation réseau de l'appareil, cliquez sur le bouton **Isoler l'appareil du réseau** ;
   - pour désactiver l'isolation réseau de l'appareil, cliquez sur le bouton **Débloquer l'appareil isolé**.

Si vous avez activé l'isolation 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.

Configuration de l'arrêt automatique de l'isolation réseau

Vous pouvez configurer l'isolation réseau pour qu'elle se désactive automatiquement après une période de temps spécifiée :

- Dans les propriétés de l'appareil.

  Le paramètre permettant de désactiver automatiquement l'isolation réseau dans les propriétés de l'appareil n'est pas disponible si l'appareil est soumis à une stratégie.

- Dans les propriétés de la stratégie.

  Les paramètres permettant de désactiver automatiquement l'isolation réseau spécifiés dans les propriétés de la stratégie s'appliquent uniquement aux appareils qui ont été isolés à la suite de la détection des indicateurs de compromission (IOC) lors de l'exécution de la tâche *Analyse IOC*.

Par défaut, l'application désactive l'isolation réseau 5 heures après son activation. Après avoir désactivé l'isolation 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'isolation réseau de l'appareil :

1. Dans la fenêtre principale de Web Console ou Kaspersky Security Center Cloud Console, sélectionnez **Actifs (Appareils) → Appareils administrés**.

   La liste des périphériques 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 12.1 for Linux**.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Accédez à l'onglet **Paramètres de l'application**.

7. Accédez à la section **Detection and Response → Endpoint Detection and Response Optimum**.

8. Dans le groupe de paramètres **Isolation réseau**, cliquez sur le lien **Configurer le déverrouillage de l'appareil**.

9. Dans la fenêtre **Configurer le déverrouillage de l'appareil** qui s'ouvre, définissez les paramètres de déverrouillage de l'appareil.

   Paramètres de déverrouillage de l'appareil

Paramètre	Description
Débloquer un appareil automatiquement isolé via	La case active ou désactive le déverrouillage automatique de l'appareil isolé après la période spécifiée dans le champ de saisie **Horloge**. Cette case est cochée par défaut.
Horloge	Champ de saisie de la période en heures après laquelle l'appareil isolé est automatiquement déverrouillé. Ce champ n'est actif que si la case **Déverrouiller l'appareil automatiquement isolé dans** est cochée.

10. Enregistrez vos modifications apportées.

Configuration de la désactivation automatique de l'isolation réseau dans les propriétés de la stratégie

Pour configurer la désactivation automatique de l'isolation réseau de l'appareil :

1. Dans la fenêtre principale de Web Console ou Kaspersky Security Center Cloud 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. Accédez à l'onglet **Paramètres de l'application**.

5. Accédez à la section **Detection and Response → Endpoint Detection and Response Optimum**.

6. Dans le groupe de paramètres **Isolation réseau**, cliquez sur le lien **Configurer le déverrouillage de l'appareil**.

7. Dans la fenêtre **Configurer le déverrouillage de l'appareil** qui s'ouvre, définissez les paramètres de déverrouillage de l'appareil.

Paramètres de déverrouillage de l'appareil

Paramètre	Description
Débloquer un appareil automatiquement isolé via	La case active ou désactive le déverrouillage automatique de l'appareil isolé après la période spécifiée dans le champ de saisie **Horloge**. Cette case est cochée par défaut.
Horloge	Champ de saisie de la période en heures après laquelle l'appareil isolé est automatiquement déverrouillé. Ce champ n'est actif que si la case **Déverrouiller l'appareil automatiquement isolé dans** est cochée.

8. Enregistrez vos modifications apportées.

Désactiver l'isolation réseau de l'appareil à partir de la ligne de commande

Pour désactiver l'isolation réseau d'un appareil à l'aide de la ligne de commande, exécutez la commande suivante :

```
kesl-control [-R] --isolation-off
```

Vous pouvez vérifier l'état de l'isolation réseau et afficher la liste des exclusions de l'isolation réseau à l'aide de la commande suivante :

```
kesl-control [-R] --isolation-stat
```

Pour l'isolation réseau, la ligne de commande affiche l'un des états suivants :

- *Isolation réseau activée*.
- *Isolation réseau désactivée*.

Configuration des exclusions de l'isolation réseau

Vous pouvez configurer les exclusions :

- dans les propriétés de la politique ;
- dans les propriétés de l'appareil.

Les connexions réseau soumises aux règles spécifiées ne seront pas bloquées sur l'appareil une fois l'isolation réseau activée.

Par défaut, l'isolation réseau exclut les profils réseau constitués de règles qui garantissent le fonctionnement ininterrompu des appareils dotés des rôles de serveur DNS/DHCP et de client DNS/DHCP.

Les exclusions définies dans les propriétés de la stratégie sont appliquées uniquement si l'isolation réseau est automatiquement activée par l'application suite à la réponse aux détections des indicateurs de compromission (IOC).

Les exclusions définies dans les propriétés de l'appareil s'appliquent uniquement si l'isolation réseau est activée manuellement dans les propriétés de l'appareil ou dans la fenêtre des détails de l'alerte.

Une stratégie active ne bloque pas l'application des exclusions de l'isolation réseau définies dans les propriétés de l'appareil.

Vous pouvez afficher une liste des exclusions de l'isolation réseau :

- dans les propriétés de la stratégie (**Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response Optimum** → lien **Exclusions**) ;
- dans les propriétés de l'appareil (**Actifs (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → lien <nom de l'application Kaspersky Endpoint Security 12.1 for Linux> → **Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response Optimum** → lien **Exclusions**) ;
- dans la ligne de commande.

Ajout et suppression d'exclusions de l'isolation réseau dans les propriétés de la stratégie dans Web Console

Dans Web Console ou Kaspersky Security Center Cloud Console, vous pouvez ajouter et supprimer des exclusions de l'isolation réseau dans les propriétés de la stratégie (**Paramètres de l'application** → **Detection and Response** → **Endpoint Detection and Response Optimum** → lien **Exclusions**).

Dans la fenêtre **Exclusions**, à l'aide des boutons au-dessus du tableau, vous pouvez effectuer les actions suivantes :

- ajouter des informations sur la connexion réseau exclue de l'une des manières suivantes :
  - cliquer sur le bouton **Ajouter**, puis saisir les informations sur la connexion réseau ;
  - cliquer sur le bouton **Ajouter depuis le profil**, puis sélectionner un profil réseau dans le dictionnaire ;
- supprimer les informations sur la connexion réseau.

Ajouter et supprimer les exclusions de l'isolation réseau dans les propriétés de l'appareil

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'isolement réseau dans les propriétés de l'appareil :

1. Dans la fenêtre principale de Web Console, sélectionnez **Actifs (Appareils)** → **Appareils administrés**.

   La liste des périphériques 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 12.1 for Linux**.

   La fenêtre des propriétés de l'application s'ouvrira.

6. Accédez à l'onglet **Paramètres de l'application**.

7. Accédez à la section **Detection and Response** → **Endpoint Detection and Response Optimum**.

8. Dans le groupe de paramètres **Isolation réseau**, cliquez sur le lien **Exclusions** pour ouvrir la fenêtre **Exclusions**.

9. 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 depuis le 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** ;

10. Enregistrez vos modifications apportées.

Ajouter une fenêtre d'exclusion de l'isolation 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	Nom de la connexion réseau.
Direction	Sens de connexion réseau.

Protocole	Protocole utilisé par la connexion réseau.
Nombre	Numéro de la connexion réseau.
Port(s)/plage(s) local(s)	Numéro(s) de port local ou plage(s) de ports locaux.
Port(s)/plage(s) distant(s)	Numéro(s) de port à distance ou plage(s) de ports à distance.
Adresse distante	Adresse IP de l'appareil à distance.

Fenêtre Dictionnaire des profils réseau

Dans cette fenêtre, vous pouvez sélectionner le profil de la connexion réseau à exclure.

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.
Shell sécurisé (SSH)	Un protocole qui permet le contrôle à distance du système d'exploitation et la tunnelisation des connexions TCP.
Modules système Linux	Modules système Linux.

Démarrage du processus

Vous pouvez lancer à distance les processus et les fichiers exécutables nécessaires sur les appareils à l'aide de la tâche *Démarrer le processus*.

Par exemple, vous pouvez lancer :

- 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 lancer la tâche *Démarrage du processus*, ainsi que modifier ses paramètres dans Web Console ou Kaspersky Security Center Cloud Console.

Vous ne pouvez pas créer, exécuter ou configurer la tâche *Démarrage du processus* à l'aide de la ligne de commande. L'affichage de la tâche *Démarrage du processus* créée dans Web Console ou Kaspersky Security Center Cloud Console n'est pas disponible à l'aide de la commande `kesl-control --get-task-list` dans la ligne de commande.

Paramètres de la tâche Démarrer le processus

Paramètre	Description
Commande exécutable	Champ de saisie de la commande de démarrage du processus. Par exemple, si vous souhaitez exécuter l'utilitaire `klnagchk` conçu pour vérifier la connexion au Serveur d'administration, vous devez saisir la commande `/<nom du répertoire>/klnagchk` puis remplir les champs restants décrits dans ce tableau ci-dessous. Le nom du répertoire peut également être saisi dans le champ **Chemin d'accès au répertoire de travail (facultatif)**. Dans ce cas, il n'est pas nécessaire de saisir le nom du répertoire dans le champ **Commande exécutable**.
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 klnagchk.log`. Cet argument indique à l'utilitaire que le résultat du travail doit être enregistré dans un fichier nommé `klnagchk.log`. Si vous devez transmettre plusieurs arguments, vous devez les séparer par des espaces.

	Par exemple, vous pouvez saisir les arguments `-logfile klnagchk.log -savecert certificate.cer`. Ces arguments indiquent à l'utilitaire qu'il doit enregistrer le résultat de son travail dans un fichier nommé `klnagchk.log`, ainsi que sauvegarder le certificat utilisé pour vérifier l'accès au Serveur d'administration dans le fichier `certificate.cer`.
Chemin d'accès au répertoire de travail (facultatif)	Champ de saisie du chemin d'accès au répertoire de travail dans lequel se trouve le script, l'utilitaire ou le fichier de l'application permettant de lancer le processus. Par exemple, vous pouvez saisir la valeur `/opt/kaspersky/klnagent64/bin/`. Si vous avez saisi un nom du répertoire dans le champ **Commande exécutable**, il n'est pas nécessaire de remplir le champ **Chemin d'accès au répertoire de travail (facultatif)**.

Le résultat de la tâche peut être consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> sous l'onglet **Résultats** de la colonne **Description**.

Arrêt du processus

Vous pouvez mettre fin à distance aux processus sur un appareil à l'aide de la tâche *Mettre fin au processus*.

Par exemple, vous pouvez terminer par :

- 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 *Démarrer le processus*.
- Scripts.

  Par exemple, vous pouvez mettre fin à distance à un script que vous avez démarré à l'aide de la tâche *Démarrer le processus*.
- Utilitaires.

  Par exemple, vous pouvez arrêter à distance l'utilitaire de test de vitesse Internet lancé à l'aide de la tâche *Démarrer le processus*.
- Annexes.

Il est impossible de terminer les processus des objets système critiques (angl. System Critical Object – SCO). SCO comprend les fichiers nécessaires au fonctionnement du système d'exploitation et de l'application Kaspersky Endpoint Security.

Vous pouvez créer et lancer la tâche *Arrêt du processus*, ainsi que modifier ses paramètres dans Web Console ou Kaspersky Security Center Cloud Console. Vous ne pouvez pas créer, exécuter ou configurer la tâche *Mettre fin au processus* à l'aide de la ligne de commande. L'affichage de la tâche *Arrêt du processus* créée dans Web Console ou Kaspersky Security Center Cloud Console n'est pas disponible à l'aide de la commande `kesl-control --get-task-list` dans la ligne de commande.

Paramètres de la tâche Mettre fin au processus

Paramètre	Description
Spécifiez le	Dans la liste déroulante, vous pouvez choisir comment spécifier le chemin d'accès au

fichier dont vous souhaitez terminer les processus	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.
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 uniquement si vous avez sélectionné la valeur **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier. Ce champ s'affiche uniquement 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 uniquement 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**.
Identifiant du processus	Champ de saisie de l'identifiant de processus (PID). Ce champ apparaît uniquement si vous avez sélectionné la valeur **Par PID** dans la liste déroulante **Spécifiez le fichier dont vous souhaitez terminer les processus**.

Le résultat de la tâche peut être consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> sous l'onglet **Résultats** de la colonne **Description**.

Reception d'un fichier depuis un appareil

Vous pouvez recevoir des fichiers depuis les appareils des utilisateurs à l'aide de la tâche *Réception d'un fichier depuis un appareil*.

Par exemple, vous pouvez recevoir un fichier journal des événements généré par une application tierce.

Vous pouvez créer et lancer la tâche *Réception d'un fichier depuis un appareil*, ainsi que modifier ses paramètres dans Web Console ou Kaspersky Security Center Cloud Console.

Vous ne pouvez pas créer, exécuter ou configurer la tâche *Réception d'un fichier depuis un appareil* à l'aide de la ligne de commande. L'affichage de la tâche *Réception d'un fichier depuis un appareil* créée dans Web Console ou Kaspersky Security Center Cloud Console n'est pas disponible à l'aide de la commande `kesl-control --get-task-list` dans la ligne de commande.

Le tableau **Réception d'un fichier** sous l'onglet **Paramètres de l'application** contient les colonnes suivantes :

- **Chemin d'accès au répertoire**.

  Chemin d'accès au répertoire du fichier situé sur l'appareil.

- **Type de vérification de la somme de contrôle**.

  Type de vérification de la somme de contrôle d'un fichier situé sur l'appareil.

À l'aide des boutons au-dessus du tableau, vous pouvez ajouter, modifier ou supprimer des données des fichiers situés sur l'appareil. La tâche *Réception d'un fichier depuis un appareil* est effectuée pour les fichiers spécifiés dans le tableau **Réception d'un fichier**.

Lorsque vous cliquez sur le bouton **Ajouter**, la fenêtre **Réception d'un fichier** s'ouvre, où vous pouvez configurer les paramètres de la tâche *Réception d'un fichier depuis un appareil*.

Paramètres de la tâche Réception d'un fichier depuis un appareil

Paramètre	Description
Précisez 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 uniquement si vous avez sélectionné **Par chemin complet** dans la liste déroulante **Précisez 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 uniquement si vous avez sélectionné la valeur **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Précisez le fichier que vous souhaitez recevoir**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier. Ce champ s'affiche uniquement si vous avez sélectionné **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Précisez 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 uniquement si vous avez sélectionné **Par chemin d'accès au répertoire et par somme de contrôle** dans la liste déroulante **Précisez le fichier que vous souhaitez recevoir**.

Suite à l'exécution de la tâche *Réception d'un fichier depuis un appareil*, une copie du fichier est enregistrée dans la sauvegarde de l'appareil. Vous pouvez télécharger cette copie depuis la sauvegarde via Web Console ou Kaspersky Security Center Cloud Console sur 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.

Tous les fichiers reçus via la tâche *Réception d'un fichier depuis un appareil* auront l'état *Infecté* dans la sauvegarde de Kaspersky Security Center, quels que soient les résultats de l'analyse des fichiers.

Le résultat de la tâche peut être consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> sous l'onglet **Résultats** de la colonne **Description**.

Suppression d'un fichier de votre appareil

Vous pouvez supprimer des fichiers de votre appareil à l'aide de la tâche *Suppression d'un fichier de votre appareil*. Cela peut être nécessaire, par exemple, pour répondre à des menaces.

Il est impossible de supprimer les objets système critiques (angl. System Critical Object – SCO). SCO comprend les fichiers nécessaires au fonctionnement du système d'exploitation et de l'application Kaspersky Endpoint Security.

Vous pouvez créer et lancer la tâche *Suppression d'un fichier de votre appareil*, ainsi que modifier ses paramètres dans Web Console ou Kaspersky Security Center Cloud Console.

Vous ne pouvez pas créer, exécuter ou configurer la tâche *Suppression d'un fichier de votre appareil* à l'aide de la ligne de commande. L'affichage de la tâche *Suppression d'un fichier de votre appareil* créée dans Web Console ou Kaspersky Security Center Cloud Console n'est pas disponible à l'aide de la commande `kesl-control --get-task-list` dans 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 uniquement 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 uniquement si vous avez sélectionné **Par chemin et somme de contrôle** dans la liste déroulante **Spécifiez le fichier à supprimer**.
Somme de contrôle du fichier	Champ de saisie de la somme de contrôle du fichier à supprimer. Ce champ s'affiche uniquement 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 uniquement 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 *Accès interdit* si vous essayez de supprimer un fichier exécutable en cours d'exécution. Créez et exécutez la tâche *Mettre fin au processus* pour ce fichier, puis réessayez.

Le résultat de la tâche peut être consulté dans la section **Actifs (Appareils)** → **Tâches** → <nom de la tâche> sous l'onglet **Résultats** de la colonne **Description**.

Intégration avec la solution Kaspersky Managed Detection and Response

La solution Kaspersky Managed Detection and Response garantit une recherche, une détection et une élimination continues des menaces visant votre organisation. L'intégration avec la solution Kaspersky Managed Detection and Response est assurée par le module de l'application Kaspersky Endpoint Security – Managed Detection and Response (ci-après également appelé MDR).

En interagissant avec Kaspersky Managed Detection and Response, l'application Kaspersky Endpoint Security peut exécuter les fonctions suivantes :

- Envoi de données de télémétrie à Kaspersky Managed Detection and Response pour la détection des menaces.
- Exécution de commandes de Kaspersky Managed Detection and Response visant à assurer des fonctions de sécurité.

Pour configurer l'intégration de l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response, il convient de procéder comme suit :

- Assurez-vous que les modules Protection contre les menaces sur les fichiers et Détection comportementale sont activés. 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.

- Activer l'utilisation de Kaspersky Security Network en mode avancé.

  Vous pouvez activer l'utilisation de Kaspersky Security Network dans la ligne de commande, dans Web Console ou dans la Console d'administration.

- Configurer Kaspersky Private Security Network L'utilisation de KPSN est requise pour envoyer la télémétrie.

  Vous pouvez configurer Kaspersky Private Security Network uniquement dans Web Console ou dans la Console d'administration.

  > La configuration de KPSN à l'aide des commandes de l'application Kaspersky Endpoint Security n'est pas disponible.

- Activer le module Kaspersky Managed Detection and Response et charger le fichier de configuration BLOB, qui se trouve dans l'archive ZIP du fichier de configuration MDR.

  Vous pouvez activer le module Managed Detection and Response et charger le fichier de configuration BLOB dans la ligne de commande, dans Web Console ou dans la Console d'administration.

Configuration de KPSN pour l'intégration avec Kaspersky Managed Detection and Response

Vous pouvez configurer l'utilisation de Kaspersky Private Security Network pour l'intégration avec Kaspersky Managed Detection and Response uniquement dans Web Console ou dans la Console d'administration.

Pour configurer KPSN, vous devez télécharger le fichier de configuration de Kaspersky Security Network (fichier avec l'extension pkcs7), qui se trouve dans l'archive ZIP du fichier de configuration MDR, sur le Serveur d'administration de Kaspersky Security Center.

En chargeant le fichier de configuration Kaspersky Security Network, 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 configurer KPSN pour l'intégration avec Kaspersky Managed Detection and Response 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 de Kaspersky Security Network (fichier avec l'extension pkcs7) et cliquez sur le bouton **Ouvrir**.
8. Cliquez sur **Enregistrer**.

Pour configurer KPSN pour l'intégration avec Kaspersky Managed Detection and Response 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 KSN privé**.

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 de Kaspersky Security Network (fichier avec l'extension pkcs7) et cliquez sur le bouton **Ouvrir**.

8. Cliquez sur le bouton **Appliquer**.

Configuration de l'intégration avec Kaspersky Managed Detection and Response dans Web Console

Dans Web Console, vous pouvez activer ou désactiver l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Managed Detection and Response et charger le fichier de configuration BLOB dans les propriétés de la stratégie (**Paramètres de l'application** → **Détection et réponse** → **Managed Detection and Response**).

Paramètres d'intégration MDR

Paramètre	Description
Managed Detection and Response activé/désactivé	Le commutateur active ou désactive le module Managed Detection and Response, nécessaire pour intégrer l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed Detection and Response. Le bouton bascule est désactivé par défaut.
Charger	En appuyant sur le bouton, vous ouvrez une fenêtre standard dans laquelle vous pouvez sélectionner le fichier de configuration BLOB.

Le fichier de configuration BLOB se trouve dans l'archive ZIP incluse dans la solution Kaspersky Managed Detection and Response.

En chargeant le fichier de configuration 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 de configuration 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 Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver l'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Managed Detection and Response et charger le fichier de configuration BLOB dans les propriétés de la stratégie (**Détection et réponse** → **Managed Detection and Response**).

Paramètres d'intégration MDR

Paramètre	Description
Activer Managed Detection and	La case active le module Managed Detection and Response, nécessaire pour intégrer l'application Kaspersky Endpoint Security avec la solution Kaspersky Managed

Response	Detection and Response. La case est décochée par défaut.
Charger	En appuyant sur le bouton, vous ouvrez une fenêtre standard de Microsoft Windows dans laquelle vous pouvez sélectionner le fichier de configuration BLOB.

Le fichier de configuration BLOB se trouve dans l'archive ZIP incluse dans la solution Kaspersky Managed Detection and Response.

En chargeant le fichier de configuration 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 de configuration 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 Managed Detection and Response ;
- charger et supprimer le fichier de configuration BLOB requis pour l'intégration ;
- 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 Managed Detection and Response à l'aide du paramètre `UseMDR` 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 `UseMDR` peut prendre les valeurs suivantes :

- `Yes` : activer le module Managed Detection and Response.
- `No` : désactiver le module Managed Detection and Response.

Vous pouvez charger et supprimer le fichier de configuration BLOB à l'aide des commandes de gestion des clés de licence.

Pour charger le fichier de configuration BLOB, exécutez la commande suivante :

```
kesl-control --load-mdr-blob <chemin d'accès au fichier de configuration MDR BLOB>
```

Pour supprimer le fichier de configuration 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.

AConfiguration 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.
  - 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 Web Console, vous pouvez configurer les paramètres de connexion du Light Agent à la SVM dans les propriétés de la stratégie (**Paramètres de l'application** → **Mode Light Agent**).

Paramètres de détection des SVM

Les paramètres décrits dans cette section s'appliquent uniquement si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels.

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 d'adresses de la 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 FQDN SVM sur une nouvelle 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 complet correspondant 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 **Ne pas tenir compte de l'emplacement des SVM** 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.

Paramètres de 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	Adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel le Serveur d'intégration est installé. Si le nom NetBIOS, localhost ou 127.0.0.1 est spécifié comme adresse, la connexion au Serveur d'intégration échoue avec une erreur.
Port	Port de connexion au Serveur d'intégration. Par défaut, le port 7271 est indiqué.
Vérifier	Lorsque vous cliquez sur le bouton, le plugin Web vérifie le certificat SSL reçu du Serveur d'intégration. Le bouton est disponible après avoir saisi l'adresse et le port de connexion au 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**.
Afficher le certificat reçu	En cliquant sur une ligne, vous pouvez visualiser des informations sur le certificat reçu du Serveur d'intégration.
Ignorer	Sélectionnez cette option pour enregistrer le certificat reçu et continuer la connexion au Serveur d'intégration. 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.

Annuler	Sélectionnez cette option pour mettre fin à la connexion au Serveur d'intégration.
Mot de passe	Mot de passe du compte administrateur du Serveur d'intégration (mot de passe du compte admin). 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.
Vérifier	En cliquant sur le bouton, le plugin Web se connecte au Serveur d'intégration. Après la connexion au Serveur d'intégration avec les droits d'administrateur, le mot de passe du compte agent est automatiquement transféré à la stratégie, qui est utilisée pour connecter les Light Agents au Serveur d'intégration. Le mot de passe est stocké sous forme chiffrée.

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 des tags pour la connexion des Light Agent	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. Vous pouvez saisir une chaîne de texte comportant jusqu'à 255 caractères comme tag. Vous pouvez utiliser n'importe quel symbole à l'exception du symbole `;`. Le champ est disponible si la case **Utiliser des tags pour la connexion des Light Agent** est cochée.

Algorithme de sélection des SVM

Dans cette fenêtre, vous pouvez spécifier quel algorithme de sélection des SVM les Light Agents pour Linux 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 de sélection	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.

des SVM standard	S'il n'y a pas de SVM locales disponibles pour se connecter, le Light Agent sélectionne la SVM qui a le moins de Light Agents connectés, quel que soit l'emplacement des SVM dans l'infrastructure virtuelle. Cette option est la sélection par défaut.
Utiliser l'algorithme de sélection des SVM avancé	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.
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 ou Numa vServer). ◦ La SVM est située dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud). 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 sur le même cluster d'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 ou Numa vServer). ◦ La SVM est déployée dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud). 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 sur 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 ou Numa vServer). ○ La SVM est située dans la même zone de disponibilité que la machine virtuelle sur laquelle Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud). S'il n'y a aucune SVM disponible pour la connexion dans le même centre de données ou zone de disponibilité où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM. • **Ne pas tenir compte de l'emplacement des SVM**. 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 **Ne pas tenir compte de l'emplacement des SVM** 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.

Paramètres de sécurité de connexion

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 sécurisée 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 sécurisée au Serveur de protection. Si la case est décochée, une connexion non sécurisée 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.

Configuration des paramètres du Light Agent dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de connexion du Light Agent à la SVM dans les propriétés de la stratégie (**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	Adresse IP au format IPv4 ou nom de domaine complet (FQDN) de l'appareil sur lequel le Serveur d'intégration est installé. 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 le nom NetBIOS, localhost ou 127.0.0.1 est spécifié comme adresse, la connexion au Serveur d'intégration échoue avec une erreur.
Port	Port de connexion au Serveur d'intégration. Par défaut, le port 7271 est indiqué.

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 les droits d'administrateur, le mot de passe du compte `agent` est automatiquement transféré à la stratégie, qui est utilisée 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 pour protéger les environnements virtuels.

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	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.

SVM définie manuellement	
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 FQDN SVM sur une nouvelle 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 complet correspondant 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 **Ne pas tenir compte de l'emplacement des SVM** 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 des tags pour la connexion des Light Agent	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. Vous pouvez saisir une chaîne de texte comportant jusqu'à 255 caractères comme tag. Vous pouvez utiliser n'importe quel symbole à l'exception du symbole `;`.

	Le champ est disponible si la case **Utiliser des tags pour la connexion des Light Agent** est cochée.

Algorithme de sélection des SVM

Dans cette fenêtre, vous pouvez spécifier quel algorithme de sélection des SVM les Light Agents pour Linux 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 de sélection des SVM standard	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. S'il n'y a pas de SVM locales disponibles pour se connecter, le Light Agent sélectionne la SVM qui a le moins de Light Agents connectés, quel que soit l'emplacement des SVM dans l'infrastructure virtuelle. Cette option est la sélection par défaut.
Utiliser l'algorithme de sélection des SVM avancé	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.
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 ou Numa vServer). ◦ La SVM est située dans le même groupe de serveurs que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud). 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 sur le même cluster d'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 ou Numa vServer).

- La SVM est déployée dans le même projet OpenStack que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud).

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 sur le même centre de données que la machine virtuelle sur laquelle le Light Agent est installé (dans une infrastructure virtuelle sur la plateforme Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Scala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux ou Numa vServer).
  - La SVM est située dans la même zone de disponibilité que la machine virtuelle sur laquelle Light Agent est installé (dans une infrastructure virtuelle gérée par la plateforme OpenStack, la plateforme VK Cloud ou la plateforme TIONICS Cloud).

S'il n'y a aucune SVM disponible pour la connexion dans le même centre de données ou zone de disponibilité où se trouve la machine virtuelle avec le Light Agent, le Light Agent ne se connecte pas à la SVM.

- **Ne pas tenir compte de l'emplacement des SVM**. 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 **Ne pas tenir compte de l'emplacement des SVM** 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.

Paramètres de sécurité de connexion

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 sécurisée 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 sécurisée au Serveur de protection. Si la case est décochée, une connexion non sécurisée 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
```

Suite à l'exécution de la commande, les informations suivantes s'affichent dans 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. Si le mode Light Agent est désactivé, l'application est utilisée en mode standard.

- 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
```

Suite à l'exécution de la commande, les informations suivantes s'affichent dans la console :

- Adresse et port du Serveur d'intégration auquel le Light Agent se connecte.
- 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
```

Suite à l'exécution de la commande, les informations suivantes s'affichent dans 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.
- Comment Light Agent détecte les SVM : à l'aide du serveur d'intégration ou à l'aide d'une liste d'adresses SVM spécifiée 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 types d'*événements* peuvent survenir 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 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.
- Dans la ligne de commande.
- Si vous utilisez l'interface utilisateur graphique de Kaspersky Endpoint Security : dans les fenêtres contextuelles de l'application.

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 inverse 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`) ;

`'\\'` est un caractère (barre oblique inverse), `'\\\\'` ce sont deux caractères (barre oblique inverse + abarre oblique inverse).

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.

- Les rapports sur les applications sont disponibles dans l'interface utilisateur graphique de Kaspersky Endpoint Security.

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 mise 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 périphériques ;
- adresses Internet des référentiels ;
- noms de fichiers, chemins d'accès aux fichiers et sommes de hash des fichiers exécutables des applications ;
- noms des catégories d'applications.

Configuration d'enregistrement des événements dans le journal du système d'exploitation

Par défaut, les événements survenus lors du fonctionnement de l'application Kaspersky Endpoint Security ne sont pas enregistrés dans le journal du système d'exploitation. Vous pouvez activer l'enregistrement des événements dans ce journal à l'aide de Web Console, de la Console d'administration ou de la ligne de commande.

Dans Kaspersky Security Center, vous pouvez également sélectionner les événements qui seront enregistrés dans le journal du système d'exploitation.

Configuration dans Web Console

Dans Web Console, vous pouvez configurer l'enregistrement des événements dans le journal du système d'exploitation dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**).

Le lien **Configurer les notifications** dans le groupe **Notifications** ouvre la fenêtre **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.

Toutes les cases sont décochées par défaut.

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 (**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.

Toutes les cases sont décochées par défaut.

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 paramètrees 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. À partir de la ligne de commande, vous pouvez configurer les paramètres suivants du journal des événements de l'application à l'aide des paramètres généraux de l'application :

- Modifier le chemin d'accès à la base de données du journal des événements de l'application 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 : 500000. Quand la quantité maximale d'événements définie est atteinte, l'application supprime les événements les plus anciens.

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.

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 événements dans Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Afficher les événements dans la ligne de commande

En utilisant la 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 du filtre >"
```

Les conditions du filtre sont spécifiées à l'aide d'une ou plusieurs expressions logiques au format `< champ > < opération de comparaison > '< valeur >'` combinées à l'aide de l'opérateur logique `and`.

Exemple :
Afficher les événements TaskStateChanged :

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Exemple :
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 >` : le chemin complet du fichier de base de données du journal des événements à partir duquel vous souhaitez récupérer 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`.

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 des événements stockés par une application est déterminé par le paramètre général de l'application `MaxEventsNumber`.

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
```

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 du filtre >" [--db < fichier de base de données >]
[-n < nombre >] [--json] [--reverse]
```

où :

- `< conditions du filtre >` : 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 >` : nombre de derniers événements de la sélection (c'est-à-dire le nombre d'enregistrements 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 du filtre >" [--db < fichier de base de données >]
[-n < nombre >] --file < nom et chemin d'accès au fichier > [--json]
```

où `--file < nom et chemin d'accès au fichier >` est le chemin complet du fichier dans lequel vous souhaitez générer les événements.

Vérification de l'intégrité des composants 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 peut remplacer un ou plusieurs modules ou fichiers exécutables d'application par d'autres fichiers contenant du code malveillant. Pour empêcher le remplacement des modules et des fichiers, l'application Kaspersky Endpoint Security peut vérifier l'intégrité des composants 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 ;
- plug-in d'administration de l'application Kaspersky Endpoint Security.

L'application 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.

C'est à l'utilitaire de vérification de l'intégrité qu'il convient de vérifier l'intégrité des modules de l'application.

L'utilitaire de vérification de l'intégrité doit être exécuté sous un compte utilisateur doté des autorisations root.

Dans le cadre de la vérification de l'intégrité, vous pouvez utiliser l'utilitaire installé avec l'application ou un utilitaire fourni sur le CD certifié.

Afin de garantir l'intégrité de l'utilitaire de vérification, il est conseillé d'opter pour la version reprise sur le disque certifié. Lors de lancement de l'utilitaire à partir du CD, il faut renseigner le chemin d'accès complet au fichier de manifeste.

L'utilitaire de vérification de l'intégrité installé avec l'application se trouve à l'emplacement suivant :

- pour la vérification du paquet de l'application, du paquet de l'interface utilisateur graphique et de l'Agent d'administration : /opt/kaspersky/kesl/bin/integrity_checker ;
- pour la vérification du plug-in d'administration Kaspersky Endpoint Security : dans le répertoire contenant les modules exécutables (DDL) du plug-in d'administration :
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_checker.exe : pour les systèmes d'exploitation 32 bits ;
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version du plug-in>.plg\integrity_checker.exe : pour les systèmes d'exploitation 64 bits ;

Les fichiers de manifeste se trouvent dans les emplacements suivants :

- /opt/kaspersky/kesl/bin/integrity_check.xml (pour la vérification de l'intégrité du paquet de l'application) ;
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml (pour la vérification de l'intégrité du paquet de l'interface utilisateur graphique) ;
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml (pour l'analyse de l'Agent d'administration des systèmes d'exploitation 32 bits) ;
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml (pour l'analyse de l'Agent d'administration des systèmes d'exploitation 64 bits).

Pour vérifier l'intégrité des composants d'application, exécutez la commande suivante :

- Pour vérifier l'intégrité du paquet de l'application et du paquet de l'interface utilisateur graphique :

  `integrity_checker [<chemin vers le fichier de manifeste>] --signature-type kds-with-filename`

- Pour vérifier le plug-in d'administration de Kaspersky Endpoint Security et de l'Agent d'administration :

  `integrity_checker [<chemin vers le fichier de manifeste>]`

  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>` : chemin d'accès au répertoire contenant la liste des certificats révoqués (Certificate Revocation List).
- `--version` : affiche la version de l'utilitaire.
- `--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 d'analyse récapitulative seront fournis.
- `--trace <nom de fichier>`, où `<nom de fichier>` est le nom du fichier dans lequel les événements avec le niveau de détail DEBUG qui se sont produits pendant l'analyse seront enregistrés.
- `--signature-type kds-with-filename` : type de signature à vérifier (ce paramètre est indispensable pour vérifier le paquet d'application, le paquet d'interface utilisateur graphique et l'Agent d'administration).
- `--single-file <fichier>` : vérifie un seul fichier inclus dans le manifeste ; les autres objets du manifeste sont ignorés.

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 *IntegrityCheckFailed* dans le journal des événements et dans Kaspersky Security Center.

Administration des applications via une interface utilisateur graphique

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.

Grâce à l'interface utilisateur 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 menaces sur les fichiers.
  - Analyse des disques amovibles.
  - Protection contre les menaces Internet.
  - Protection contre les menaces réseau.
  - Protection contre le chiffrement.
  - Gestion du pare-feu.
  - Contrôle des applications.
  - Contrôle des appareils.
  - Détection comportementale.
  - Contrôle de l'intégrité du système.
- Démarrer et arrêter des tâches d'analyse :
  - Analyse des logiciels malveillants.
  - Analyse des zones critiques.
  - Analyser les conteneurs.
- Démarrer et arrêter les tâches de mise à jour et de restauration de la base de données.
- Lancer une analyse personnalisée des fichiers et des répertoires (lancée lorsque vous cliquez sur le fichier ou le répertoire que vous souhaitez analyser).
- Activer ou désactiver l'utilisation de Kaspersky Security Network.
- Afficher les statistiques et les rapports des applications.
- 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.
- Afficher des informations sur les objets placés dans la sauvegarde.
- Générer des fichiers de trace de l'application.

Lorsque le module et la tâche de l'application s'exécute en mode informatif, l'interface utilisateur graphique de l'application affiche l'avertissement *Mode de fonctionnement informatif sélectionné* pour le module et la tâche.

Interface utilisateur graphique

Icône de l'application dans la zone de notification

Après avoir installé le paquet d'interface utilisateur graphique de l'application Kaspersky Endpoint Security sur l'appareil, l'icône de l'application apparaît dans la zone de notification de la barre des tâches à droite.

L'icône de l'application agit comme un raccourci vers le menu contextuel et la fenêtre principale de l'application.

Le menu contextuel de l'icône de l'application contient les éléments suivants :

- **Kaspersky Endpoint Security 12.1 for Linux**. Ouvre la fenêtre principale 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.
- **Sortie**. Quitte l'interface utilisateur graphique de l'application.

Fenêtre principale de l'application

Vous pouvez ouvrir la fenêtre principale de l'application d'une des manières suivantes :

- 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.
- En sélectionnant le nom de l'application dans le menu de l'application du gestionnaire de fenêtres du système d'exploitation.

La fenêtre principale de l'application est divisée en plusieurs parties :

- La partie centrale de la fenêtre principale de l'application affiche l'état de la protection de l'appareil. Lorsque vous cliquez sur cette zone de la fenêtre, la fenêtre **Centre de protection** s'ouvre. 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 bouton **Analyse** affiche l'état de la tâche d'analyse des logiciels malveillants et le nombre de menaces détectées. Ce bouton permet d'ouvrir la fenêtre **Analyse**. 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 bouton **Mise à jour** affiche l'état de la tâche *Mise à jour*. Ce bouton permet d'ouvrir la fenêtre **Mise à jour**. Dans cette fenêtre, vous pouvez exécuter les tâches *Mise à jour* et *Annulation de la mise à jour*. En outre, vous pouvez afficher des rapports pour ces tâches.
- La partie inférieure de la fenêtre principale de l'application 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 **Configuration**. 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 **Support**. Cliquer sur ce bouton ouvre la fenêtre **Assistance**, qui affiche la version actuelle de l'application et les informations suivantes :

  - **Clé** : clé de licence active ajoutée à l'application ou informations sur l'absence de clé. En utilisant le lien dans ce champ, vous pouvez ouvrir la fenêtre **Licence**, qui affiche des informations détaillées sur la licence.

  - **État de la clé** : informations sur l'état de la clé de licence 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 ;

  Au bas de la fenêtre, des liens vers les ressources d'informations de Kaspersky et un lien ouvrant la fenêtre **Traces** sont affichés. Cette fenêtre vous permet de créer des fichiers de trace de l'application et configurer le niveau de détail des fichiers de trace.

- La partie 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). Cliquer sur cette zone de la fenêtre ouvre la fenêtre **Licence**, 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.

Activer ou désactiver les modules de l'application

À l'aide de l'interface utilisateur graphique, vous pouvez activer et désactiver les modules de l'application. Si le module est activé, le bouton **Désactiver** est disponible. Par défaut, seuls les modules Protection contre les menaces sur les fichiers, 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.

Si le module est désactivé, le bouton **Activer** est disponible.

Pour activer ou désactiver un module de l'application :

1. Ouvrez la fenêtre principale 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 **Activer** ou **Désactiver** 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'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).

Démarrer et arrêter la tâche de mise à jour

Pour démarrer ou arrêter une tâche de mise à jour :

1. Ouvrez la fenêtre principale 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'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

Grâce à l'interface utilisateur graphique, vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network.

Pour activer l'utilisation de Kaspersky Security Network :

1. Ouvrez la fenêtre principale 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. 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 standard KSN**, 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 termes de la Déclaration** de **Kaspersky Security Network**.
6. Cliquez sur **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'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.

Affichage des rapports

À l'aide de l'interface utilisateur graphique, vous pouvez visualiser les rapports de l'application. Les rapports enregistrent des informations sur le fonctionnement des modules et des tâches 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 sont affichés dans une fenêtre qui s'ouvre en cliquant sur le bouton **Rapports** situé en bas de la fenêtre principale de l'application.

Les rapports suivants sont disponibles dans l'application :

- **Statistiques**. Ce rapport contient des informations statistiques sur le fonctionnement du module Protection contre les menaces sur les fichiers et sur les tâches d'analyse. Vous pouvez mettre à jour le rapport affiché en cliquant sur le bouton **Recharger**.
- **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 menaces sur les fichiers.
  - Analyse des disques amovibles.
  - Protection contre le chiffrement.
  - Protection contre les menaces Internet.
  - Protection contre les menaces réseaux.
  - Gestion du pare-feu.

- Contrôle des applications.
- Contrôle des périphériques.
- Détection comportementale.
- Contrôle de l'intégrité du système.

- **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 vérifications de l'intégrité du système.

Pour consulter un rapport :

1. Ouvrez la fenêtre principale 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 afficher des informations détaillées sur un événement, sélectionnez cet événement dans le rapport.

   Une section qui contient les attributs de cet événement s'affiche au bas de la fenêtre.

Pour faciliter le traitement des rapports, vous pouvez modifier la présentation des données à l'écran de la manière suivante :

- Filtrez la liste des événements par période d'occurrence.
- Utilisez la fonction de recherche pour trouver un événement spécifique.
- Affichez l'événement sélectionné dans une section distincte.

Afficher les objets de la sauvegarde

À l'aide de l'interface utilisateur graphique, vous pouvez effectuer les actions suivantes avec les objets de la sauvegarde :

- 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'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 utilisateur 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.

Vous pouvez activer l'application en ajoutant une clé de licence active.

L'*activation* est le processus 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 vous utilisez l'application sous une licence qui n'inclut pas la fonctionnalité Kaspersky Endpoint Detection and Response Optimum, pour activer cette fonctionnalité, vous devez ajouter une clé de licence supplémentaire de Kaspersky Endpoint Detection and Response Optimum Add-on (ci-après, la "clé EDR Optimum").

Vous pouvez également 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.

La clé de réserve ne peut être ajoutée qu'après l'ajout de la clé de licence active.

Ajout d'une clé de licence

Pour ajouter une clé de licence active à l'application :

1. Ouvrez la fenêtre principale de l'application.
2. Exécutez une des actions suivantes :
   - Dans la partie inférieure de la fenêtre principale de l'application, 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 de l'application, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, ouvrez la fenêtre **Licence** à l'aide du lien dans le champ **Clé**.

La fenêtre **Licence** s'ouvre. 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. Vous pouvez activer l'application à l'aide d'une licence commerciale ou d'une licence d'évaluation.

   Pour activer une 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, cliquez sur le bouton **Ajouter une clé** et dans la fenêtre qui s'ouvre, sélectionnez un fichier avec l'extension de clé.

      La fenêtre affichera les informations sur la clé et la licence qui lui est associée.

   b. Cliquez sur le bouton **Activer**.

   Pour 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 ajouté la clé active de l'application, vous pouvez ajouter une clé de réserve et, si nécessaire, une clé EDR Optimum supplémentaire. Pour démarrer la procédure d'ajout d'une clé de réserve ou supplémentaire, utilisez le bouton **Ajouter** en haut de la fenêtre **Licence**.

Suppression de la clé de licence

Pour supprimer une clé de licence ajoutée à une application :

1. Ouvrez la fenêtre principale de l'application.

2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale de l'application, 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 de l'application, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, ouvrez la fenêtre **Licence** à l'aide du lien dans le champ **Clé**.

   La fenêtre **Licence** s'ouvre.

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 sur la licence

Pour consulter les informations sur la licence :

1. Ouvrez la fenêtre principale de l'application.
2. Exécutez une des actions suivantes :

   - Dans la partie inférieure de la fenêtre principale de l'application, 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 de l'application, cliquez sur bouton **Assistance** et dans la fenêtre **Assistance** qui s'ouvre, ouvrez la fenêtre **Licence** à l'aide du lien dans le champ **Clé**.

   La fenêtre **Licence** s'ouvre.

La fenêtre affiche des informations sur la licence sous laquelle l'application est utilisée et sur la licence associée à la clé de réserve si la clé de réserve est ajoutée 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 les informations sur les clés actives et les licences associées :

- Le type de licence active de l'application, la restriction de licence et la date d'expiration de la licence.
- **Clé** est une succession unique de caractères alphanumériques.
- **Statut 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 au format UTC.
- **Nom de l'application** est le 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.

Si vous avez ajouté une clé active EDR Optimum à l'application, les informations sur cette clé et sa licence associée sont également affichées dans le groupe **Licences actives**.

Le groupe **Clés de réserve** affiche les informations sur les clés de réserve et les licences associées :

- Le type de clé de réserve, la restriction de licence et la période de validité de la licence associée à la clé.
- **Clé** est une succession unique de caractères alphanumériques.
- **Type de licence** : type de licence associé à la clé de réserve.
- **Nom de l'application** est le 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.

Si vous avez ajouté une clé de réserve EDR Optimum à l'application, les informations sur cette clé et sa licence associée sont également affichées dans le groupe **Clés de réserve**.

Création d'un fichier de trace

À l'aide de l'interface utilisateur graphique, vous pouvez créer des fichiers de trace de l'application et configurer le niveau de détail des fichiers de trace.

Pour créer un fichier de trace :

1. Ouvrez la fenêtre principale 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 **Traces** pour ouvrir la fenêtre **Traces**.
4. Dans la liste déroulante **Niveau**, sélectionnez le niveau de détail du fichier de trace.

   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 trace.
6. Reproduisez la situation dans laquelle vous rencontrez un problème.
7. Cliquez sur le bouton **Désactiver** pour arrêter le processus de traces.

Les fichiers de trace créés sont stockés dans le répertoire /var/log/kaspersky/kesl/.

Application conteneur Kaspersky Endpoint Security (conteneur KESL)

Le kit de distribution de l'application Kaspersky Endpoint Security contient les fichiers pour la compilation de l'application en conteneur (ci-après conteneur KESL) en vue de l'intégration dans les systèmes externes afin de pouvoir analyser les images de conteneur dans les référentiels contenant des images.

Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, la fonctionnalité du conteneur KESL n'est pas prise en charge.

Le conteneur KESL vous permet de :

- Analyser les images de conteneurs hébergées dans les référentiels.
- Transférer les images vérifiées qui ne contiennent pas d'objets infectés vers un référentiel approuvé.

Après le déploiement, l'activation et la configuration du conteneur KESL, les modules fonctionnels et tâches suivants de l'application Kaspersky Endpoint Security y sont disponibles :

- Module Protection contre les menaces sur les fichiers
- Tâches d'analyse :
  - Analyse des logiciels malveillants ;
  - Analyse des zones critiques ;
  - Analyse du conteneur.
- Module Surveillance du conteneur.

Les fonctions supplémentaires suivantes de l'application Kaspersky Endpoint Security sont disponibles dans le conteneur KESL :

- Activation de l'application à l'aide d'un fichier clé ou d'un code d'activation.
- Mise à jour des bases de données de l'application et restauration des mises à jour des bases de données.
- Enregistrement de copies de sauvegarde des fichiers sur la sauvegarde située sur l'appareil.

L'interaction avec le conteneur KESL s'effectue via API REST et vous pouvez également configurer les paramètres du conteneur KESL dans Kaspersky Security Center à l'aide des stratégies.

Pour garantir le bon fonctionnement du conteneur KESL dans Kaspersky Security Center, il est conseillé de placer les appareils qui correspondent aux conteneurs KESL dans un groupe d'administration distinct avec sa propre stratégie. Dans les propriétés de la stratégie, toutes les fonctions et paramètres de l'application Kaspersky Endpoint Security peuvent être modifiés, mais la configuration des paramètres qui ne sont pas pris en charge dans le conteneur KESL n'affecte pas le fonctionnement du conteneur KESL.

L'administration du conteneur KESL via la ligne de commande n'est pas pris en charge.

Si un conteneur KESL a été activé lors du déploiement et connecté à Kaspersky Security Center, configuré pour distribuer automatiquement la clé de licence aux appareils administrés, cette clé ne s'applique pas aux appareils correspondant aux conteneurs KESL.

Déploiement et activation du conteneur KESL

Description du paquet de déploiement

Le paquet de déploiement contient les fichiers suivants :

- docker-service-<version>.tgz : archive contenant les fichiers indispensables à la création de l'image ;
- kesl-<version>.rpm : paquet d'installation de l'application Kaspersky Endpoint Security ;
- klnagent.rpm : paquet d'installation de l'Agent d'administration de Kaspersky Security Center.

L'archive docker-service-<version>.tgz contient les fichiers suivants :

- kesl-service : répertoire des fichiers de l'application en conteneur ;
- Dockerfile : fichier pour la création de l'image docker d'une version antérieure à 18.06 ;
- Dockerfile.1809 : fichier pour la création de l'image docker d'une version postérieure à 18.05 ;
- build.sh.example : exemple de script pour la création de l'image ;
- run.sh.example : exemple de script de lancement du conteneur KESL ;
- kesl-service.config.example : exemple de fichier de configuration de l'application en conteneur ;
- klnagent.conf.example : exemple de fichier de configuration pour la connexion à Kaspersky Security Center ;
- readme.md : aide brève.

Déploiement et activation du conteneur KESL

Pour préparer le conteneur KESL en vue de son utilisation :

1. Décompactez l'archive tar -xvf docker-service-<version>.tgz.
2. Si vous souhaitez configurer les paramètres du conteneur KESL via Kaspersky Security Center, procédez comme suit :
   a. Dans le fichier klnagent.conf.example, renseignez les valeurs des variables de l'Agent d'administration. Vous trouverez des informations complémentaires dans l'aide de Kaspersky Security Center (section « *Installation de l'Agent d'administration pour Linux en mode silencieux (avec fichier de rapports)* »).
   b. Copiez klnagent.conf.example dans kesl-service/klnagent.conf.
3. Récoltez l'image Docker du conteneur KESL à l'aide du script d'installation build.sh.example :

a. En cas d'utilisation d'un serveur proxy, indiquez les valeurs requise pour la variable COMMON_AGRS.

b. Si nécessaire, remplacez le nom de l'image kesl-service par le nom requis.

c. Copiez build.sh.example dans build.sh et donnez-lui l'attribut de fichier exécutable.

d. Lancez build.sh.

4. Confirmez que la compilation a réussi en exécutant la commande `docker images -a`.

   Le résultat suivant doit s'afficher :

   ```
   REPOSITORY TAG IMAGE ID CREATED SIZE
   kesl-service latest <hex> < heure de création > < taille >
   ```

5. Activez le conteneur KESL d'une des méthodes suivantes :

   - Via Kaspersky Security Center. Pour activer un conteneur KESL, vous devez ajouter la clé aux appareils qui correspondent aux conteneurs KESL dans Web Console ou dans la Console d'administration.

     > Pour garantir le bon fonctionnement du conteneur KESL dans Kaspersky Security Center, il est conseillé de placer les périphériques qui correspondent aux conteneurs KESL dans un groupe d'administration distinct avec sa propre stratégie. Lorsque le conteneur KESL est arrêté, ces périphériques seront automatiquement supprimés du groupe d'administration, et la clé utilisée sur ces périphériques sera libérée.

   - Via le fichier de configuration.

   - Via une variable d'environnement (cf. Étape 7).

6. Configurez le conteneur KESL (Configuration du conteneur KESL, Paramètres du conteneur KESL).

7. Lancez le conteneur KESL à l'aide de la commande `docker run --privileged --init -p < port_du_conteneur_KESL >:< port_du_périphérique > \`

   ```
   -e < variable_1> -e < variable_2> ... -e < variable_n> \
   -v < point de montage_1> -v < point de montage_2> ... -v < point de montage_n> \
   < nom_de_l'image >
   ```

   où :

   - `< port_du conteneur KESL >` désigne le port du conteneur KESL qui doit être accessible pour le réseau en-dehors du conteneur KESL ;

   - `< port_périphérique >` désigne le port du périphérique sur lequel le conteneur KESL est installé.

   Lors de l'exécution d'un conteneur KESL, vous pouvez activer le conteneur KESL via une variable d'environnement :

   - Si vous utilisez un code d'activation, ajoutez le paramètre `KRAS4D_ACTIVATION='< code d'activation >'` :

     ```
     docker run ... -e KRAS4D_ACTIVATION='< code d'activation >'
     ```

   - Si vous utilisez un fichier de clés, ajoutez les paramètres `KRAS4D_ACTIVATION='< fichier clé >'` et `KRAS4D_KEYPATH=/root/kesl-service/keys` :

```
docker run ... -e KRAS4D_ACTIVATION='<fichier clé>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <chemin d'accès au dossier des clés>:/root/kesl-service/keys
```

Vous pouvez obtenir un exemple de commande d'exécution dans le fichier run.sh.example.

Configuration du conteneur KESL

Les paramètres du conteneur KESL peuvent être configurés de plusieurs manières :

- Par défaut (si aucune autre méthode n'est indiquée).
- Depuis un Fichier de configuration. Dans ce cas, les valeurs du fichier de configuration ont priorité sur les valeurs par défaut.
- Transfert des valeurs vers le conteneur KESL lors de son lancement sous la forme de variables d'environnement. Les variable d'environnement ont priorité sur les paramètre du fichier de configuration.
- Dans le corps d'une requête d'analyse. Les paramètres dans le corps de la requête ont la priorité maximale, mais sont valides pour une seule requête.

Paramètres du conteneur KESL

Le tableau suivant reprend les paramètres du conteneur KESL et leur valeur par défaut.

Paramètres du conteneur KESL

Description du paramètre	Valeurs possibles	Valeur par défaut
Port pour l'écoute de l'API REST		8085
Gravité des événements	`debug` : débogage `info` : pour information `warning` : avertissement `error` : erreur `critical` : critique `noset` : non défini	noset
Clé d'autorisation	Si le paramètre `KRAS4D_XAPIKEY` a été défini, la vérification de la présence de l'en-tête x-api-key et de sa correspondance à la valeur du paramètre `KRAS4D_XAPIKEY` a lieu. Si ces conditions ne sont pas remplies, la requête est rejetée. Si ce paramètre manque, l'analyse n'a pas lieu.	
Code d'activation ou fichier clé	Pour pouvoir activer un conteneur KESL à l'aide d'un code d'activation lors du lancement du conteneur KESL, il faut renseigner le code d'activation dans le fichier de configuration ou le transmettre via une variable d'environnement : `docker run ... -e KRAS4D_ACTIVATION='<code d'activation>'`	

	Pour pouvoir activer un conteneur KESL à l'aide d'un fichier clé lors du lancement du conteneur KESL, il faut renseigner le fichier clé dans le fichier de configuration ou le transmettre via une variable d'environnement : `docker run ... -e KRAS4D_ACTIVATION='<fichier clé>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <chemin d'accès au dossier des clés>:/root/kesl-service/keys` Pour pouvoir activer le conteneur KESL à l'aide d'un fichier clé, le point de montage /root/kesl-service/keys doit exister.	
Paramètres d'analyse supplémentaires	Le paramètre facultatif `KRAS4D_SCANOPTIONS` permet de configurer les paramètres de la tâche Analyse du conteneur : `docker run ... -e KRAS4D_SCANOPTIONS='<paramètres>'` où `<paramètres>` représente les paramètres de la tâche Analyse du conteneur.	
Paramètres avancés de mise à jour	Le paramètre facultatif `KRAS4D_UPDATEOPTIONS` permet de configurer les paramètres de la tâche de mise à jour : `docker run ... -e KRAS4D_UPDATEOPTIONS='<paramètres>'` où `<paramètres>` représente les paramètres de la tâche Mise à jour `SourceType`, `ApplicationUpdateMode` et les paramètres de la section `CustomSources.item_#`.	
Mettre à jour les bases de l'application au lancement du conteneur KESL	Par défaut, le téléchargement des bases de l'application dans le répertoire /var/opt/kaspersky/kesl/private/updates a lieu au lancement du conteneur KESL. Pour permettre le fonctionnement simultané de plusieurs conteneurs KESL avec un exemplaire des bases de l'application et/ou accélérer le lancement du conteneur du conteneur KESL, il est conseillé de placer ce répertoire sur l'appareil où se trouve le conteneur KESL via montage : `docker run ... -v <chemin d'accès au répertoire des bases>:/var/opt/kaspersky/kesl/private/updates`	True
Ne pas traiter l'image si elle se trouve déjà dans le référentiel cible		False
Temps d'attente maximal pour l'exécution des commandes de l'application en secondes		600
Temps d'attente maximal pour l'exécution de la tâche de mise à jour des bases de l'application, en secondes		600
Nom du fichier de configuration du conteneur KESL		kesl-service.config

Variables d'environnement

Les variables d'environnement suivantes peuvent intervenir dans la configuration du conteneur KESL.

- KRAS4D_PORT : port d'écoute de l'API REST.
- KRAS4D_LOGLEVEL : gravité de l'événement.
- KRAS4D_XAPIKEY : clé d'autorisation de la requête.
- KRAS4D_ACTIVATION : code d'activation ou nom du fichier clé.
- KRAS4D_SCANOPTIONS : paramètres d'analyse avancés.
- KRAS4D_UPDATEOPTIONS : paramètres de mise à jour avancés.
- KRAS4D_FORCEUPDATE : mettre à jour les bases de l'application au lancement du conteneur KESL.
- KRAS4D_SKIPIMAGEIFEXISTS : ne pas traiter l'image si elle se trouve déjà dans le référentiel cible.
- KRAS4D_GENERALTIMEOUT : temps maximal d'attente pour l'exécution des commandes de l'application.
- KRAS4D_UPDTASKTIMEOUT : temps d'attente maximal pour l'exécution de la tâche de mise à jour des bases de l'application.
- KRAS4D_CFGNAME : nom du fichier de configuration du conteneur KESL.

Fichier de configuration

Le fichier de configuration du conteneur KESL possède l'extension yaml. Pour permettre la lecture des paramètres d'un fichier, il faut monter le chemin /root/kesl-service/config/ sur l'appareil où est installé le conteneur KESL et indiquer le nom du fichier de configuration si celui-ci diffère du nom par défaut. Ainsi, il est possible d'indiquer un fichier de configuration pour chaque sélection de conteneurs KESL.

Exemple de lancement d'un conteneur KESL :

```
docker run ... \
-e KRAS4D_CFGNAME='unique_file_name' \
-v <HOST_PATH>:/root/kesl-service/config \
kesl-service
```

Le tableau ci-dessous reprend les paramètres du fichier de configuration et les variables d'environnement correspondantes.

Correspondance des paramètres aux variables d'environnement

Paramètre du fichier de configuration	Variable d'environnement
Section common	
port: <port d'écoute>	# KRAS4D_PORT=8085
sqlpath: <chemin d'accès complet au fichier de la base des résultats des	# KRAS4D_SQLPATH

analyses>	
certdir: <chemin du répertoire contenant les certificats des registres>	# KRAS4D_CERTDIR
keypath: <chemin du répertoire contenant les clés de licence>	# KRAS4D_KEYPATH
tmppath: <chemin d'accès complet au répertoire temporaire>	# KRAS4D_TMPPATH
logpath: <chemin d'accès complet au journal des événements>	# KRAS4D_LOGPATH
loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
Section control	
xapikey: <clé d'autorisation de la requête>	# KRAS4D_XAPIKEY=None
forceupdate: <mise à jour forcée des base au lancement du conteneur [True|False]>	# KRAS4D_FORCEUPDATE
activation: <code d'activation ou nom du fichier clé tiré de /root/kesl-service/config/>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION
scanoptions: <paramètres d'analyse [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <ne pas analyser l'image si elle se trouve sur le serveur sur lequel il faut copier l'image analysée>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <temps d'attente maximal pour l'exécution des commandes de l'application>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <temps d'attente maximal pour l'exécution de la tâche de mise à jour des bases de l'application>	# KRAS4D_UPDTASKTIMEOUT
Section repositories	
<server>:<port>: adresse et port du registre d'images qui requiert une autorisation lors de la requête d'analyse	
Sous-section credentials	
user: nom d'utilisateur pour l'autorisation dans le registre d'images	
pass: mot de passe pour l'autorisation dans le registre d'images	

Exemple de fichier de configuration :

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

Points de montage accessibles

Pour pouvoir utiliser un conteneur KESL, vous pouvez utiliser les points de montage suivants :

- /root/kesl-service/data/scans.sqlite : chemin d'accès au fichier de la base de données des résultats de l'analyse ;
- /var/opt/kaspersky/kesl/private/updates : chemin d'accès aux bases de l'application ;
- /root/kesl-service/certificates : chemin vers le répertoire contenant les certificats des référentiels ;
- /root/kesl-service/keys : chemin vers le répertoire contenant les clés de licence ;
- /var/log/kaspersky/ : chemin d'accès au répertoire du journal des événements ;
- /root/kesl-service/config/ : chemin d'accès au fichier de configuration ;
- /var/lib/containers/vfs-storage : point de montage obligatoire pour garantir le bon fonctionnement de l'utilitaire Podman.

Administration du conteneur KESL via l'API REST

L'interaction avec le conteneur KESL s'opère via l'API REST. Grâce à l'API REST, vous pouvez :

- Exécuter l'analyse d'un fichier ou de plusieurs. Pour ce faire, envoyer la requête d'analyse (POST).

  Exemple :
  POST http://<server>:<port>/scans

  Fichier ou plusieurs fichiers.

- Exécuter l'analyse d'une ou de plusieurs images Docker. Pour ce faire, envoyer la requête d'analyse (POST).

  Exemple :
  POST http://<server>:<port>/scans

  Lien vers la ou les images Docker à analyser.

- Exécuter l'analyse d'une ou de plusieurs images Docker avec des paramètres avancés. Pour ce faire, envoyer la requête d'analyse (POST).

  Exemple :
  POST http://<server>:<port>/scans

  JSON d'un type déterminé.

- Obtenir la liste des sessions d'analyse. Pour ce faire, envoyez une requête d'obtention d'informations sur les sessions d'analyse (GET).

  Exemple :
  GET http://<server>:<port>/scans

- Obtenir des informations sur la session d'analyse. Pour ce faire, envoyez une requête d'obtention d'informations sur les sessions d'analyse (GET).

  Exemple :
  GET http://<server>:<port>/scans/<ID unique de la session d'analyse>

- Ajouter un certificat de registre sans redémarrer le conteneur KESL. Pour ce faire, envoyez une requête d'ajout de certificat de registre (POST).

  Exemple :
  POST http://<server>:<port>/addcert

- Obtenir les informations sur l'état du conteneur KESL. Pour ce faire, envoyez une demande pour obtenir des informations sur l'état du conteneur KESL (GET).

  Exemple :
  GET http://<server>:<port>/status

Requête d'analyse (POST)

Fonction

Analyse d'un objet indiqué dans le corps de la requête.

L'analyse des objets suivants est prise en charge :

- un fichier ;
- plusieurs fichiers ;
- une ou plusieurs images Docker dans un référentiel donné ;
- une ou plusieurs images Docker dans un référentiel donné avec des paramètres avancés.

Chemin

http://<server>:<port>/scans[?wait=1]

Paramètres

Le paramètre obligatoire `wait` définit le type de session d'analyse.

Si le paramètre possède la valeur `1`, alors l'analyse synchronisée a lieu et l'application envoie un rapport à la fin de l'analyse.

Si le paramètre possède la valeur `0`, l'analyse réalisée est de type asynchrone et la réponse prend la forme suivante :

```
{

  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",
```

```
  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"

}
```

où :

- id représente l'identificateur unique de la session d'analyse ;
- location représente le chemin pour la requête d'information au sujet de cette section sous la forme http://<server>:<port>/scans/<location>.

En-têtes de requête

La requête peut contenir les en-têtes suivantes :

- Content-Type

  Définit le type d'objet soumis à l'analyse.

  Valeurs acceptées :

  - application/octet-stream : un fichier ;
  - multipart/form-data : plusieurs fichiers ;
  - text/plain : une ou plusieurs images Docker dans un référentiel donné ;
  - application/json : une ou plusieurs images Docker dans un référentiel donné avec des paramètres avancés.

- x-api-key (facultatif)

  Clé API définie dans la variable d'environnement KRAS4D_XAPIKEY ou la variable xapikey du fichier de configuration.

Erreurs possibles

Si l'en-tête Content-Type contient une valeur qui n'est pas prise en charge, l'application renvoie une erreur comme suit :

```
{

  "error"={

"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"

  },

  "status"="error"

}
```

Requête d'analyse d'un fichier

Content-Type

application/octet-stream

Corps de la requête

Fichier.

Exemple de réponse :


```
{
  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",
  "created": "Mon, 01 Mar 2021 06:54:38 GMT",
  "progress": 100,
  "scan_result": {
"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
```

```
}
```

Requête d'analyse de plusieurs fichiers

Content-Type

multipart/form-data

Corps de la requête

Plusieurs fichiers.

Exemple de réponse :

```
{
  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",
  "created": "Mon, 01 Mar 2021 06:55:43 GMT",
  "progress": 100,
  "scan_result": {
"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
```

```
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```


Requête d'analyse d'images Docker

Content-Type

text/plain

Corps de la requête

Lien vers la ou les images Docker à analyser.

Vous avez le choix entre :

- Chemin du référentiel vers une image unique (par exemple, https://index.docker.io/jerbi/eicar:latest).
- Masque de chemin correspondant à plusieurs images (par exemple, https://index.docker.io/<name mask>:<tag mask>). Les caractères ? et * peuvent être utilisés pour spécifier le masque.

Exemple de réponse :


```
{

  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",

  "created": "Sun, 31 Jan 2021 10:29:20 GMT",

  "progress": 100,

  "scan_result": {

"jerbi/eicar:latest": {
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}

  },

  "status": "completed",

  "verdicts": [

"infected"

  ]

}
```


Erreurs possibles

Pour obtenir la liste des images selon un masque, il faut utiliser une requête avec l'API REST Docker.

Toutefois, cette option est interdite sur de nombreux serveurs publics pour motif de sécurité. Une tentative d'analyse d'images selon un masque sur de tels serveurs se soldera par un échec.

Exemple d'erreur :


```
{

  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",

  "created": "Mon, 01 Mar 2021 07:02:22 GMT",

  "scan_errors": [

{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
},
[
"Unauthorized"
]
  ],

  "status": "completed"

}
```


Requête d'analyse d'images Docker avec des paramètres avancés

Content-Type

application/json

Corps de la requête

JSON du type suivant :

```
{
  "source": "https://index.docker.io/jerbi/eicar:latest",
  "params": {
"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
}
},
"on_complete": {
"body": {
"session_id": "100",
},
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }
}
```

Paramètres avancés de la requête

La section `params` peut contenir les paramètres suivants :

- `destination` (facultatif) : serveur sur lequel il faut copier l'image analysée.
- `skipimageifexists` (facultatif) : ne pas analyser et ne pas copier les images si le serveur de réception possède déjà une image portant le même nom et le même hash SHA256. Ce paramètre doit être utilisé uniquement en présence du paramètre `destination`.
- `custom_callbacks` (facultatif) : décrit les requêtes à envoyer après la fin de l'analyse :
  - on_detect : requête envoyée en cas de détection d'une menace.
  - on_complete : requête envoyée à chaque fois qu'une analyse est terminée.

La description du corps de la requête peut contenir une variable `$infected` qui sera remplacée par une liste d'objets infectés.

Exemple de réponse :


```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
}
  ],
  "scan_params": {
"destination": "https://fake",
"skipimageifexists": true
  },
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
```

```
  "verdicts": [

"infected"

  ]

}
```

Requête d'obtention d'informations sur les sessions d'analyse (GET)

Fonction

Obtenir des informations sur les sessions d'analyse.

Chemin

http://<server>:<port>/scans[?force] : requête d'obtention de la liste de sessions

http://<server>:<port>/scans/<identificateur unique de session d'analyse>[?force] : requête d'obtention d'informations sur une session en particulier

Paramètres

Le conteneur KESL conserve les données relatives aux sessions d'analyse en mémoire, avec écriture dans la base de données des résultats d'analyse.

Le paramètre facultatif `?force` lance la lecture des informations de la base de données quand plusieurs exemplaires de conteneur KESL utilisent la même base de données. En cas d'absence du paramètre, les informations fournies concerneront uniquement les sessions initialisées par un exemplaire concret du conteneur KESL.

Requête d'obtention de la liste des sessions d'analyse

Chemin

http://<server>:<port>/scans[?force]

Exemple de réponse :

```
{

  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {

"progress": 100,
"status": "completed"
```

```
  },

  "655b96fc-34ca-4915-9c41-d52724a277de": {

"progress": 100,
"status": "completed"

  },

  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {

"progress": 100,
"status": "completed"

  },

  "c32ca88f-2d24-47ec-b040-0540366bea4b": {

"progress": 100,
"status": "completed"

  },

  "df11ad81-26aa-42f9-94bb-39dee4304807": {

"progress": 0,
"status": "completed"

  },

  "fa25340f-4898-497f-ab59-8df494f4ea47": {

"progress": 100,
"status": "completed"

  }

}
```

Requête d'obtention des informations sur une session concrète

Chemin

http://<server>:<port>/scans/<ID unique de session d'analyse>[?force]

Exemple de réponse :

```
{
  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",
  "created": "Mon, 01 Mar 2021 06:45:19 GMT",
  "progress": 100,
  "scan_result": {
"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
}
```


Requête d'ajout d'un certificat de registre (POST)

Fonction

Ajout d'un certificat de registre sans redémarrage du conteneur KESL.

Chemin

http://<server>:<port>/addcert

En-têtes de requête

La requête contient l'en-tête Content-Type.

Valeurs acceptées :

- application/octet-stream : un fichier de certificat ;
- multipart/form-data :plusieurs fichiers de certificats.

Demande d'information sur l'état du conteneur KESL (GET)

Fonction

Obtenir des informations sur l'état actuel du conteneur KESL et des paramètres d'état de l'application qui affectent l'état du conteneur KESL (l'état de l'application, de la licence et des bases de données).

Chemin

http://<server>:<port>/status

Exemple de réponse :

```
{'product info': {'databases_date': '< date de sortie des bases de données >',
'databases_loaded': True, 'license_expiration': '< date d'expiration de la licence >',
'license_info': 'The key is valid', 'policy': 'Not applied', 'version': '< version de
l'application >'}, 'status': 'service available'}
```

Erreurs possibles

Exemple d'erreur (l'application ne s'exécute pas dans le conteneur KESL) :

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
```

Un exemple d'erreur (les bases de données de l'application n'ont pas été téléchargées) :

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '< date d'expiration de la licence >', 'license_info':
'Inconsistent update', 'policy': 'Not applied', 'version': '< version de
l'application >'}, 'status': 'service not available', 'status_reason': ['Databases not
loaded', 'License error: Inconsistent update']}
```

Un exemple d'erreur (la date d'expiration de la licence a expiré) :

```
{'product info': {'databases_date': '<date de sortie de la base de données>',
'databases_loaded': True, 'license_expiration': '< date d'expiration de la licence >',
'license_info': 'Expired', 'policy': 'Not applied', 'version': '<version kesl>'},
'status': 'service not available', 'status_reason': ['License error: Expired']}
```

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 connaissances des Conditions d'accès au Support 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 .

Assistance 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 trace* ou *un fichier dump*.

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 le périphérique et des rapports détaillés sur le fonctionnement des composants 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 composants 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 le périphérique 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 paramètres de fonctionnement 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 périphérique, ainsi qu'une violation de la disponibilité et de l'intégrité des informations traitées.

À propos des fichiers de trace de l'application

Le *fichier de trace* 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 trace de l'application ne sont pas générés. Vous pouvez activer ou désactiver la création des fichiers de trace de l'application et configurer le niveau de détails des fichiers de trace 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 trace de l'application, les fichiers de trace sont conservés par défaut dans le répertoire /var/log/kaspersky/kesl/. Les privilèges root sont requis pour accéder à ce répertoire.

Les fichiers de trace sont stockés sur le périphérique aussi longtemps que l'application est en cours d'utilisation et sont supprimés définitivement lorsque l'application est supprimée. Les fichiers de trace ne sont pas automatiquement envoyés à Kaspersky.

Les fichiers de trace 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 trace de l'application

Les fichiers de trace contiennent les informations générales suivantes :

- Heure de l'évènement.
- Numéro du thread d'exécution.
- Composant de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (pour information, avertissement, événement critique ou erreur).
- Une description de l'événement impliquant l'exécution d'une commande par un composant de l'application et le résultat de l'exécution de cette commande.

Les fichiers de trace peuvent stocker les informations suivantes en plus des données générales :

- États des composants de l'application et de leurs données d'exploitation.
- Données sur l'activité de l'utilisateur dans l'application.
- Données sur le matériel installé sur le périphérique.
- 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 Web, 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.
- 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 configurer les paramètres de traçage de l'application dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, le groupe **Paramètres de traçage et d'enregistrement de vidage**) (cf. le tableau ci-dessous).

Paramètres de traçage de l'application

Paramètre	Description
Chemin d'accès au répertoire contenant les fichiers de trace	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de trace sont stockés. Valeur par défaut : /var/log/kaspersky/kesl. Si vous indiquez un autre répertoire, veillez à ce que le compte sous les autorisations duquel Kaspersky Endpoint Security fonctionne puisse y accéder en lecture et en écriture. L'accès au répertoire de stockage des fichiers de trace défini par défaut requiert les autorisations root.
Nombre maximum de fichiers de trace	Champ de saisie pour le nombre maximum de fichiers de trace de l'application. Valeur par défaut : 10.
Taille maximale du fichier de trace (Mo)	Champ de saisie pour la taille maximale du fichier de trace de l'application (en mégaoctets). Valeur par défaut : 500.

Vous devez redémarrer l'application pour appliquer les paramètres de trace.

Configuration des paramètres de traçage dans la Console d'administration

Dans la Console d'administration, vous pouvez configurer les paramètres de traçage de l'application dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**).

Dans le groupe **Paramètres de traçage et d'enregistrement de vidage**, 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 trace	Champ de saisie pour le chemin d'accès au répertoire dans lequel les fichiers de trace sont stockés. Valeur par défaut : /var/log/kaspersky/kesl.

	Si vous indiquez un autre répertoire, veillez à ce que le compte sous les autorisations duquel Kaspersky Endpoint Security fonctionne puisse y accéder en lecture et en écriture. L'accès au répertoire de stockage des fichiers de trace défini par défaut requiert les autorisations root.
Taille maximale du fichier de trace (Mo)	Champ de saisie pour la taille maximale du fichier de trace de l'application (en mégaoctets). Valeur par défaut : 500.
Nombre maximum de fichiers de trace	Champ de saisie pour le nombre maximum de fichiers de trace de l'application. Valeur par défaut : 10.

Vous devez redémarrer l'application pour appliquer les paramètres de trace.

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 traces de l'application et de préciser le niveau de détail dans les fichiers de trace. Le paramètre peut prendre les valeurs suivantes :

- `Detailed` : crée un fichier de trace détaillé.
- `MediumDetailed` : crée un fichier de trace contenant des messages d'information et d'erreur.
- `NotDetailed` : crée un fichier de trace contenant des notifications relatives aux erreurs.
- `None` (valeur par défaut) : ne crée pas de fichier de trace.

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, veillez à ce que le compte sous les autorisations duquel Kaspersky Endpoint Security fonctionne puisse y accéder en lecture et en écriture. L'accès au répertoire de stockage des fichiers de trace défini par défaut requiert les autorisations root.

`TraceMaxFileCount` : vous permet de spécifier le nombre maximum de fichiers de trace d'application. Le paramètre peut prendre des valeurs de 1 à 10 000. Valeur par défaut : 10.

`TraceMaxFileSize` vous permet de spécifier la taille maximale du fichier de trace 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 trace 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 trace 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'identifiant 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 trace, 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 trace du plug-in Web 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 trace du plug-in Web.

Les fichiers de trace du plug-in Web 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 trace du plug-in Web 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 trace contiennent les informations générales suivantes :

- Heure de l'évènement.
- Numéro du thread d'exécution.
- Composant de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (pour information, avertissement, événement critique ou erreur).
- Une description de l'événement impliquant l'exécution d'une commande par un composant de l'application et le résultat de l'exécution de cette commande.

En plus des données générales, les fichiers de trace 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 dump

Un *fichier dump* contient toutes les informations sur la mémoire de travail des processus de l'application Kaspersky Endpoint Security au moment de la création du fichier dump. Par défaut, aucun fichier de vidage n'est créé. Vous pouvez activer ou désactiver l'enregistrement du dump lorsqu'une application plante.

Si vous avez activé l'enregistrement du dump, par défaut les fichiers de dump sont stockés dans les répertoires /var/opt/kaspersky/kesl/common/dumps et /var/opt/kaspersky/kesl/common/dumps-user.

L'accès aux fichiers dump requiert les privilèges root.

Les fichiers dump sont stockés sur le périphérique aussi longtemps que l'application est en cours d'utilisation et sont supprimés définitivement lorsque l'application est supprimée. Les fichiers dump ne sont pas automatiquement envoyés à Kaspersky.

Les fichiers dump peuvent contenir des données personnelles. Il est conseillé de protéger les informations contre l'accès non autorisé avant leur transfert à Kaspersky.

Activation ou désactivation de l'enregistrement des dumps

Si vous gérez l'application Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez activer ou désactiver l'enregistrement du dump dans les paramètres de la stratégie de Kaspersky Endpoint Security à l'aide de Web Console ou à l'aide 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 dump personnalisés peuvent ne pas être créés. Assurez-vous que la valeur du paramètre sysctl est `kernel.yama.ptrace_scope=0`.

Activation ou désactivation de l'enregistrement de dump dans Web Console

Dans Web Console, vous pouvez activer ou désactiver l'enregistrement de vidage dans les propriétés de la stratégie (**Paramètres de l'application** → **Paramètres généraux** → **Paramètres de l'application**, le groupe **Paramètres de traçage et d'enregistrement de vidage**).

Paramètres d'enregistrement de vidage

Paramètre	Description
Créer un fichier de vidage	La case active ou désactive la création d'un fichier de vidage lorsque

en cas de plantage de l'application	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 de vidage.

Activation et désactivation de l'enregistrement de dump dans la Console d'administration

Dans la Console d'administration, vous pouvez activer ou désactiver l'enregistrement du dump dans les propriétés de la stratégie (**Paramètres généraux** → **Paramètres de l'application**).

Dans le groupe **Paramètres de traçage et d'enregistrement de vidage**, cliquer sur le lien **Configurer** pour ouvrir la fenêtre dans laquelle vous pouvez configurer les paramètres d'enregistrement de vidage.

Paramètres d'enregistrement de vidage

Paramètre	Description
Créer un fichier de vidage 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 de vidage.

Activation et désactivation de l'enregistrement du dump dans la ligne de commande

Pour activer ou désactiver l'enregistrement de dump 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 de dump lorsque l'application plante.
   - `CoreDumps=no` : désactiver l'enregistrement du dump.
4. Si vous souhaitez modifier le répertoire par défaut dans lequel les fichiers du dump sont enregistrés, spécifiez le chemin d'accès au répertoire dans le paramètre `CoreDumpsPath`.
5. Lancez Kaspersky Endpoint Security.

À propos du diagnostic à distance des appareils 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 trace ;
- télécharger des fichiers de trace ;
- 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 périphériques administrés s'affiche.

2. Sélectionnez l'appareil pour lequel vous souhaitez effectuer des diagnostics à distance et cliquez sur le nom de l'appareil.

   La fenêtre des propriétés de l'appareil s'ouvrira.

3. Sous l'onglet **Additionnel**, 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 trace**, cliquez sur le lien **Journaux d'installation à distance**.

   La fenêtre **Journaux d'événements de trace 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.

Analyse de la connexion manuelle au Serveur d'administration. Utilitaire klnagchk

Le kit de distribution de l'Agent d'administration comprend l'utilitaire klnagchk destiné à analyser la connexion au Serveur d'administration.

Après l'installation de l'Agent d'administration, l'utilitaire est placé dans le répertoire /opt/kaspersky/klnagent/bin sur les systèmes d'exploitation 32 bits et /opt/kaspersky/klnagent64/bin sur les systèmes d'exploitation 64 bits. En fonction des arguments utilisés, l'Agent d'administration exécute les actions suivantes au démarrage :

- Écrit dans le fichier journal des événements ou affiche à l'écran les valeurs des paramètres de connexion de l'Agent d'administration installé sur l'appareil client au Serveur d'administration ;
- Écrit dans le fichier journal des événements ou affiche à l'écran les statistiques de l'Agent d'administration (depuis son dernier lancement) et les résultats de l'exécution de l'utilitaire ;
- Essaie d'établir une connexion entre l'Agent d'administration et le Serveur d'administration ;
- Si la connexion échoue, il envoie un paquet ICMP pour vérifier l'état du périphérique sur lequel est installé le Serveur d'administration.

Syntaxe de l'utilitaire

```
klnagchk [-logfile <nom du fichier>] [-sp] [-savecert <chemin d'accès u fichier du certificat>] [-restart]
```

Description des clés

- `-logfile <nom du fichier>` : consigne les valeurs des paramètres de connexion de l'Agent d'administration au Serveur d'administration et les résultats de l'exécution de l'utilitaire dans le fichier journal des événements. Si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur s'affichent à l'écran.
- `-sp` : affiche le mot de passe d'authentification de l'utilisateur sur le serveur proxy. Le paramètre est utilisé si la connexion au Serveur d'administration est établie via un serveur proxy.
- `-savecert <nom du fichier>` : enregistre le certificat d'authentification de l'accès au Serveur d'administration dans le fichier indiqué.
- `-restart` : relance l'Agent d'administration.

Connexion manuelle au Serveur d'administration. Utilitaire klmover

Le kit de distribution de l'Agent d'administration comprend l'utilitaire klmover destiné à administrer la connexion au Serveur d'administration.

Après l'installation de l'Agent d'administration, l'utilitaire est placé dans le répertoire /opt/kaspersky/klnagent/bin sur les systèmes d'exploitation 32 bits et /opt/kaspersky/klnagent64/bin sur les systèmes d'exploitation 64 bits. En fonction des arguments utilisés, l'Agent d'administration exécute les actions suivantes au démarrage :

- Connecte l'Agent d'administration au Serveur d'administration en utilisant les paramètres indiqués.
- Écrit dans le fichier journal des événements ou affiche à l'écran les résultats d'une opération.

Syntaxe de l'utilitaire

```
klmover [-logfile <nom du fichier>] {-address <adresse du serveur>} [-pn <numéro de port>] [-ps <numéro de port SSL>] [-nossl] [-cert <chemin d'accès au fichier du certificat>] [-silent] [-dupfix]
```

Description des clés

- `-logfile <nom du fichier>` : enregistre les résultats de l'exécution de l'utilitaire dans le fichier indiqué. Si la clé n'est pas utilisée, les résultats et les messages d'erreur sont affichés dans stdout.
- `-address <adresse du serveur>` : adresse du Serveur d'administration pour la connexion. L'adresse indiquée peut être l'adresse IP, NetBIOS ou le nom DNS du périphérique.
- `-pn <numéro de port>` : numéro du port qui servira à la connexion non chiffrée au Serveur d'administration. Par défaut, le port 14000 est utilisé.
- `-ps <numéro de port SSL>` : numéro du port SSL qui servira à la connexion chiffrée au Serveur d'administration via le protocole SSL. Par défaut, le port 13000 est utilisé.

- `-nossl` : se connecte au serveur d'administration via une connexion non chiffrée. Si la clé n'est pas indiquée, la connexion de l'Agent au Serveur d'administration est établie via le protocole chiffré SSL.

- `-cert <chemin d'accès au fichier du certificat>` : utilise le fichier indiqué du certificat pour l'authentification de l'accès à un nouveau Serveur d'administration. Si la clé n'est pas utilisée, l'Agent d'administration obtient un certificat à la première connexion au Serveur d'administration.

- `-silent` : démarre l'utilitaire en mode non interactif. L'utilisation de la clé peut être utile, par exemple, lors du lancement de l'utilitaire à partir d'un script de lancement lors de l'inscription de l'utilisateur.

- `-dupfix` : ce fichier clé est utilisé si l'installation de l'Agent d'administration a été exécutée de manière inhabituelle, non pas à l'aide du kit de distribution, mais, par exemple, par restauration à partir d'une image de disque.

- `-cloningmode 1` : active le mode de clonage.

- `-cloningmode 0` : désactive le mode de clonage.

Appendices

Cette section contient des renseignements qui viennent compléter le contenu principal de l'aide.

Appendice 1. Optimisation de l'utilisation des ressources

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

Pour consulter la consommation des ressources de 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 le fonctionnement de Kaspersky Endpoint Security pendant l'analyse des objets ralentit considérablement le système, il convient de configurer l'application pour optimiser l'utilisation des ressources du système.

Détermination de la tâche qui utilise les ressources

Pour identifier la ou les tâches de l'application qui utilisent les ressources du système, il faut faire la distinction entre l'utilisation des ressources des tâches Protection contre les menaces sur les fichiers (type OAS) et les tâches d'analyse à la demande (types ODS et ContainerScan).

Si l'application est administrée par une stratégie de Kaspersky Security Center, il faut autoriser l'administration des tâches locales lors de l'étude.

Analyse du fonctionnement de la tâche Protection contre les menaces sur les fichiers

Pour analyser le fonctionnement de la tâche Protection contre les menaces sur les fichiers :

1. Arrêtez toutes les tâches d'analyse et de surveillance.
2. Confirmez que des tâches d'analyse à la demande ne seront pas lancées pendant la vérification ou qu'aucune tâche n'est planifiée. Vous pouvez réaliser cette opération via Kaspersky Security Center ou localement en

procédant comme suit :

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

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

b. Pour obtenir les paramètres de planification d'une tâche d'analyse des logiciels malveillants, exécutez la commande suivante :

```
kesl-control --get-schedule <ID de ma tâche>
```

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

c. Pour obtenir les paramètres de planification de toutes vos tâches d'analyse des logiciels malveillants, le cas échéant, et indiquer leur lancement manuel, procédez comme suit :

```
kesl-control --set-schedule <ID de ma tâche> RuleType=Manual
```

3. Pour activer la création d'un fichier de trace 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 menaces sur les fichiers, 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.

Quand elle est soumise à une charge, l'application enregistrer beaucoup d'information dans les fichiers de travail. Par défaut, le système conserver 5 fichiers de 500 Mo chacun. Pour cette raison, les informations les plus anciennes sont supprimées. Si les problèmes de performance et d'utilisation des ressources ne se manifestent plus, cela signifie qu'ils sont probablement dû à la tâche d'analyse à la demande. Vous pouvez alors analyser le fonctionnement des tâches d'analyse de type ContainerScan et ODS.

6. Pour désactiver la création de fichiers de trace de l'application, exécutez la commande suivante :

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

7. Pour créer 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.

8. Déterminez si les objets qui ont été analysé le plus souvent sont dangereux. En cas de difficultés, contactez le Support Technique.

Par exemple, vous pouvez décider que des répertoires et des fichiers journaux ne présentent aucun danger s'ils contiennent un processus de confiance ou des fichiers de base de données.

9. Prenez note du chemin d'accès aux objets qui d'après vous ne posent aucun danger. Vous en aurez besoin par la suite pour configurer les exclusions de l'analyse.

10. Si divers services enregistrent souvent des fichiers, ces fichiers seront à nouveau analysés dans la fille d'attente. Pour créer 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 $9}' | sort | uniq -c | sort -k1 -n -r
```

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

11. Si le compteur pour un fichier atteint une valeur de plusieurs milliers en quelques heures, décidez si vous pouvez faire confiance à ce fichier afin de l'exclure de l'analyse.

    La logique d'identification est identique à celle décrite pour l'analyse antérieure (cf. Point 8) : les fichiers journaux peuvent être considérés comme inoffensifs, car ils ne peuvent être exécutés.

12. Même si certains fichiers sont exclus de la protection permanente, ils peuvent toujours être interceptés par l'application. Si l'exclusion de certains fichiers de la protection permanente n'apporte pas un gain de performance considérable, vous pouvez complètement exclure de l'interception le point de montage où se trouvent ces fichiers. Pour ce faire, procédez comme suit :

    a. Obtenez la liste des fichiers interceptés par l'application en exécutant la commande suivante :

    ```
    grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
    ```

    b. Utilisez la liste résultante pour identifier les chemins où un grand nombre d'interceptions d'opérations de fichiers se produisent, et configurez les exclusions de l'interception.

Analyse du fonctionnement des tâches d'analyse à la demande

Une utilisation importante des ressources peut également être due à l'utilisation de tâches de type ODS et ContainerScan. Respectez les recommandations suivantes lors de l'utilisation de tâches de type ODS :

- Assurez-vous que plusieurs tâches d'analyse à la demande ne vont pas être lancées simultanément. L'application accepte ce mode de fonctionnement, mais il peut augmenter fortement l'utilisation des ressources. Vérifiez la planification de toutes les tâches de type ODS et ContainerScan localement (comme dans la description pour la tâche Protection contre les menaces sur les fichiers) ou via Kaspersky Security Center.
- Lancez l'analyse quand le serveur est soumis à la charge la moins importante.
- Confirmez que le chemin indiqué pour l'analyse ne pointe pas vers des ressources distantes montées (SMB / NFS). Si la tâche consiste à analyser une ressource distante et qu'il n'est pas possible de l'exécuter directement sur le serveur proposant la ressource, évitez de lancer l'analyse sur des serveurs hébergeant des services critiques, car une tâche de ce genre peut durer très longtemps (en fonction de la vitesse de connexion et de la quantité de fichiers).
- Optimisez les paramètres de la tâche d'analyse avant son lancement.

Configuration de la tâche Protection contre les menaces sur les fichiers

Après avoir analysé le fonctionnement de la tâche Protection contre les menaces sur les fichiers, vous avez composé la liste des répertoires et des fichiers qui peuvent être exclus de l'analyse. Il reste alors à les ajouter aux exclusions.

Exclusions d'analyse

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
```

Exclusions de l'interception

Si vous souhaitez exclure les fichiers d'un répertoire particulier non seulement de l'analyse, mais également de l'interception, vous pouvez exclure le point de montage dans son ensemble.

Pour exclure l'intégralité du point de montage :

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, saisissez 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).

Il est également conseillé d'exclure un point de montage s'il s'agit d'une ressource distante avec une connexion instable ou lente.

Modification du type d'analyse

Par défaut, la tâche de protection contre les menaces sur les fichiers peut analyser les fichiers à l'ouverture ou à la fermeture. S'il s'avère, lors de l'analyse du fonctionnement de la tâche Protection contre les menaces sur les fichiers, que trop de fichiers écrits ont été identifiés, vous pouvez faire passer la tâche au mode de fonctionnement opérationnel uniquement lors de l'ouverture du fichier en saisissant la commande suivante :

```
kesl-control --set-set 1 ScanByAccessType=Open
```

Dans ce mode de fonctionnement, les modifications introduites dans le fichier après l'ouverture ne seront pas analysées avant la prochaine consultation du fichier.

Configuration de la tâche d'analyse à la demande

Exclusions d'analyse

Pour les tâches d'analyse à la demande avec les types ODS et ContainerScan, vous pouvez configurer des exclusions d'analyse. La configuration est similaire à la configuration des exclusions de l'analyse pour la tâche Protection contre les menaces sur les fichiers .

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 exceptions.

Restriction de l'utilisation de la mémoire pour le décompactage des archives

La tâche d'analyse à la demande lors d'une analyse récursive décompacte les archives pendant l'analyse en utilisant la mémoire vive. Par défaut, l'application a accès à 40 % de toute la mémoire vive disponible, mais jamais inférieure à 2 Go. Pour cette raison, si le système possède plus de 5 Go de mémoire vive, il est possible de limiter l'utilisation de la mémoire manuellement. Ceci convient particulièrement aux serveurs qui disposent de centaines de giga-octets de mémoire vive.

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'exécution des tâches d'analyse de type OAS, ODS et ContainerScan.

Par défaut, l'application n'utilise pas plus de 40 % de toute la mémoire vive disponible. Pour les systèmes dotés de grandes quantités de la mémoire vive (plus de 5 Go), limiter l'utilisation de la mémoire peut être utile.

Vous pouvez réguler la quantité de la mémoire vive utilisée par l'application lors de l'analyse des fichiers à l'aide du paramètre `ScanMemoryLimit` dans le fichier de configuration kesl.ini. La valeur du paramètre par défaut est 8192 Mo.

Le paramètre limite uniquement la quantité de mémoire utilisée lors de l'analyse des fichiers, autrement dit, la quantité totale de mémoire consommée par l'application peut être supérieure à la valeur spécifiée par ce paramètre.

Pour spécifier la restriction d'utilisation de la mémoire lors de l'analyse des fichiers :

1. Démarrez Kaspersky Endpoint Security.
2. Ouvrez le fichier /var/opt/kaspersky/kesl/common/kesl.ini pour le modifier.
3. Dans la section **[General]** : spécifiez la quantité de la mémoire vive requise dans la valeur du paramètre `ScanMemoryLimit` :

   `ScanMemoryLimit=< quantité de mémoire en mégaoctets >`

   La valeur minimale est de 2048 Mo. Si vous spécifiez une valeur inférieure à 2 048 Mo, l'application utilisera la valeur minimale.

   Si vous spécifiez une valeur supérieure à la taille de la mémoire vive du système, l'application utilisera jusqu'à 40 % de toute la mémoire vive disponible.
4. Lancez Kaspersky Endpoint Security.

La restriction d'utilisation de la mémoire lors de l'analyse des fichiers change après le redémarrage de l'application.

Appendice 2. 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 pour gérer les paramètres généraux d'analyse du conteneur.
- -D : commandes de gestion par le contrôle des appareils.
- -E : commandes pour gérer les événements de l'application.
- -F : commandes de gestion du pare-feu.
- -H : commandes de contrôle pour les appareils bloqués.
- -L – commandes de gestion des clés de licence.
- -N : commandes pour gérer les paramètres d'analyse des connexions chiffrées.
- -R – commandes permettant de gérer les paramètres d'intégration de l'application Kaspersky Endpoint Security avec Kaspersky Endpoint Detection and Response (KATA) et avec 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 d'affichage des événements.

Commandes de gestion des paramètres et des tâches de l'application

-T : préfixe qui indique que la commande appartient au groupe de commandes de gestion des paramètres et des tâches de l'application.

-C : préfixe qui indique que la commande appartient au groupe de commandes de gestion des paramètres généraux de l'analyse du conteneur.

-N : préfixe qui indique que la commande appartient au groupe des commandes de gestion des paramètres d'analyse des connexions chiffrées.

Commande kesl-control --export-settings

La commande vous permet d'afficher tous les paramètres de l'application sur la console ou d'exporter vers un 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] --export-settings [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres de l'application seront enregistrés.

`--json` : afficher 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 chiffrées, 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>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés dans l'application.

`--json` : importer les paramètres 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.

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 être exécutée que si l'application est utilisée en mode standard.

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>` : chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'application seront affichés. 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 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>` est le nom et la valeur de l'un des paramètres généraux de l'application.

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés dans l'application.

`--json` : importer les paramètres d'un fichier de configuration au format JSON dans l'application. 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 <identifiant/nom de la tâche> [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès au fichier de configuration dans lequel les paramètres de la tâche seront affichés. 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 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 <identifiant/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 <identifiant/nom de la tâche> --file <chemin d'accès au fichier de configuration> [--json]
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

`<nom du paramètre>=<valeur du paramètre>` : nom et valeur de l'un des paramètres de la tâche.

`--add-path <chemin d'accès>` : ajouter le chemin d'accès au répertoire contenant les objets en cours d'analyse.

`--del-path <chemin d'accè>` : supprimer le chemin d'accès au répertoire contenant les objets en cours d'analyse.

`--add-exclusion <chemin d'accès>` : ajouter le chemin d'accès au répertoire contenant les objets qu'il faut exclure de l'analyse.

`--del-exclusion <chemin d'accès>` : chemin d'accès au répertoire contenant les objets exclus

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres de la tâche vont être importés.

`--json` : importer les paramètres 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.

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 <identifiant/nom de la tâche> --set-to-default
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <identifiant/nom de la tâche> [--file <chemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès au fichier de configuration dans lequel les paramètres de planification des tâches seront affichés. 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 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 <identifiant/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 <identifiant/nom de la tâche> --file <chemin d'accès au
fichier de configuration> [--json]
```

Arguments et clés

`< identifiant/nom de la tâche >` : identifiant attribué à la tâche au moment de la création, ou le nom de la tâche sur la ligne de commande.

`<nom du paramètre>=<valeur du paramètre>` : nom et valeur de l'un des paramètres de planification des tâches.

`--file <chemin d'accès au fichier de configuration>` : chemin complet vers le fichier de configuration à partir duquel les paramètres de planification des tâches seront importés.

`--json` : importer les paramètres 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.

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 <identifiant/nom de la tâche> [--json]
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <hemin d'accès au fichier de configuration>] [--json]
```

Arguments et clés

`<nom de la tâche>` : le nom que vous spécifiez pour une nouvelle tâche.

`<type de tâche>` : désignation du type de tâche en cours de création.

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès complet au fichier de configuration dont les paramètres seront utilisés lors de la création de la tâche.

`--json` : importer les paramètres 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.

Commande kesl-control --delete-task

La commande permet de supprimer la tâche.

Syntaxe de la commande

```
kesl-control [-T] --delete-task <identifiant/nom de la tâche>
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <identifiant/nom de la tâche> [-W] [--progress]
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <identifiant/nom de la tâche> [-W]
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <identifiant/nom de la tâche>
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 <identifiant/nom de la tâche>
```

Arguments et clés

`<identifiant/nom de la tâche>` : identifiant attribué à la tâche au moment de la 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 d'accès>` : chemin d'accès au fichier ou au répertoire qu'il faut vérifier. Vous pouvez spécifier plusieurs chemins d'accès, séparés par des espaces.

`--action <action>` : action que l'application va 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 pour un conteneur ou une image.

Syntaxe de la commande

```
kesl-control [-T] --scan-container <conteneur/image[:tag]>
```

Arguments et clés

`<conteneur/image[:tag]>` est le nom ou l'identifiant 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/*/fichier ou /dir/*/*/fichier.

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/**/fichier*/ ou /dir/fichier**/.

Le masque ** ne peut être utilisé qu'une seule fois dans un nom de répertoire. Par exemple, /dir/**/**/fichier 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 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> : chemin d'accès au fichier de configuration dans lequel les paramètres généraux de l'analyse du conteneur seront affichés. 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 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>` est le nom et la valeur de l'un des paramètres généraux de l'analyse du conteneur.

`--file <chemin d'accès au fichier de configuration>` : 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 d'un fichier de configuration au format JSON dans l'application. 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 de vérification des connexions chiffrées

-N : préfixe qui indique que la commande appartient au groupe des commandes de gestion des paramètres d'analyse des connexions chiffrées.

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 de vérification des connexions chiffrées 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>` : chemin d'accès au fichier dans lequel les paramètres de l'analyse des connexions chiffrées seront affichés. 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 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 de vérification des connexions chiffrées 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>` est le nom et la valeur de l'un des paramètres d'analyse des connexions chiffrées.

`--file <chemin d'accès au fichier de configuration>` : chemin d'accès au fichier de configuration à partir duquel seront importés les paramètres de vérification des connexions sécurisées.

`--json` : importer les paramètres d'un fichier de configuration au format JSON dans l'application. 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 --add-certificate

La commande permet d'ajouter un certificat à la liste des certificats que l'application considérera comme fiables.

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 souhaitez ajouter, au format PEM ou DER.

Commande kesl-control --remove-certificate

La commande permet de supprimer un certificat de la liste des certificats de confiance.

Syntaxe de la commande

```
kesl-control [-N] --remove-certificate <objet du certificat>
```

Commande kesl-control --list-certificates

La commande permet d'afficher une liste de certificats de confiance.

Syntaxe de la commande

```
kesl-control [-N] --list-certificates
```

Commandes de statistiques

-S : préfixe qui indique que la commande appartient au groupe des commandes des 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 --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 <nom et 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 du filtre>"]
```

Arguments et clés

`<conditions du filtre>` : une ou plusieurs expressions logiques au format `<champ> <opération de comparaison> '<valeur>'` combinées à l'aide de l'opérateur logique `and` pour afficher des événements actuels spécifiques.

Commandes de gestion des événements de l'application

-E : un préfixe indiquant que la commande appartient au groupe de commandes de gestion des événements de l'application.

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 du filtre>" [--db <fichier de base de données>] [-n <nombre>] [--file <nom et chemin d'accès au fichier>] [--json] [--reverse]
```

Arguments et clés

< fichier de base de données > : le chemin complet du fichier de base de données du journal des événements à partir duquel vous souhaitez récupérer 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 du filtre > : 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 > : nombre de derniers événements de la sélection (c'est-à-dire le nombre d'enregistrements à partir de la fin de la sélection) à afficher.

`--file` < nom et chemin d'accès au fichier > est le chemin complet du fichier dans lequel vous souhaitez générer 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

-L : préfixe qui indique que la commande appartient au groupe des commandes de gestion des 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. 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 une clé de licence active de l'application et une clé de licence active EDR Optimum. 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 >` : 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.

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.

À l'aide de cette commande, vous pouvez ajouter à la fois une clé de licence de réserve de l'application et une clé de licence de réserve EDR Optimum. 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 >` : 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.

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]
```

Arguments et clés

`--edr-optimum` : supprimer la clé de licence active EDR Optimum. Si vous ne spécifiez pas la clé `--edr-optimum`, la clé de licence active de l'application Kaspersky Endpoint Security sera supprimée.

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]
```

Arguments et clés

`--edr-optimum` : supprimer la clé de licence de réserve EDR Optimum. Si vous ne spécifiez pas la clé `--edr-optimum`, la clé de licence de réserve de l'application Kaspersky Endpoint Security sera supprimée.

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 charger le fichier de configuration BLOB requis pour l'intégration avec Kaspersky Managed Detection and Response.

Syntaxe de la commande

```
kesl-control [-L] --load-mdr-blob <chemin d'accès au fichier de configuration MDR BLOB>
```

Commande kesl-control --remove-mdr-blob

La commande `--remove-mdr-blob` vous permet de supprimer le fichier de configuration BLOB requis 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

-F : préfixe qui indique que la commande appartient au groupe de commandes de gestion du pare-feu.

Commande kkesl-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 <direction>] [--remote <adresse distante>[:<plage de
ports>]] [--local <adresse locale>[:<plage de ports>]] [--at <index>]
```

Arguments et clés

`--name <nom de la règle>` : nom de la règle de paquet réseau.

`--action <action>` : action à réaliser sur les connexions définies dans cette règle de paquet réseau.

`--protocol <протокол>` : type de protocole de transfert de données pour lequel vous souhaitez surveiller l'activité réseau.

`--direction <direction>` : direction de l'activité réseau surveillée.

`--remote <adresse distante>[:<plage de ports>]` : adresse réseau de l'appareil à distance.

`--local <adresse locale>[:<plage de ports>]` : adresse réseau de l'appareil sur lequel l'application Kaspersky Endpoint Security est installée.

`--at <index>` : numéro de série 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 <index>
```

Arguments et clés

`--name <nom de la règle>` : nom de la règle de paquet réseau.

`--index <index>` : numéro de série 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 <index>

kesl-control [-F] --move-rule --index <index> --at <index>
```

Arguments et clés

`--name <nom de la règle>` : nom de la règle de paquet réseau.

`--index <index>` : numéro de série actuel de la règle dans la liste des règles de paquets réseau.

`--at <index>` : nouveau numéro de série 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>` : nom prédéfini de la zone réseau.

`--address <adresse>` : adresse réseau ou 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 <index de l'adresse>
```

Arguments et clés

`--zone <zone>` : nom prédéfini de la zone réseau.

`--address <adresse>` : adresse réseau ou sous-réseau.

`--index <index de l'adresse>` : numéro de série 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

-H – préfixe indiquant 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 réseaux.

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>` : Adresse IP de l'appareil ou du sous-réseau (IPv4 /IPv6, y compris les adresses abrégées). Vous pouvez spécifier plusieurs adresses IP ou sous-réseaux des appareils, séparés par des espaces.

Commandes de gestion du Contrôle des appareils

-D : préfixe qui indique que la commande appartient au groupe des commandes de gestion du contrôle des appareils.

Commande kesl-control --get-device-list

La commande permet d'afficher sur la console une liste des appareils installés sur l'appareil client ou connectés à celui-ci.

Syntaxe de la commande

```
kesl-control [-D] --get-device-list [--json]
```

Arguments et clés

`--json` : afficher les données au format JSON.

Commandes de gestion du Contrôle des applications

-A : préfixe facultatif qui indique que la commande appartient au groupe des commandes de gestion du contrôle des appareils.

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>` : noms des catégories sur lesquelles vous souhaitez afficher des 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 au format JSON dans lequel les paramètres seront affichés.

`--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>` : 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>` : chemin d'accès complet au fichier de configuration avec les paramètres des catégories.

Commande kesl-control --get-settings

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>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres seront affichés.

`--json` : afficher les données au format JSON.

Commande kesl-control --set-settings

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>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés.

`--json` : importer les données d'un fichier au format JSON.

Commande kesl-control --set-to-default

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

La commande permet d'afficher une liste des paramètres configurés du Contrôle Internet.

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>` : chemin d'accès complet au fichier de configuration dans lequel les paramètres seront affichés.

`--json` : afficher les données au format JSON.

Commande kesl-control --set-settings

La commande permet de modifier la liste des paramètres configurés du Contrôle Internet.

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>` : chemin d'accès complet au fichier de configuration depuis lequel les paramètres vont être importés.

`--json` : importer les données d'un fichier au format JSON.

Commande kesl-control --set-to-default

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

-B : préfixe qui indique que la commande appartient au groupe des commandes d'administration de la sauvegarde.

Commande kesl-control --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 du filtre>"
```

Arguments et clés

`<conditions du filtre>` : 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 du filtre>"] [-n <nombre>] [--json] [--reverse]
```

Arguments et clés

`<conditions du filtre>` : 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.

`<numéro>` : le nombre d'objets récents du stockage qui doivent être affichés. 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.

Commande kesl-control --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 <nom et chemin d'accès au fichier>]
```

Arguments et clés

`<identifiant de l'objet>` : identifiant de l'objet dans la sauvegarde.

où `--file <nom et chemin du fichier>` est le nouveau nom de fichier et le chemin d'accès au répertoire dans lequel il faut 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 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 pour gérer les paramètres d'intégration de Kaspersky Endpoint Detection and Response (KATA)

-R – un préfixe indiquant que la commande appartient au groupe de commandes permettant de gérer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) et avec Kaspersky Endpoint Detection and Response Optimum.

Commande kesl-control --add-kataedr-server-certificate

La commande vous permet d'ajouter ou de remplacer un certificat de serveur KATA précédemment ajouté.

Syntaxe de la commande

```
kesl-control [-R] --add-kataedr-server-certificate <nom et chemin d'accès au fichier>
```

Arguments et clés

`<nom et chemin d'accès au fichier>` : nom et chemin d'accès au fichier contenant le certificat du serveur.

Commande kesl-control --remove-kataedr-server-certificate

La commande permet de supprimer le certificat du serveur KATA.

Syntaxe de la commande

```
kesl-control [-R] --remove-kataedr-server-certificate
```

Commande kesl-control --query-kataedr-server-certificate

La commande vous permet d'afficher des informations sur le certificat du serveur KATA.

Syntaxe de la commande

```
kesl-control [-R] --query-kataedr-server-certificate
```

Commande kesl-control --add-kataedr-client-certificate

La commande vous permet d'ajouter ou de remplacer un certificat client précédemment ajouté utilisé pour sécuriser la connexion au serveur KATA.

Syntaxe de la commande

```
kesl-control [-R] --add-kataedr-client-certificate <nom et chemin d'accès au fichier>
```

Arguments et clés

`<nom et chemin d'accès au fichier>` : est le nom et le chemin d'accès au cryptocontainer (archive au format PFX) contenant le certificat client et la clé privée.

Commande kesl-control [-R] --remove-kataedr-client-certificate

La commande permet de supprimer le certificat client utilisé pour sécuriser la connexion au serveur KATA.

Syntaxe de la commande

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Commande kesl-control [-R] --query-kataedr-client-certificate

La commande vous permet d'afficher des informations sur le certificat client.

Syntaxe de la commande

```
kesl-control [-R] --query-kataedr-client-certificate
```

Commande kesl-control --isolation-stat

La commande permet d'afficher l'état actuel de l'isolation du 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 pour gérer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response Optimum

-R – un préfixe indiquant que la commande appartient au groupe de commandes permettant de gérer les paramètres d'intégration avec Kaspersky Endpoint Detection and Response (KATA) et avec Kaspersky Endpoint Detection and Response Optimum.

L'activation ou la désactivation de l'intégration avec Kaspersky Endpoint Detection and Response Optimum s'effectue à l'aide du paramètre `UseEdrOptimum` dans les paramètres généraux de l'application.

Commande kesl-control --isolation-stat

La commande permet d'afficher l'état actuel de l'isolation du 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 applicatives en mode Light Agent pour la protection des environnements virtuels

-V – préfixe indiquant que la commande appartient au groupe de commandes de l'application Kaspersky Endpoint Security utilisée en mode Light Agent pour protéger les environnements virtuels (dans le cadre de la solution 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
```

Appendice 3. 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 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 [ ].

- Saisissez les valeurs 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 en suivant les instructions des spécialistes du Support Technique.

Paramètres du fichier de configuration kesl.ini

Paramètre	Description	Valeur
La section **[Général]** contient les paramètres suivants :		
`Locale`	Norme locale utilisée pour localiser les textes envoyés par l'application Kaspersky Endpoint Security à Kaspersky Security Center (événements, notifications, résultats de tâches et autres). La localisation de l'interface utilisateur graphique et le la ligne de commande de l'application dépendent de la localisation renseignée par la variable d'environnement `LANG`. Si la variable d'environnement `LANG` renseigne une localisation qui n'est pas compatible avec l'application Kaspersky Endpoint Security, l'interface utilisateur et la ligne de commande apparaissent en anglais.	Les paramètres régionaux d défini par la norme RFC 30 Si le paramètre `Locale` n'e langue du système d'exploit Si l'application ne parvient p version linguistique du syst si la version n'est pas comp l'application, la valeur par de est sélectionnée.
`PackageType`	Format du progiciel installé. La définition de cette option n'affecte pas le fonctionnement de l'application. La valeur du paramètre est renseignée automatiquement lors de la configuration initiale de l'application.	`rpm` : un RPM est installé. `deb` : un paquet DEB est ins
`UseFanotify`	Utilisation de la technologie fanotify.	`true/yes` : le système d'ex

	La définition de cette option n'affecte pas le fonctionnement de l'application. La valeur du paramètre est renseignée automatiquement lors de la configuration initiale de l'application.	charge la technologie fanot `false/no` : le système d'ex pas en charge la technologi
`KsvlaMode`	Mode d'utilisation de l'application Kaspersky Endpoint Security. La définition de cette option n'affecte pas le fonctionnement de l'application. La valeur du paramètre est renseignée automatiquement lors de la configuration initiale de l'application.	`true/yes` : l'application est Light Agent pour protéger virtuels. `false/no` : l'application est standard.
`StartupTraces`	Activation de la création de fichiers de trace au lancement de l'application.	`true/yes` : crée des fichier lancement de l'application. `false/no` (valeur par défa fichiers de trace au lancem
`RevealSensitiveInfoInTraces`	Affichage des informations dans les fichiers de trace qui peuvent contenir des données personnelles (par exemple, des mots de passe).	`true/yes` : afficher des inf contenir des données pers fichiers de trace de l'applica `false/no` (valeur par défa d'informations pouvant cor personnelles dans les fichie
`AsyncTraces`	Activation du traçage asynchrone, dans lequel les informations sont écrites pour tracer les fichiers de manière asynchrone.	`true/yes` : activer le traça `false/no` (par défaut) : ne traçage asynchrone.
`CoreDumps`	Permettre la création d'un fichier dump lorsque l'application plante.	`true/yes` : créer un fichier l'application échoue. `false/no` (valeur par défa fichier dump lorsque l'applic
`CoreDumpsPath`	Chemin d'accès au répertoire où sont stockés les fichiers dump.	Valeur par défaut : /var/opt/kaspersky/kesl/co L'accès au répertoire de sto dump défini par défaut requ root.
`MinFreeDiskSpace`	Quantité minimale de mémoire disque qui restera après l'écriture du fichier dump, en mégaoctets.	Valeur par défaut : 300.
`ScanMemoryLimit`	Restriction d'utilisation de la mémoire par l'application en mégaoctets.	Valeur par défaut : 8192.
`MachineId`	ID unique du périphérique de l'utilisateur.	La valeur du paramètre est automatiquement lors de l'i 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
`MaxInotifyWatches`	Limitation du nombre d'abonnements aux modifications de fichiers et de	Valeur par défaut : 300000

	répertoires (user watches) indiqué dans /proc/sys/fs/inotify/max_user_watches.	
`MaxInotifyInstances`	Limitation du nombre d'abonnements aux modifications de fichiers et de répertoires pour chaque utilisateur.	Valeur par défaut : 2048.
`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 : 50.
`DisableFileAvActions`	Désactivation des fonctions de désinfection et de suppression de fichiers pour les modules de l'application après l'installation. Si les fonctions de désinfection et de suppression de fichiers sont désactivées, si une menace est détectée, l'application ne tente pas de désinfecter ou de supprimer les fichiers dans lesquels une menace est détectée, mais informe uniquement l'utilisateur qu'une menace a été détectée.	`true/yes` : désactiver les f désinfection et de suppres du lancement de l'applicati `false/no` (valeur par défa désactiver les fonctions de suppression de fichiers lors l'application après l'installat
`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 du périphérique. L'application utilisera les DNS publics suivants par ordre d'apparition : • Google Public DNS™ (8.8.8.8). • Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168).	`true/yes` : utiliser le DNS p aux serveurs de Kaspersky. `false/no` (valeur par défa DNS public pour accéder au Kaspersky. Les demandes de l'applic contenir des adresses de l'adresse IP externe de l'u l'application établit une c avec le serveur DNS. Ces nécessaires, par exemple certificat d'une ressourc l'accès via HTTPS. Si l'app serveur DNS public, les rè des données sont régies confidentialité de ce serv empêcher une applicatio serveur DNS public, cont Technique pour obtenir u
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 périphérique que l'application installée, que ce logiciel	La valeur est indiquée sous décimal ou hexadécimal ave Valeur par défaut : 0x100.

	utilise le neuvième bit du masque de paquet TCP et qu'un conflit se produit.	
`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 périphérique 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 décimal ou hexadécimal ave Valeur par défaut : 0x200.
`BypassFwMark`	Étiquette qui marque les paquets créés ou analysés par l'application afin qu'ils ne tombent pas à nouveau dans le programme pour vérification.	La valeur est indiquée sous décimal ou hexadécimal ave Valeur par défaut : 0x400.
`BypassNFlogMark`	Étiquette qui marque les paquets créés ou analysés par l'application afin qu'ils ne soient pas consignés dans le journal de l'utilitaire iptable.	La valeur est indiquée sous décimal ou hexadécimal ave Valeur par défaut : 0x800.
`ProxyRouteTable`	Numéro de table de routage.	Valeur par défaut : 101.
La section **[Virtualization]** contient les paramètres suivants :		
`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. La définition de cette option n'affecte pas le fonctionnement de l'application. La valeur du paramètre est renseignée automatiquement lors de la configuration initiale de l'application.	`true/yes` : la machine virtu comme serveur. `false/no` : la machine virtu 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. La définition de cette option n'affecte pas le fonctionnement de l'application. La valeur du paramètre est renseignée automatiquement lors de la configuration initiale de l'application.	`true/yes` : le mode de pro l'infrastructure VDI est acti `false/no` : le mode de pro l'infrastructure VDI est dés
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 minute
`StartupTimeout`	Le temps maximum d'attente pour démarrer l'application (en minutes) avant le redémarrage du processus kesl.	Valeur par défaut : 3 minute

`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 en réponse à un message PING reçu.	Valeur par défaut : 2000 ms
`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 lancera la procédure d'arrêt du processus kesl.	Valeur par défaut : 2 minute
`ConnectTimeout`	Intervalle de temps maximum entre le moment où le processus kesl est lancé et le moment où l'application établit une connexion avec le serveur Watchdog. Si l'application n'a pas le temps de créer une connexion dans cet intervalle de temps, le serveur Watchdog lancera la procédure d'arrêt du processus kesl.	Valeur par défaut : 3 minute
`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 ms.
`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 minute
`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 d'arrêt du processus kesl.	`off` : l'utilisation de la mém pas limitée. `< valeur >%` : valeur de 1 à de la taille de la mémoire. `< valeur >MB` : valeur en m `lowest/< valeur >%/< va` plus basse entre la valeur e valeur en mégaoctets. `highest/< valeur >%/< v` plus élevée entre la valeur e valeur en mégaoctets. `auto` : jusqu'à 50 % de la m mais pas moins de 2 Go et

		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 d'arrêt du processus kesl.	`off` (valeur par défaut) : l'ut mémoire virtuelle n'est pas < `valeur` >`MB` : valeur en m
`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 d'arrêt du processus kesl.	`off` (valeur par défaut) : la n'est pas limitée. < `valeur` >`%` : valeur de 0 à de la taille de la mémoire. < `valeur` >`MB` : valeur en m `lowest/`< `valeur` >`%/`< `va` plus basse entre la valeur e valeur en mégaoctets. `highest/`< `valeur` >`%/`< `v` plus élevée entre la valeur e valeur en mégaoctets.
`TrackProductCrashes`	Activer la surveillance de la stabilité des applications. Si la surveillance de la stabilité des applications est activée, le serveur Watchdog surveille le nombre d'arrêts anormaux des applications.	`true/yes` : activer la surve des applications. `false/no` (valeur par défa surveillance de la stabilité d
`ProductHealthLogFile`	Chemin d'accès au fichier utilisé pour surveiller la stabilité de l'application.	Valeur par défaut : /var/opt/kaspersky/kesl/pr
`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 se
`WarnAfter_#_crash`	Nombre d'arrêts anormaux de l'application requis pour afficher une notification d'instabilité de l'application.	Valeur par défaut : 10. Si la valeur est 0, la notifica l'application ne s'affiche pa
`WarnRemovingThreshold`	Intervalle de temps (en secondes) après lequel l'état instable de l'application sera effacé.	Valeur par défaut : 86400 s
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 lors du fonctionnement du module Surveillance du conteneur. 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 l'environnement containerd fonctionnement du module conteneur. `false/no` : ne pas activer l l'environnement containerd fonctionnement du module conteneur.

Paramètres des tâches de ligne de commande par défaut

Cette section contient les paramètres par défaut de toutes les ltâches 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

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

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

FirstAction=Recommended

SecondAction=Skip

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

FirstAction=Recommended

SecondAction=Skip

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

FirstAction=Recommended

SecondAction=Skip

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)

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Paramètres par défaut de la tâche de Backup (ID:10)

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

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

[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

FirstAction=Recommended

SecondAction=Skip

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
```

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

CreateGoldenImage=No

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Paramètres par défaut de la tâche KATAEDR (ID:24)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Paramètres par défaut pour la tâche Web_Control (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

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.

Paramètres généraux de l'application

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 répertoire standard du fichier Samba est indiqué par défaut. Valeur par défaut : /etc/samba/s Le relancement de l'application e après la modification de ce para

`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 répertoire standard du fichier NFS est indiqué par défaut. Valeur par défaut : /etc/exports Le relancement de l'application e après la modification de ce para
`TraceLevel`	Activer le traçage des applications et le niveau de détails des fichiers de trace.	`Detailed` : crée un fichier de tra `MediumDetailed` : crée un fichi contenant des messages d'infor `NotDetailed` : crée un fichier d des notifications relatives aux er `None` (valeur par défaut) : ne cré trace.
`TraceFolder`	Répertoire dans lequel se trouvent les fichiers de trace de l'application.	Valeur par défaut : /var/log/kasp Si vous indiquez un autre réperto le compte sous les autorisations Endpoint Security fonctionne pu lecture et en écriture. L'accès au stockage des fichiers de trace d requiert les autorisations root. Le relancement de l'application e après la modification de ce para
`TraceMaxFileCount`	Spécifie le nombre maximal de fichiers de trace d'application.	1 à 10 000 Valeur par défaut : 10. Le relancement de l'application e après la modification de ce para
`TraceMaxFileSize`	Définit la taille maximale d'un fichier de trace de l'application (en mégaoctets).	1 à 1000 Valeur par défaut : 500. Le relancement de l'application e après la modification de ce para
`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 n'est pas disponible sur les systèmes d'exploitation qui utilisent la technologie fanotify.	4096 à 33 554 432 Valeur par défaut : 16384. Après avoir modifié la valeur de relancez la tâche Protection cor sur les fichiers.
`DetectOtherObjects`	Activer la détection des applications légitimes que les intrus peuvent utiliser pour endommager les appareils ou les données.	`Yes` : activer la détection des ap que les intrus peuvent utiliser pc appareils ou les données.

		`No` (valeur par défaut) : désactiv applications légitimes que les int pour endommager les appareils
`NamespaceMonitoring`	Activation de l'analyse des espaces de noms et 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) : active l espaces de noms et des conten `No` : désactive la surveillance des 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 menaces sur les fichiers et Contrôle des appareils.	`Yes` (valeur par défaut) : bloquer pendant l'analyse. `No` : ne pas bloquer l'accès aux f l'analyse. L'accès à n'importe que autorisé, la vérification est effec asynchrone. Ce mode d'intercep sur les fichiers a moins d'impact performances du système pend fonctionnement, mais il existe ur menace dans un fichier ne soit p supprimée si, lors de l'analyse, ce exemple, changer de nom avant prenne une décision sur l'état de
`UseKSN`	Activation de l'utilisation de Kaspersky Security Network.	`Basic` : activer l'utilisation de Ka Network en mode standard. `Extended` : activer l'utilisation d Security Network en mode avan `No` (valeur par défaut) : désactiv Kaspersky Security Network.
`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 fonctio lequel Kaspersky Endpoint Secu version allégée des bases de do malveillants. `No` (valeur par défaut) – utilisez de la base de données des logic Le mode Cloud est automatiq désactivé si l'utilisation de KS
`UseMDR`	Activation du module	`Yes` : activer le module Managec

	Managed Detection and Response pour l'intégration avec Kaspersky Managed Detection and Response.	Response. `No` (valeur par défaut) : désactiv Managed Detection and Respon
`UseProxy`	Activation de l'utilisation d'un serveur proxy par les modules de l'application Kaspersky Endpoint Security. Un serveur proxy peut être utilisé pour interagir avec Kaspersky Security Network, avec Kaspersky Endpoint Detection and Response (KATA) pour activer l'application et lors de la mise à jour des bases de données et des modules de l'application. Si Kaspersky Endpoint Security est utilisé en mode Light Agent pour protéger les environnements virtuels, l'utilisation d'un serveur proxy pour se connecter à Kaspersky Security Network, SVM et Serveur d'intégration n'est pas prise en charge.	`Yes` : active l'utilisation d'un serv `No` (valeur par défaut) : désactiv serveur proxy. Si `Yes` est sélectionné, l'intégrat Endpoint Detection and Respon effectuée via un serveur proxy.
`ProxyServer`	Paramètres du serveur proxy au format `[<utilisateur>[:<mot de passe>]@]<adresse du serveur proxy a>[:<port>]`. Pour se connecter via un proxy HTTP, il est recommandé d'utiliser un compte utilisateur séparé qui n'est pas utilisé pour l'authentification dans d'autres systèmes. Le proxy HTTP utilise une connexion non sécurisée et le compte utilisateur peut être compromis.	—
`MaxEventsNumber`	Quantité maximale d'événements qui sera enregistrée dans l'application. Quand la quantité maximale d'événements définie est atteinte, l'application supprime	Valeur par défaut : 500 000. Si la valeur attribuée est 0, les év pas conservés.

	les événements les plus anciens.	
`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 4 294 967 295 Valeur par défaut : 0. Si la valeur 0 est attribuée, l'utilis ne peut pas exécuter de tâches personnalisée. Si vous avez installé le paquet d' graphique lors de l'installation de paramètre `LimitNumberOfScar` par défaut la valeur `5`.
`UseSyslog`	Activation de l'enregistrement des informations relatives aux événements dans syslog. L'accès à syslog requiert les privilèges root.	`Yes` : active l'enregistrement des relatives aux événements dans s `No` (valeur par défaut) : désactiv des informations relatives aux év syslog.
`EventsStoragePath`	Répertoire de la base de données dans lequel l'application enregistre les informations relatives aux événements. L'accès à la base de données des événements par défaut requiert les privilèges root.	Valeur par défaut : /var/opt/kaspersky/kesl/private
`ExcludedMountPoint.item_#`	Point de montage que vous souhaitez exclure de la zone d'analyse. L'exclusion est appliquée dans le fonctionnement des modules Protection contre les menaces sur les fichiers, Protection contre le chiffrement, Surveillance du conteneur et dans la tâche Analyse des lecteurs amovibles, et est également configurée dans le fonctionnement des tâches d'analyse (types 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 opérations de fichiers tous les re montés sur le périphérique via le et NFS. `Mounted:NFS` : exclut de l'interc opérations de fichiers tous les re montés sur le périphérique via le `Mounted:SMB` : exclut de l'interc opérations de fichiers tous les re montés sur l'ordinateur via le pro `Mounted:<type de système` exclut de l'interception des opér tous les répertoires montés avec système de fichiers indiqué. `/Mnt` : exclut de l'interception le point de montage /mnt (y comp répertoires) utilisé comme point temporaire pour les disques amo `<chemin qui contient le masque /mnt/user* ou /mnt/**/user_share>` : exclut les objets qui se trouvent dans le montage dont le nom contient le

		Vous pouvez utiliser le caractè pour former un masque de no de répertoire. Vous pouvez saisir le caractèr ensemble de caractères (y co ensemble vide) quelconque de caractère `/` dans le nom du fi répertoire. Par exemple, `/dir/ /dir/*/*/fichier`. Vous pouvez saisir deux carac consécutifs pour remplacer n ensemble de caractères (y co ensemble vide) dans le nom du répertoire, y compris le caract exemple, `/dir/**/fichier*` `/dir/fichier**/`. Le masque `**` ne peut être ut fois dans un nom de répertoir `/dir/**/**/fichier` est ur incorrect. Pour exclure le point de monta devez indiquer exactement `/d` astérisques). Le masque `/dir/*` exclut tou montage d'un niveau inférieur mais pas le point de montage Le masque `/dir/**` exclut to montage à n'importe quel nive sous `/dir`, mais pas le point d lui-même. Vous pouvez utiliser le symbol n'importe quel caractère uniqu de fichier ou de répertoire.
`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 a` exclut de l'analyse le processus d local spécifié. Vous pouvez utilis pour spécifier le chemin.

		Vous pouvez utiliser le caractè pour former un masque de no de répertoire. Vous pouvez saisir le caractèr ensemble de caractères (y co ensemble vide) quelconque de caractère `/` dans le nom du fi répertoire. Par exemple, `/dir` `/dir/*/*/fichier`. Vous pouvez saisir deux carac consécutifs pour remplacer n ensemble de caractères (y co ensemble vide) dans le nom du répertoire, y compris le caract exemple, `/dir/**/fichier*` `/dir/fichier**/`. Le masque `**` ne peut être ut fois dans un nom de répertoir `/dir/**/**/fichier` est ur incorrect. Vous pouvez utiliser le symbol n'importe quel caractère uniqu de fichier ou de répertoire.
`UseOnDemandCPULimit`	Activez les limites d'utilisation du processeur pour les tâches de type *ODS*, *ContainerScan* et *InventoryScan*.	`Yes` active la limitation de la con ressources du processeur pour l *ODS*, *ContainerScan* et *Inventor* `No` (valeur par défaut) : désactiv consommation des ressources C 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*.	10–100 Valeur par défaut : 100.
`UseEdrOptimum`	Activation du module EDR Optimum pour l'intégration avec Kaspersky Endpoint Detection and Response Optimum.	`Yes` : activer le module EDR Opt `No` (valeur par défaut) : désactiv Optimum.

Paramètres généraux d'analyse des conteneurs

Les paramètres généraux de l'analyse du conteneur sont utilisés lors de l'analyse en temps réel des espaces de noms et 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 menaces sur les fichiers sont utilisés. L'action réalisée sur un conteneur suite à la détection d'un objet infectés dépend également des paramètres définis pour la tâche Protection contre les menaces sur les fichiers (cf. tableau ci-dessous).	`StopContainerIfFailed` (valeur par défaut) : arrête le conteneur en cas d'échec de la désinfection ou de la suppression d'un objet infecté. `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.
`UseDocker`	Utilisation de l'environnement Docker.	`Yes` (valeur par défaut) : utilise l'environnement Docker. `No` : n'utilise pas l'environnement 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.

L'action entreprise sur un conteneur lorsqu'un objet infecté est détecté peut changer en fonction des valeurs spécifiées des paramètres `FirstAction` et `SecondAction` de la tâche Protection contre les menaces sur les fichiers.

Dépendance de l'action sur le conteneur par rapport à l'action spécifiée lorsqu'une menace est détectée

Valeur du paramètre FirstAction / SecondAction	Action exécutée sur le conteneur lorsque l'action sélectionnée est StopContainerIfFailed
`Disinfect`	Arrêter le conteneur en cas d'échec de la désinfection de l'objet infecté.
`Remove`	Arrêter le conteneur en cas d'échec de la suppression de l'objet infecté.

Paramètres d'analyse des connexions chiffrées

Paramètres d'analyse des connexions chiffrées

Paramètre	Description	Valeurs
`EncryptedConnectionsScan`	Active ou désactive l'analyse du trafic chiffré. Pour le protocole FTP, l'analyse des connexions chiffrées est désactivée par défaut.	`Yes` (valeur par défaut) : active l'analyse des connexions chiffrées. `No` : désactiver 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.
`UntrustedCertificateAction`	L'action entreprise par l'application lorsqu'elle rencontre un	`Allow` (valeur par défaut) : autorise la connexion réseau établie lors de la visite d'un domaine avec un certificat douteux.

	certificat non vérifié.	`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`	Spécifie la 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.
La section **[Exclusions.item_#]** contient les domaines à exclure de l'analyse. L'application n'analyse pas les connexions chiffrées établies lors de la visite de domaines spécifiés.		
`DomainName`	Spécifie le nom de domaine. Vous pouvez utiliser des masques pour spécifier le domaine.	La valeur par défaut n'est pas définie.
La section **[NetworkPorts.item_#]** contient les ports réseau que l'application doit surveiller.		
`PortName`	Description du port réseau.	La valeur par défaut n'est pas définie.
`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

Paramètres de la programmation du lancement d'une 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>]; [<fréquence 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.	
`RunMissedStartRules`	Démarrage d'une tâche ignorée après le lancement de l'application.	`Yes` : démarrer la tâche ignorée après le lancement de l'application. `No` : ne pas activer le lancement d'une tâche ignorée après le lancement de l'application.

Appendice 4. 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 les arguments 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 l'application ne sont pas chargées (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 leur confirmation, à l'aide de l'argument `--accept`.

74 : la mise à jour requiert le redémarrage de l'application Kaspersky Endpoint Security ;

75 : il faut redémarrer le périphérique ;

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 le périphérique ;

128 : erreur inconnue ;

65 : toutes les autres erreurs.

Appendice 5. 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 de protection contre les menaces sur les fichiers 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 de protection contre les menaces sur les fichiers à l'aide de la commande suivante :

```
kesl-control --set-settings 1 --file <chemin d'accès complet au fichier>
```

Sources d'informations sur Kaspersky Endpoint Security

Page de Kaspersky Endpoint Security sur la Base de connaissances

La *Base de connaissances* est une section du site Internet du Support Technique de Kaspersky.

Sur la page de Kaspersky Endpoint Security dans la Base de connaissances, vous pouvez lire des articles fournissant des informations utiles, des recommandations et des réponses aux questions les plus fréquentes sur 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 des actualités du Support Technique.

Discussion sur les applications de Kaspersky dans le Forum

Si votre question ne nécessite pas de réponse immédiate, vous pouvez en discuter avec les experts Kaspersky et d'autres utilisateurs dans notre Forum.

Sur le Forum, vous pouvez lire les sujets de discussion existants, poster vos commentaires et créer de nouveaux sujets de discussion.

Glossaire

Abonnement

Utilisation de l'application selon les paramètres sélectionnés (date de fin, nombre de périphériques). 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.

Base de données d'adresses Internet de phishing

Liste des adresses des ressources Internet identifiées par les spécialistes de Kaspersky comme des ressources de phishing. La base de données est régulièrement mise à jour et est incluse dans la distribution des applications de Kaspersky.

Base de données d'adresses Internet malveillantes

Liste d'adresses de ressources Internet dont le contenu peut être considéré comme dangereux. Cette liste, compilée par des spécialistes de Kaspersky, est régulièrement mise à jour et est incluse dans la distribution des applications 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 que Kaspersky vous remet avec le fichier clé ou le code d'activation. Il contient des informations sur la licence octroyée.

Clé active

Clé que l'application utilise actuellement.

Clé de réserve

Clé qui permet à l'utilisateur d'utiliser l'application, mais qui n'est pas actuellement en cours d'utilisation.

Désinfection d'objets

Méthode de traitement des objets infectés qui débouche sur une récupération complète ou partielle des données. La désinfection n'est pas applicable à tous les objets infectés.

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 de périphériques réunis dans Kaspersky Security Center en fonction des fonctions exécutées et de l'ensemble des applications de Kaspersky qui y sont installées. Les périphériques 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. Installé sur chaque machine virtuelle qui doit être protégée.

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.

Périphérique de confiance

Un périphérique auquel un accès complet est autorisé à tout moment pour les utilisateurs spécifiés dans les paramètres du périphérique de confiance.

Serveur d'administration

Composant de Kaspersky Security Center qui stocke centralement les informations relatives à toutes les applications de Kaspersky installées dans le réseau de l'entreprise et qui les gère.

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 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 périphériques 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 périphériques 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

cf. 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

Le *système SIEM (Security Information and Event Management)* est une solution de gestion des informations et des événements dans le système de sécurité d'une organisation.

Tâche de groupe

Tâche définie pour un groupe d'administration et exécutée sur tous les périphériques administrés inclus dans ce groupe d'administration.

Information 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.

Avis de marques déposées

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Amazon est une marque commerciale d'Amazon.com, Inc. ou ses affiliés.

FireWire est une marque commerciale 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 terme Bluetooth, la marque et les logos sont la propriété de Bluetooth SIG Inc.

Ubuntu et LTS sont des marques de commerce déposées de Canonical Ltd.

Citrix, XenServer sont des marques commerciales de Citrix Systems, Inc. et/ou filiales enregistrées aux États-Unis et dans les offices de brevets étrangers.

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.

Docker et le logo Docker sont des marques ou des marques déposées de Docker, Inc. aux États-Unis et/ou dans d'autres pays. Docker, Inc. Et d'autres parties peuvent également détenir des droits sur les marques de commerce décrites par d'autres termes utilisés dans ce 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, Core sont des marques commerciales d'Intel Corporation, déposées aux États-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux Etats-Unis et dans 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 OpenStack Foundation aux États-Unis et dans d'autres pays.

Oracle et JavaScript sont des marques déposées d'Oracle et/ou de ses filiales.

Red Hat, Red Hat Enterprise Linux, CentOS 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.

VMware, VMware NSX, VMware NSX Manager, VMware Tools, VMware vCenter, VMware vSphere sont des marques commerciales de VMware, Inc. ou sont des marques déposées de VMware, Inc. aux États-Unis ou dans d'autres juridictions.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, sous licence exclusive de X/Open Company Limited.