kaspersky

Kaspersky Endpoint Security for Windows 11.1.1

Contenu

A propos de Kaspersky Endpoint Security for Windows

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

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

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

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

Le fonctionnement des modules du contrôle est géré par les règles suivantes :

- Le Contrôle des applications utilise les règles de Contrôle des applications.
- Le Contrôle des appareils utilise des règles d'accès aux appareils et des règles d'accès aux bus de connexion.
- Le Contrôle Internet utilise les règles d'accès aux ressources Internet.
- Le Contrôle évolutif des anomalies utilise des règles du Contrôle évolutif des anomalies.

Les modules de protection sont les modules suivants :

- **Détection comportementale**. Ce module reçoit des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent offrir une protection plus efficace.
- **Protection contre les Exploits**. Le module traque les fichiers exécutables lancés par les applications vulnérables. S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier.
- **Prévention des intrusions**. Le module enregistre les actions réalisées par les applications dans le système d'exploitation et gère les actions des applications en fonction du groupe dans lequel le module place cette application. Il existe un ensemble de règles défini pour chaque groupe. Ces règles gèrent l'accès aux données personnelles de l'utilisateur et aux ressources du système d'exploitation. Les données personnelles de l'utilisateur sont les fichiers d'utilisateur dans le dossier Mes documents, les fichiers cookie, les fichiers contenant les informations sur l'activité utilisateur, ainsi que les fichiers, les dossiers et les clés de registre avec les paramètres de fonctionnement et les informations importantes sur les applications le plus souvent utilisées.
- **Réparation des actions malicieuses**. Le composant permet à Kaspersky Endpoint Security d'annuler les actions exécutées par les programmes malveillants dans le système d'exploitation.
- **Protection contre les fichiers malicieux**. Ce module permet d'éviter l'infection du système de fichiers de l'ordinateur. Le composant est opérationnel directement après le lancement de Kaspersky Endpoint Security. Il

se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les périphériques de stockage de masse branchés. Le module intercepte toute tentative de requête au fichier et recherche dans celui-ci la présence éventuelle de virus et autres applications présentant une menace.

- **Protection contre les menaces Internet**. Le composant analyse le trafic qui arrive sur l'ordinateur de l'utilisateur via le protocole HTTP et FTP et définit également si une adresse Internet appartient à la base des adresses Internet malveillantes ou de phishing.

- **Protection contre les menaces par emails**. Le composant analyse l'ensemble des messages électroniques entrants et sortants à la recherche d'éventuels virus et d'autres applications présentant une menace.

- **Protection contre les menaces réseau**. Le module recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque l'activité réseau de l'ordinateur attaquant.

- **Pare-feu**. Le module assure la protection des données personnelles stockées sur l'ordinateur de l'utilisateur en bloquant la majorité des menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local. Ce module filtre toute l'activité du réseau en fonction de deux types de règles : les règles réseau pour les applications et les règles réseau pour les paquets.

- **Protection BadUSB**. Le module permet d'empêcher la connexion de périphériques USB infectés qui imitent un clavier.

- **Fournisseur de protection AMSI**. Le composant analyse les objets selon la requête de l'application tierce et transmet les résultats de l'analyse à l'application qui a envoyé la requête.

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

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

L'application Kaspersky Endpoint Security prévoit les tâches suivantes :

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

- **Analyse complète**. Kaspersky Endpoint Security lance l'analyse du système d'exploitation y compris la mémoire du noyau, les objets chargés au lancement du système d'exploitation, les secteurs d'amorçage, la sauvegarde du système d'exploitation et tous les disques durs et amovibles.

- **Analyse personnalisée**. Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur.

- **Analyse des zones critiques**. Kaspersky Endpoint Security analyse la mémoire du noyau et les objets et secteurs d'amorçage chargés au lancement du système d'exploitation.

- **Mise à jour**. Kaspersky Endpoint Security charge les mises à jour de la base et des modules de l'application. Ceci garantit l'actualité de la protection de l'ordinateur contre les virus et autres applications dangereuses.

- **Restauration de la dernière mise à jour**. Kaspersky Endpoint Security annule la dernière mise à jour des bases de données et des modules. Cela permet de revenir à l'utilisation des bases et les modules de l'application antérieurs le cas échéant, par exemple si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sûre.

Administration à distance via Kaspersky Security Center

L'application Kaspersky Security Center permet de lancer et d'arrêter Kaspersky Endpoint Security à distance sur un poste client, d'effectuer la gestion des tâches, de configurer les paramètres de fonctionnement de l'application et d'utiliser le chiffrement des fichiers et le chiffrement du disque.

La fonction de chiffrement des fichiers permet de chiffrer les fichiers et les dossiers stockés sur les disques locaux de l'ordinateur. La fonction de chiffrement du disque permet de chiffrer les disques durs et les disques amovibles.

Fonctions de service de l'application

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

- **Rapports**. Pendant le fonctionnement de l'application, celle-ci génère un rapport pour chaque module de l'application. Les rapports permettent également de surveiller les résultats de l'exécution des tâches. Les rapports contiennent les listes des événements survenus pendant le fonctionnement de Kaspersky Endpoint Security et dans toutes les opérations exécutées par l'application. En cas de problème, vous pouvez envoyer ces rapports aux experts de Kaspersky ce qui leur permettra d'analyser la situation plus en détail.

- **Stockage des données**. Si l'application détecte des fichiers infectés lors de la recherche d'éventuels virus ou autres programmes dangereux sur l'ordinateur, elle bloque les fichiers en question. Kaspersky Endpoint Security sauvegarde les copies des fichiers réparés ou supprimés dans la *sauvegarde*. Kaspersky Endpoint Security met les fichiers qui n'ont pas été traités pour une raison quelconque sur la *liste des menaces actives*. Vous pouvez analyser les fichiers, restaurer les fichiers vers leur dossier d'origine et purger les stockages.

- **Service des notifications**. Le Service des notifications tient l'utilisateur au courant des événements qui ont un impact sur l'état de la protection de l'ordinateur et sur le fonctionnement de Kaspersky Endpoint Security. Les notifications peuvent être affichées sur l'écran ou envoyées par courrier électronique.

- **Kaspersky Security Network**. La participation de l'utilisateur au fonctionnement de Kaspersky Security Network permet d'augmenter l'efficacité de la protection grâce à une utilisation plus rapide des informations relatives à la réputation des fichiers, des sites Internet et du logiciel fournies par les utilisateurs du monde entier.

- **Licence**. L'achat d'une licence permet d'utiliser toutes les fonctions de l'application, d'accéder à la mise à jour des bases et des modules de l'application et de bénéficier du support technique par téléphone ou courrier électronique pour toute question liée à l'installation, à la configuration et à l'utilisation de l'application.

- **Support Technique**. Tous les utilisateurs inscrits de Kaspersky Endpoint Security peuvent bénéficier de l'aide des experts du Support Technique de Kaspersky. Vous pouvez envoyer la demande au Support Technique de Kaspersky depuis le portail Kaspersky CompanyAccount ou par téléphone.

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

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

1. Elle désactive les fonctions de contrôle et de protection (la fonction de chiffrement reste active).

2. Elle avertit l'utilisateur de la désactivation de ces fonctions.

3. Après la mise à jour des bases ou la mise en œuvre des bases des modules de l'application, la fonction tente d'en rétablir le fonctionnement.

L'application obtient des informations relatives aux erreurs répétitives qui entraînent l'arrêt du fonctionnement à l'aide d'algorithmes spéciaux développés par les experts de Kaspersky. Cette information est nécessaire pour le rétablissement de l'application.

Distribution

La distribution contient les paquets de distribution suivants :

- **Strong encryption (AES256)**

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

- **Lite encryption (AES56)**

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

Chaque paquet de distribution contient les fichiers suivants :

`kes_win.msi`	Paquet d'installation de Kaspersky Endpoint Security.
`setup_kes.exe`	Les fichiers nécessaires à l'installation de l'application selon tous les moyens disponibles ;
`kes_win.kud`	Fichier pour la création du paquet d'installation de Kaspersky Endpoint Security.
`klcfginst.msi`	Paquet d'installation du plug-in d'administration Kaspersky Endpoint Security pour Kaspersky Security Center.
`bases.cab`	Les fichiers des paquets de mise à jour utilisés lors de l'installation de l'application.
`cleaner.cab`	Fichiers pour la suppression des applications incompatibles.
`incompatible.txt`	Le fichier contenant la liste des applications incompatibles.
`ksn_<ID de la langue>.txt`	Le fichier à l'aide duquel vous pouvez prendre connaissance des conditions de participation à Kaspersky Security Network.
`license.txt`	Le fichier qui vous permet de prendre connaissance du Contrat de licence et de la Politique de confidentialité.
`installer.ini`	Le fichier contenant les paramètres interne de la distribution.

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

Configurations logicielles et matérielles

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

Configuration minimale requise :

- Espace disponible sur le disque dur : 2 Go ;
- processeur de 1 GHz (avec prise en charge des instructions SSE2) ;
- Mémoire vive :
  - pour le système d'exploitation 32 bits : 1 Go ;
  - pour le système d'exploitation 64 bits : 2 Go.

Systèmes d'exploitation compatibles pour les postes de travail :

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 et suivants ;
- Windows 8 Professional / Enterprise ;
- Windows 8.1 Professional / Enterprise ;
- Windows 10 Home / Pro / Education / Enterprise.

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

Systèmes d'exploitation compatibles pour les serveurs de fichiers :

- Windows Small Business Server 2008 Standard / Premium (64 bits) ;
- Windows Small Business Server 2011 Essentials / Standard (64 bits) ;

  Microsoft Small Business Server 2011 Standard (64 bits) est pris en charge uniquement avec Service Pack 1 installé pour Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64 bits) ;
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 et suivants ;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 et suivants ;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter ;
- Windows Server 2016 Essentials / Standard / Datacenter ;

- Windows Server 2019 Essentials/Standard/Datacenter.

Les particularité de la prise en charge des systèmes d'exploitation Microsoft Windows Server 2016 et Microsoft Windows Server 2019 sont reprises dans la base des connaissances du Support Technique :

Plateformes virtuelles compatibles :

- VMware Workstation 14 ;
- VMware ESXi 6.5 U1 ;
- Microsoft Hyper-V 2016 Server
- Microsoft Hyper-V 2019 Server
- Citrix XenServer 7.2 ;
- Citrix XenDesktop 7.17 ;
- Citrix XenApp 7.17 ;
- Citrix Provisioning Services 7.17.

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

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

Comparaison des fonctions de Kaspersky Endpoint Security

Fonction	Poste de travail	Serveur de fichiers
Protection avancée		
Kaspersky Security Network	✓	✓
Détection comportementale	✓	✓
Protection contre les Exploits	✓	✓
Prévention des intrusions	✓	–
Réparation des actions malicieuses	✓	✓
protection principale contre les menaces.		
Protection contre les fichiers malicieux	✓	✓
Protection contre les menaces Internet	✓	–
Protection contre les menaces par emails	✓	–
Firewall	✓	✓
Protection contre les menaces réseau	✓	✓

Protection BadUSB	✓	✓
Fournisseur de protection AMSI	✓	✓
Contrôles de sécurité		
Contrôle des applications	✓	✓
Contrôle des périphériques	✓	–
Contrôle Internet	✓	–
Contrôle évolutif des anomalies	✓	–
Chiffrement des données		
Kaspersky Disk Encryption	✓	–
Chiffrement de disque BitLocker	✓	✓
Chiffrement des fichiers	✓	–
Chiffrement des disques amovibles	✓	–
Enpoint Sensor	✓	✓

Compatibilité avec les autres applications de Kaspersky

Kaspersky Endpoint Security recherche la présence éventuelle d'autres applications de Kaspersky avant l'installation.

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

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.

  La suppression automatique de Kaspersky Anti-Ransomware Tool n'est pas prise en charge. Supprimez Kaspersky Anti-Ransomware Tool manuellement.

- Kaspersky Anti Targeted Attack Platform (y compris les composants Sensor et Endpoint Sensors).
- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server.

- Kaspersky Embedded Systems Security.

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

Nouveautés

Nouvelles fonctionnalités et améliorations de Kaspersky Endpoint Security 11.1.1 for Windows :

1. Systèmes d'exploitation pris en charge :
   - Ajout de la prise en charge du système d'exploitation Windows 10 May 2019 Update (19H1, version 1903).
   - Ajout de la prise en charge de la migration de la version Kaspersky Endpoint Security 11.1.1 for Windows installée lors de la mise à jour du système d'exploitation Windows 7 / 8 / 8.1 vers Windows 10.
   - Ajout de la prise en charge de l'intégration à Windows Defender Security Center.
   - Ajout de la prise en charge de Antimalware Scan Interface (AMSI).
   - Prise en charge des sous-systèmes Windows pour Linux (Windows Subsystem for Linux, WSL). La prise en charge de WSL ne requiert aucune configuration complémentaire de l'application. La détection des menaces dans l'environnement GNU/Linux s'opère au niveau du système d'exploitation Windows. Il n'est pas nécessaire d'installer des solutions antivirus complémentaires dans l'environnement GNU/Linux. Pour en savoir plus sur le sous-système Windows pour Linux, consultez le site de Microsoft.
2. Prise en charge de l'application via Kaspersky Security Center 11 Web Console.
3. Prise en charge de la mise à jour des bases depuis les serveurs de Kaspersky via le protocole HTTPS.
4. Ajout du nouveau composant Contrôle évolutif des anomalies. Le composant traque et bloque les actions potentiellement dangereuses, atypiques pour l'ordinateur protégé.
5. Ajout de l'analyse du trafic HTTPS.
6. Ajout au module Prévention des intrusions d'une fonction de protection contre les attaques qui exploitent une vulnérabilité du protocole ARP pour falsifier les adresses MAC des appareils.
7. Ajout d'un indicateur de niveau de protection au package d'installation utilisé pour le déploiement à distance de l'application. L'indicateur affiche le niveau de sécurité lors de la sélection des modules de l'application à installer.
8. Ajout de la catégorie "Cryptodevises et mining" pour le module Contrôle Internet.
9. Contrôle des applications:
   - Possibilité de créer et de modifier les catégories d'applications depuis les stratégies de Kaspersky Endpoint Security 11.1.1 for Windows.
   - Améliorations des rapports sur les lancements d'application bloqués.
10. Possibilité d'élargir les droits d'accès aux périphériques portables (MTP) pour le Contrôle des périphériques.
11. Autres perfectionnement :
    - Réduction de la consommation des ressources du système lors de l'utilisation de l'application en arrière plan.
    - Optimisation du mécanisme d'exclusions de l'analyse pour garantir le fonctionnement des processus et des services critiques pour le système. Fin de la nécessité de créer les exclusions prédéfinies recommandées par les experts de Kaspersky lors de l'installation.
    - Ajout dans Kaspersky Security Center d'un rapport sur l'état des modules de l'application.

- Ajout dans les paramètres de la protection par mot de passe de la possibilité de définir des utilisateurs de domaine et es groupes autorisés à administrer l'application.

- Ajout de la possibilité de protéger par mot de passe la restauration d'objets depuis la Sauvegarde.

- Ajout de la possibilité d'enrichir les listes d'exclusions de la zone de confiance à l'aide de listes définies dans les profils.

Licence de l'application

Cette section fournit des informations sur les concepts généraux liés à la licence d'application.

À propos du Contrat de licence

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

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

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

- Pendant l'installation de Kaspersky Endpoint Security en mode interactif.
- en lisant le document license.txt. Ce document est inclus dans le kit de distribution de l'application.

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

À propos de la licence

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

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

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

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

Les types de licence suivants sont proposés :

- *Evaluation* : une licence gratuite conçue pour découvrir l'application.

  En général, la durée de validité d'une licence d'essai est brève. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

  Vous ne pouvez activer l'application avec une licence d'essai qu'une seule fois.

- *Commerciale* : licence payante octroyée à l'achat de l'application.

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

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

A propos du certificat de licence

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

Il reprend les informations suivantes relatives à la licence octroyée :

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

A propos de l'abonnement

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

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

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

Pour utiliser Kaspersky Endpoint Security sur abonnement, il est nécessaire d'entrer le code d'activation fourni par le prestataire de services. Une fois que le code d'activation est appliqué, la clé active est installée. La clé active détermine la licence d'utilisation de l'application dans le cadre de l'abonnement. Il est possible d'installer une clé complémentaire uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé ou d'un abonnement.

Le choix des possibilités de gestion de l'abonnement diffère selon les prestataires de services. Le prestataire de services peut ne pas proposer de période de grâce où l'application continue à fonctionner après la date d'expiration.

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

A propos du code d'activation

Un *code d'activation* est une séquence alphanumérique unique de vingt lettres et chiffres latins que vous recevez lors de l'achat d'une licence commerciale pour Kaspersky Endpoint Security.

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

L'activation de l'application à l'aide d'un code d'activation entraîne l'installation d'une clé active. Il est possible d'installer une clé complémentaire uniquement à l'aide d'un code d'activation et non pas à l'aide d'un fichier clé ou d'un abonnement.

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

A propos de la clé

Une *clé* est une séquence alphanumérique unique. La clé permet l'utilisation de l'application conformément aux conditions figurant dans le Certificat de licence (au type de licence, à la durée de validité de la licence, aux restrictions imposées par la licence).

Pour la clé installée selon un abonnement, le certificat de licence n'est pas proposé.

La clé peut être ajoutée à l'application à l'aide du code d'activation ou du fichier clé.

Vous pouvez ajouter, modifier ou supprimer des clés. La clé peut être bloquée par Kaspersky en cas de non-respect du Contrat de licence Utilisateur final. Si la clé est bloquée, une autre clé sera nécessaire pour utiliser l'application.

Si la clé d'une licence dont la validité expire est supprimée, les fonctions de l'application ne seront plus accessibles. Il est impossible d'ajouter à nouveau une telle clé après la suppression.

Une clé peut être active ou complémentaire.

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

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

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

Si la clé est placée dans la liste noire des clés, les fonctions accessibles de l'application seront celles définies par la licence activant l'application pendant 8 jours. Kaspersky Security Network et les mises à jours des bases de données et des modules de l'application sont accessibles sans restrictions. L'application notifie l'utilisateur sur le placement de la clé dans la liste noire des clés. A l'issue des huit jours, les fonctions de l'application sont limitées comme dans le cas d'une expiration de la licence : l'application fonctionne sans mise à jour et Kaspersky Security Network n'est pas accessible.

A propos du fichier clé

Un *fichier clé* est un fichier portant l'extension .key que Kaspersky vous fournit après que vous avez acheté Kaspersky Endpoint Security. Le fichier clé permet d'ajouter une clé pour activer l'application.

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

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

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

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

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

A propos de la collecte des données

Si vous avez activé Kaspersky Endpoint Security à l'aide d'un code d'activation, vous acceptez de transmettre automatiquement les informations suivantes en vue de confirmé la légalité de l'utilisation du programme :

- type, version et localisation de Kaspersky Endpoint Security ;
- versions des mises à jour installées de Kaspersky Endpoint Security ;
- identifiant de l'ordinateur et l'identifiant de l'installation de Kaspersky Endpoint Security sur l'ordinateur ;
- numéro de série et identificateur de la clé active ;
- type, version et nombre de bits du système d'exploitation, nom de l'environnement virtuel, installation ou non de l'application Kaspersky Endpoint Security dans l'environnement virtuel ;
- identifiants des composants de Kaspersky Endpoint Security actifs au moment de l'octroi des informations.

Kaspersky peut aussi utiliser ces informations pour générer des statistiques sur la diffusion et l'utilisation de l'application de Kaspersky.

En utilisant le code d'activation, vous acceptez de transmettre automatiquement les données citées ci-dessus. Si vous ne voulez pas envoyer ces informations à Kaspersky, vous pouvez activer Kaspersky Endpoint Security à l'aide du fichier clé.

En acceptant les dispositions du Contrat de licence, vous acceptez de transmettre automatiquement les informations suivantes :

- Lors de la mise à jour de Kaspersky Endpoint Security :
  - version de Kaspersky Endpoint Security ;
  - identifiant de Kaspersky Endpoint Security ;
  - clé active ;
  - identifiant unique du lancement de la tâche de mise à jour ;
  - identifiant unique d'installation de Kaspersky Endpoint Security.
- Lors de la navigation via les liens de l'interface de Kaspersky Endpoint Security :
  - version de Kaspersky Endpoint Security ;
  - version du système d'exploitation ;
  - date d'activation de Kaspersky Endpoint Security ;
  - date de fin de la durée de validité de la licence ;
  - date de création de la clé ;
  - date d'installation de Kaspersky Endpoint Security ;
  - identifiant de Kaspersky Endpoint Security ;
  - identifiant de la vulnérabilité du système d'exploitation détectée ;
  - identifiant de la dernière mise à jour installée pour Kaspersky Endpoint Security ;
  - hash du fichier détecté qui constitue une menace et nom de cet objet selon la classification de Kaspersky ;
  - catégorie d'erreur d'activation de Kaspersky Endpoint Security ;
  - code d'erreur d'activation de Kaspersky Endpoint Security ;
  - nombre de jours restant avant l'expiration de la clé ;
  - nombre de jours écoulés depuis l'ajout de la clé ;
  - nombre de jours écoulés depuis l'expiration de la licence ;
  - nombre d'ordinateurs couverts par les licences actives ;

- clé active ;
- durée de validité de la licence de Kaspersky Endpoint Security ;
- état actuel de la licence ;
- type de licence active ;
- type de l'application ;
- identifiant unique du lancement de la tâche de mise à jour ;
- identifiant unique d'installation de Kaspersky Endpoint Security.
- identifiant unique de l'installation de l'application sur l'ordinateur ;
- langue de l'interface de Kaspersky Endpoint Security.

Les informations obtenues par Kaspersky sont protégées conformément à la législation en vigueur et aux politiques de Kaspersky.

Pour en savoir plus sur l'obtention, le traitement, la conservation et la suppression des informations relatives à l'utilisation de l'application après l'acceptation du Contrat de licence et de la Déclaration de Kaspersky Security Network, veuillez lire le contenu de ces derniers ou rendez-vous sur le site Internet de Kaspersky. Les fichiers license.txt et ksn_<ID de la langue>.txt qui contiennent les textes du Contrat de licence et de la Déclaration de Kaspersky Security Network figurent dans le kit de distribution.

A propos des modes d'activation de l'application

L'*activation* est une procédure qui consiste à insérer un code dans le logiciel Kaspersky afin d'en activer sa licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence. La procédure d'activation de l'application est incluse avec l'ajout de la clé.

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

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

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

- Via la ligne de commande.

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

Administration de l'application via l'interface locale

Cette section présente l'administration de Kaspersky Endpoint Security via l'interface locale.

Installation et suppression de l'application

Cette section explique comment installer Kaspersky Endpoint Security, comment procéder à la configuration initiale de l'application, comment réaliser la mise à jour d'une version antérieure et comment supprimer l'application.

Installation de l'application

Cette section explique comment installer Kaspersky Endpoint Security et réaliser la configuration initiale.

A propos des méthodes d'installation de l'application

Kaspersky Endpoint Security peut être installé localement (directement sur l'ordinateur de l'utilisateur) ou à distance depuis le poste de travail de l'administrateur.

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

- en mode interactif à l'aide de l'Assistant d'installation de l'application.

  Ce mode requiert votre intervention tout au long du processus.

- En mode silencieux depuis la ligne de commande.

  Une fois que vous aurez lancé l'installation en mode silencieux, vous n'aurez plus à intervenir dans l'installation.

L'installation à distance de l'application sur les ordinateurs du réseau peut être réalisée à l'aide d'un des éléments suivants :

- le logiciel Kaspersky Security Center (les détails sont disponibles dans l'aide de Kaspersky Security Center) ;
- l'éditeur de gestion des stratégies de groupe Microsoft Windows (cf. la documentation qui accompagne le système d'exploitation) ;
- Gestionnaire de configuration System Center.

Les paramètres d'installation de Kaspersky Endpoint Security reçus via le fichier setup.ini, possèdent la priorité la plus élevée. Lors de l'installation, Kaspersky Endpoint Security utilise les paramètres avec la priorité la plus élevée. Lors de l'installation, Kaspersky Endpoint Security utilise les paramètres avec la priorité la plus élevée.

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

Installation de l'application à l'aide de l'assistant d'installation de l'application

L'interface de l'Assistant d'installation de l'application est composée d'une série de fenêtres qui correspondent aux différentes étapes de l'installation de l'application. Vous pouvez naviguer entre les pages de l'assistant de configuration à l'aide des boutons **Précédent** et **Suivant**. Pour fermer l'Assistant de configuration une fois sa tâche terminée, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant de configuration à n'importe quelle étape, cliquez sur le bouton **Annuler**.

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

1. Copiez le dossier du kit de distribution sur l'ordinateur de l'utilisateur.

2. Lancer le fichier setup_kes.exe.

   Une fois que le fichier setup_kes.exe a été lancé, Kaspersky Endpoint Security recherche la présence éventuelles d'applications incompatibles sur l'ordinateur. Par défaut, si une telle application est détectée, l'installation est interrompue et la liste des applications incompatibles avec Kaspersky Endpoint Security qui ont été détectées s'affiche. Pour continuer l'installation, il faut supprimer ces applications de l'ordinateur.

Étape 1. Vérification de la configuration du système par rapport à la configuration requise

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

- Si le système d'exploitation et le Service Pack répondent ou non aux exigences logicielles pour l'installation du produit.
- Respect des configurations logicielle et matérielle ;
- Présences des privilèges pour l'installation du logiciel.

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

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

Si la liste des applications détectées contient des versions précédentes de Kaspersky Endpoint Security, toutes les données qui peuvent être migrées (par exemple, les informations sur l'activation, les paramètres de l'application), sont conservées et sont utilisées lors de l'installation de Kaspersky Endpoint Security 11.1.1 for Windows, et la version précédente de l'application est supprimée automatiquement. Cela se concerne les versions suivantes de l'application :

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (version 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (version 10.2.4.674).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (version 10.2.5.3201).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (version 10.2.6.3733).

- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (version 10.3.3.275).
- Kaspersky Endpoint Security 11.0.0 for Windows (version 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (version 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.0.1 SF1 (version 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.1.0 (version 11.1.0.15919).

Étape 2. Fenêtre d'accueil de la procédure d'installation

Si les conditions d'installation de l'application correspondent parfaitement à la configuration requise, la fenêtre de départ s'ouvre après l'exécution du paquet d'installation. La fenêtre de départ contient les informations relatives au début de l'installation de Kaspersky Endpoint Security sur l'ordinateur.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 3. Consultation du contrat de licence et de la Politique de confidentialité

Cette étape de l'assistant d'installation vous permet de devez prendre connaissance du Contrat de licence conclu entre vous et Kaspersky.

Lisez attentivement le Contrat de licence et la Politique de confidentialité. Si vous êtes d'accord avec tous les points du Contrat de licence et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

- **les termes et conditions de ce Contrat de licence utilisateur final ;**
- **politique de confidentialité décrivant le traitement des données.**

L'installation de l'application sur votre appareil se poursuit après que vous avez coché les deux cases.

Si vous n'acceptez pas les dispositions du Contrat de licence et de la Politique de confidentialité, annulez l'installation de l'application en cliquant sur le bouton **Annuler**.

Étape 4. Sélection des modules de l'application à installer

Cette étape vous permet de sélectionner les modules de Kaspersky Endpoint Security que vous voulez installer. Le module Protection contre les fichiers malicieux doit obligatoirement être installé. Vous ne pouvez pas annuler son installation.

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

- Protection BadUSB.

- Chiffrement des fichiers.
- Chiffrement du disque.
- Administration BitLocker.
- Endpoint Sensor.

Administration BitLocker exécute les fonctions suivantes :

- administration du chiffrement Windows BitLocker intégré au système d'exploitation ;
- configuration du chiffrement dans les paramètres de la stratégie de Kaspersky Security Center et vérification de leur adéquation à l'ordinateur administré ;
- lancement des processus de chiffrement et de déchiffrement ;
- surveillance de l'état de chiffrement sur l'ordinateur administré ;
- conservation centralisée des clés de récupération sur le Serveur d'administration Kaspersky Security Center.

Endpoint Sensor est un module de Kaspersky Anti Targeted Attack Platform (KATA). Cette solution a été développée pour détecter en temps utiles les menaces telles que les attaques ciblées. Le module surveille en permanence les processus ouverts par les connexions réseaux et les fichiers modifiés et transmet ces informations à Kaspersky Anti Targeted Attack Platform.

Pour sélectionner un module à installer, cliquez sur l'icône en regard du nom du module pour afficher le menu contextuel et sélectionnez **La fonctionnalité sera installée sur le disque dur local**. Pour plus d'informations sur les tâches exécutées par le module sélectionné et sur l'espace libre requis sur le disque dur pour l'installation du module, veuillez consulter la partie inférieure de la fenêtre actuelle de l'Assistant d'installation de l'application.

Pour afficher des informations détaillées sur l'espace disponible sur les disques durs locaux, cliquez sur le bouton **Volume**. Les informations seront affichées dans la fenêtre **Exigences d'espace disque** qui s'ouvre.

Pour annuler l'installation du module, sélectionnez l'option **La fonctionnalité sera indisponible** dans le menu contextuel.

Pour revenir à la liste des composants installés par défaut, cliquez sur le bouton **Réinitialiser**.

Étape 5. Sélection du dossier de destination

Cette étape est disponible si vous sélectionnez *Installation personnalisée* de l'application.

A cette étape, vous pouvez indiquer le chemin d'accès au dossier d'installation dans lequel l'application sera installée. Pour sélectionner le dossier de destination de l'application, cliquez sur le bouton **Parcourir**.

Pour afficher des informations sur l'espace disponible sur les disques durs locaux, cliquez sur le bouton **Volume**. Les informations s'affichent dans la fenêtre **Espace disque requis** qui s'ouvre.

Étape 6. Préparation de l'installation de l'application

Il est conseillé de protéger le processus d'installation car l'ordinateur pourrait abriter des applications malveillantes capable de perturber l'installation de Kaspersky Endpoint Security.

Le processus d'installation est activé par défaut.

Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop). Dans ce cas, interrompez l'installation et relancez l'Assistant d'installation de l'application. A l'étape "Préparation de l'installation de l'application", décochez la case **Protéger le processus d'installation de l'application**.

La case **Garantir la compatibilité avec Citrix PVS** active/désactive la fonction qui installe les pilotes en mode de compatibilité Citrix PVS.

Cochez cette case uniquement si vous utilisez la technologie Citrix Provisioning Services.

La case **Ajoutez le chemin du fichier avp.com à la variable système %PATH%** active/désactive une option qui ajoute le chemin du fichier avp.com à la variable système %PATH%.

Si la case est cochée, il n'est pas nécessaire de saisir le chemin d'accès au fichier exécutable pour lancer Kaspersky Endpoint Security ou n'importe quelle tâche de l'application via la ligne de commande. Il suffit de saisir le nom du fichier exécutable et l'instruction pour le lancement de la tâche correspondante.

Cliquez sur le bouton **Installer** afin d'installer l'application.

Les connexions réseau actuelles peuvent être interrompues au cours de l'installation de l'application sur l'ordinateur. La majorité des connexions réseau interrompues se rétablit après la fin de l'installation de l'application.

Étape 7. Installation de l'application

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

Si vous exécutez la mise à jour de la version précédente de l'application, sur cette étape la migration des paramètres et la suppression de la version précédente de l'application est aussi exécutée.

Une fois l'installation de Kaspersky Endpoint Security réussie, l'Assistant de configuration initiale de l'application est lancé.

Installation de l'application via la ligne de commande

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

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

Pour installer l'application ou la mettre à jour, procédez comme suit :

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

3. Exécutez la commande :

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

ou

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

`EULA`	Acceptation ou refus des dispositions du contrat de licence Utilisateur final. Valeurs possibles : • `1` – acceptation des dispositions du Contrat de licence Utilisateur final. • `0` – refus des dispositions du Contrat de licence Utilisateur final. Le texte Contrat de licence utilisateur final fait partie de la distribution de Kaspersky Endpoint Security. L'acceptation des dispositions du contrat de licence Utilisateur final est une condition indispensable pour installer l'application ou pour la mettre à jour.
`PRIVACYPOLICY`	Acceptation ou rejet de la Politique de confidentialité. Valeurs possibles : • `1` – acceptation de la Politique de confidentialité. • `0` – rejet de la Politique de confidentialité. Le texte de la Politique de confidentialité fait partie du kit de distribution de Kaspersky Endpoint Security. L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.
`KSN`	Participation ou non au Kaspersky Security Network (KSN). Si le paramètre n'est pas précisé, Kaspersky Endpoint Security sollicitera la confirmation de la participation à KSN au premier lancement de l'application. Valeurs possibles : • `1` : acceptation de la participation à KSN. • `0` : refus de la participation à KSN (valeur par défaut). Le paquet de distribution de Kaspersky Endpoint Security est optimisé pour l'utilisation de Kaspersky Security Network. Si vous avez refusé de participer au Kaspersky Security Network, mettez à jour Kaspersky Endpoint Security directement à l'issue de l'installation.
`ALLOWREBOOT=1`	Redémarrage automatique de l'ordinateur après l'installation ou la mise à jour de l'application, le cas échéant. Si le paramètre n'est pas défini, le redémarrage automatique de l'ordinateur est interdit. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.
`ADDLOCAL`	Sélection de composants supplémentaires pour l'installation. Par défaut, tous les modules à l'exceptions des modules suivants sont sélectionnés

	pour l'installation : Protection BadUSB, Chiffrement des fichiers, Chiffrement du disque, Administration de BitLocker et Endpoint Sensor. Valeurs possibles : • `MSBitLockerFeature`. Procède à l'installation du module Administration de BitLocker. • `AntiAPTFeature`. L'installation du module Endpoint Sensor a lieu.
`SKIPPRODUCTCHECK=1`	Désactivation de la recherche de logiciels incompatibles. La liste des applications incompatibles figure dans le fichier incompatible.txt du kit de la distribution. Si le paramètre n'est pas spécifié, l'installation de Kaspersky Endpoint Security est interrompue en cas de détection d'une application incompatible.
`SKIPPRODUCTUNINSTALL=1`	Interdiction de la suppression automatique de l'application incompatible détectée. Si le paramètre n'est pas spécifié, Kaspersky Endpoint Security tente de supprimer l'application incompatible.
`KLLOGIN`	Définition du nom d'utilisateur pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (module Protection par mot de passe). Le nom d'utilisateur est défini avec les paramètres `KLPASSWD` et `KLPASSWDAREA`. Le nom d'utilisateur par défaut est KLAdmin.
`KLPASSWD`	Définition du mot de passe pour l'accès à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (le mot de passe est défini en même temps que les paramètres `KLLOGIN` et `KLPASSWDAREA`). Si vous avez indiqué un mot de passe, mais que vous n'avez pas défini le nom d'utilisateur à l'aide du paramètre `KLLOGIN`, le nom d'utilisateur KLAdmin sera utilisé par défaut.
`KLPASSWDAREA`	Définition de la zone d'action du mot de passe pour l'accès à Kaspersky Endpoint Security. Quand l'utilisateur tente d'exécuter une action depuis cette zone, Kaspersky Endpoint Security demande les identifiants de l'utilisateur (paramètres `KLLOGIN` et `KLPASSWD`). Pour indiquer plusieurs valeurs, utilisez le caractère "`;`". Valeurs possibles : • `SET` – modification des paramètres de l'application. • `EXIT` – arrêt de l'application. • `DISPROTECT` – désactivation des modules de protection et arrêt des tâches d'analyse. • `DISPOLICY` – désactivation de la stratégie de Kaspersky Security Center. • `UNINST` – suppression de l'application de l'ordinateur. • `DISCTRL` – désactivation des modules de contrôle. • `REMOVELIC` – suppression de la clé. • `REPORTS` – consultation des rapports.
`ENABLETRACES`	Activation ou désactivation du traçage de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier %ProgramData %/Kaspersky Lab après le lancement. Valeurs possibles :

	• `1` : le traçage est activé. • `0` : le traçage est désactivé (valeur par défaut).
`TRACESLEVEL`	Niveau de détail du traçage Valeurs possibles : • `100` (critique). Uniquement les messages relatifs aux erreurs irrémédiables. • `200` (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables. • `300` (diagnostique). Messages relatifs à toutes les erreurs et collecte des messages d'avertissement. • `400` (important). Tous les avertissements et messages relatifs aux erreurs normales et irrémédiables et ensemble de messages proposant des informations complémentaires. • `500` (ordinaire). Tous les avertissements et les messages relatifs aux erreurs normales et irrémédiables et messages avec des informations détaillées sur le fonctionnement en mode normal (valeur par défaut). • `600` (bas). Tous les messages possibles.

Exemple :

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

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

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

Après l'installation de l'application, Kaspersky Endpoint Security active la licence d'essai si vous n'avez pas indiqué le code d'activation dans le fichier setup.ini. En général, la durée de validité d'une licence d'essai est brève. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, vous devez activer une licence commerciale.

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

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

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

Pour appliquer les paramètres des fichiers setup.ini, install.cfg et setup.reg, installez ces fichiers dans le dossier contenant le kit de distribution de Kaspersky Endpoint Security.

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

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

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

1. Ouvrez la console Configuration Manager.
2. Dans la partie droite de la console, dans le groupe **Administration des applications** choisissez la section **Paquets**.
3. Dans la partie supérieure de la console, dans le panne d'administration, cliquez sur le bouton **Créer un paquet**.

   L'*Assistant de création de paquets et d'applications* est lancé.
4. Dans l'Assistant de création de paquets et d'applications, procédez comme suit :

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

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

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

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

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

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

   - Cochez la case **Lancer d'abord une autre application** si vous voulez qu'une autre application soit lancée avant l'installation de Kaspersky Endpoint Security.

     Choisissez l'application dans la liste déroulante **Application** ou indiquez le chemin d'accès au fichier exécutable de cette application à l'aide du bouton **Parcourir**.

- Choisissez l'option **Cette application peut être lancée uniquement sur les plateformes indiquées** dans le groupe **Configuration de la plateforme** si vous voulez que l'application soit installée uniquement dans les systèmes d'exploitation indiqués.

  Cochez dans la liste les applications en regard des systèmes d'exploitation sur lesquels Kaspersky Endpoint Security doit être installé.

Cette étape est facultative.

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

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

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

   L'*Assistant déploiement du logiciel* est lancé.

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

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

   - Dans le champ **Logiciel**, saisissez le nom unique du paquet d'installation ou choisissez le paquet d'installation de la liste à l'aide du bouton **Parcourir**.

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

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

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

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

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

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

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

Le fichier setup.ini comprend les sections suivantes :

- `[Setup]` – paramètres généraux d'installation de l'application.

- `[Components]` – sélection des modules de l'application à installer. Si aucun module n'a été désigné, tous les modules disponibles pour le système d'exploitation sont installés. La Protection contre les fichiers malicieux est un module obligatoire qui est installé sur l'ordinateur, quels que soient les paramètres définis dans ce groupe.

- `[Tasks]` – sélection des tâches à ajouter à la liste des tâches de Kaspersky Endpoint Security. Si aucune tâche n'est désignée, toutes les tâches sont reprises dans la liste des tâches de Kaspersky Endpoint Security.

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

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

Paramètres du fichier setup.ini

Section	Paramètre	Description
`[Setup]`	`InstallDir`	Chemin d'accès au dossier d'installation de l'application.
	`ActivationCode`	Code d'activation de Kaspersky Endpoint Security.
	`Eula`	Acceptation ou refus des dispositions du contrat de licence Utilisateur final. Valeurs possibles : • `1` – acceptation des dispositions du Contrat de licence Utilisateur final. • `0` – refus des dispositions du Contrat de licence Utilisateur final. Le texte Contrat de licence utilisateur final fait partie de la distribution de Kaspersky Endpoint Security. L'acceptation des dispositions du contrat de licence Utilisateur final est une condition indispensable pour installer l'application ou pour la mettre à jour.
	`PrivacyPolicy`	Acceptation ou rejet de la Politique de confidentialité. Valeurs possibles : • `1` – acceptation de la Politique de confidentialité. • `0` – rejet de la Politique de confidentialité. Le texte de la Politique de confidentialité fait partie du kit de distribution de Kaspersky Endpoint Security. L'acceptation des dispositions de la Politique de confidentialité est une condition indispensable pour installer l'application ou pour la mettre à jour.
	`KSN`	Participation ou non au Kaspersky Security Network (KSN). Si le paramètre n'est pas précisé, Kaspersky Endpoint Security sollicitera la confirmation de la participation à KSN au premier lancement de l'application. Valeurs possibles : • `1` : acceptation de la participation à KSN. • `0` : refus de la participation à KSN (valeur par défaut).

		Le paquet de distribution de Kaspersky Endpoint Security est optimisé pour l'utilisation de Kaspersky Security Network. Si vous avez refusé de participer au Kaspersky Security Network, mettez à jour Kaspersky Endpoint Security directement à l'issue de l'installation.
	`Login`	Définition du nom d'utilisateur pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (module Protection par mot de passe). Le nom d'utilisateur est défini avec les paramètres `Password` et `PasswordArea`. Le nom d'utilisateur par défaut est KLAdmin.
	`Password`	Définition du mot de passe pour l'accès à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security (le mot de passe est défini en même temps que les paramètres `Login` et `PasswordArea`). Si vous avez indiqué un mot de passe, mais que vous n'avez pas défini le nom d'utilisateur à l'aide du paramètre `Login`, le nom d'utilisateur KLAdmin sera utilisé par défaut.
	`PasswordArea`	Définition de la zone d'action du mot de passe pour l'accès à Kaspersky Endpoint Security. Quand l'utilisateur tente d'exécuter une action depuis cette zone, Kaspersky Endpoint Security demande les identifiants de l'utilisateur (paramètres `Identifiant` et `Mot de passe`). Pour indiquer plusieurs valeurs, utilisez le caractère "`;`". Valeurs possibles : • `SET` – modification des paramètres de l'application. • `EXIT` – arrêt de l'application. • `DISPROTECT` – désactivation des modules de protection et arrêt des tâches d'analyse. • `DISPOLICY` – désactivation de la stratégie de Kaspersky Security Center. • `UNINST` – suppression de l'application de l'ordinateur. • `DISCTRL` – désactivation des modules de contrôle. • `REMOVELIC` – suppression de la clé. • `REPORTS` – consultation des rapports.
	`SelfProtection`	Activation ou désactivation du mécanisme de protection de l'installation de l'application. Valeurs possibles : • `1` – activation du mécanisme de protection de l'installation de l'application.

		• `0` – désactivation du mécanisme de protection de l'installation de l'application. Vous pouvez désactiver la protection de l'installation. La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Endpoint Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop).
	`Reboot=1`	Redémarrage automatique de l'ordinateur après l'installation ou la mise à jour de l'application, le cas échéant. Si le paramètre n'est pas défini, le redémarrage automatique de l'ordinateur est interdit. Le démarrage n'est pas requis lors de l'installation de Kaspersky Endpoint Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.
	`AddEnvironment`	Ajout dans la variable système %PATH% du chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security. Valeurs possibles : • `1` – ajouter à la variable système %PATH% le chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security. • `0` – le chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security n'est pas ajouté à la variable système %PATH%.
	`AMPPL`	Activation ou désactivation de la protection du service Kaspersky Endpoint Security à l'aide de la technologie AM-PPL (Antimalware Protected Process Light). Valeurs possibles : • `1` – la protection du service Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est activée. • `0` – la protection du service Kaspersky Endpoint Security à l'aide de la technologie AM-PPL est désactivée.
	`SetupReg`	Activation de l'enregistrement des clés du registre du fichier setup.reg dans le registre. Le paramètre `SetupReg` prend la valeur : setup.reg.

	EnableTraces	Activation ou désactivation du traçage de l'installation de l'application. Kaspersky Endpoint Security enregistre les fichiers de traçage dans le dossier %ProgramData %/Kaspersky Lab. Valeurs possibles : • 1 : le traçage de l'application est activé. • 0 : le traçage de l'installation de l'application est désactivé (valeur par défaut).
	TracesLevel	Niveau de détail du traçage Valeurs possibles : • 100 (critique). Uniquement les messages relatifs aux erreurs irrémédiables. • 200 (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables. • 300 (diagnostique). Messages relatifs à toutes les erreurs et collecte des messages d'avertissement. • 400 (important). Tous les avertissements et messages relatifs aux erreurs normales et irrémédiables et ensemble de messages proposant des informations complémentaires. • 500 (ordinaire). Tous les avertissements et les messages relatifs aux erreurs normales et irrémédiables et messages avec des informations détaillées sur le fonctionnement en mode normal (valeur par défaut). • 600 (bas). Tous les messages possibles.
[Components]	ALL	Installation de tous les modules. Si vous attribuez la valeur 1 au paramètre, tous les modules seront installés, quels que soient les paramètres d'installation des modules séparés.
	MailThreatProtection	Protection contre les menaces par emails.
	WebThreatProtection	Protection contre les menaces Internet.
	AMSI	Fournisseur de protection AMSI.
	HostIntrusionPrevention	Prévention des intrusions.
	BehaviorDetection	Détection comportementale.
	ExploitPrevention	Protection contre les Exploits.
	RemediationEngine	Réparation des actions malicieuses.
	Firewall	Firewall
	NetworkThreatProtection	Protection contre les menaces réseau.
	WebControl	Contrôle Internet.
	DeviceControl	Contrôle des périphériques.
	ApplicationControl	Contrôle des applications.

	`AdaptiveAnomaliesControl`	Contrôle évolutif des anomalies.
	`FileEncryption`	Bibliothèques pour le chiffrement des fichiers.
	`DiskEncryption`	Bibliothèques pour le chiffrement du disque.
	`BadUSBAttackPrevention`	Protection BadUSB.
	`AntiAPT`	Endpoint Sensor.
	`AdminKitConnector`	Connecteur de l'Agent d'administration pour administrer à distance l'application via Kaspersky Security Center. Valeurs possibles : • `1` – installation du module externe de l'Agent d'administration. • `0` – le module externe de l'Agent d'administration n'est pas installé.
`[Tasks]`	`ScanMyComputer`	Tâche d'analyse complète. Valeurs possibles : • `1` – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • `0` – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security.
	`ScanCritical`	Tâche d'analyse rapide. Valeurs possibles : • `1` – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • `0` – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security.
	`Updater`	Tâche de mise à jour. Valeurs possibles : • `1` – la tâche est reprise dans la liste des tâches de Kaspersky Endpoint Security. • `0` – la tâche n'est pas reprise dans la liste des tâches de Kaspersky Endpoint Security.

Mise à jour de la version précédente de l'application

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

- Pour mettre à jour la version précédente jusqu'à Kaspersky Endpoint Security for Windows 11.1.1, il n'est pas obligatoire de supprimer la version précédente de l'application.
- Avant de commencer la mise à jour de l'application, il est conseillé de fermer toutes les applications en cours d'exécution.
- Si les disques durs de l'ordinateur ont été soumis au Chiffrement intégral du disque (FDE), il faudra les déchiffrer tous avant de réaliser la mise à niveau depuis Kaspersky Endpoint Security de la version 10 vers la version 11.0.

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

Vous pouvez mettre à jour les applications suivantes jusqu'à la version Kaspersky Endpoint Security for Windows 11.1.1 :

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (version 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (version 10.2.4.674).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (version 10.2.5.3201).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (version 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (version 10.3.3.275).
- Kaspersky Endpoint Security 11.0.0 for Windows (version 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (version 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.0.1 SF1 (version 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.1.0 (version 11.1.0.15919).

Lors de la mise à jour de Kaspersky Endpoint Security 10 Service Pack 2 for Windows jusque Kaspersky Endpoint Security for Windows 11.1.1, les fichiers placés dans la Sauvegarde et dans la Quarantaine de la version antérieure de l'application sont transférés dans la nouvelle version. Pour les versions de Kaspersky Endpoint Security antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows, le transfert des fichiers placés dans la sauvegarde ou dans la quarantaine dans la version antérieure de l'application n'a pas lieu.

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

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

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

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

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

- Console d'administration (MMC) de Kaspersky Security Center.

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

Déclaration de Kaspersky Security Network

La fenêtre **Kaspersky Security Network** s'ouvre lorsque vous démarrez Kaspersky Endpoint Security pour la première fois après l'installation, si vous n'avez pas confirmé votre accord pour participer à Kaspersky Security Network pendant l'installation. Cette fenêtre contient la Déclaration de Kaspersky Security Network.

Dans la fenêtre **Kaspersky Security Network**, vous pouvez sélectionner l'une des options suivantes :

- **J'accepte les termes du Kaspersky Security Network**.

  Si vous choisissez cette option, Kaspersky Endpoint Security exploite, dans le fonctionnement de ses composants, les informations sur la réputation des fichiers, des sites Internet et des applications fournies par les bases de Kaspersky Security Network.

- **Je refuse les termes du Kaspersky Security Network**.

  Si vous choisissez cette option, Kaspersky Endpoint Security exploite uniquement les informations stockées dans les bases locales de l'application.

  Le kit de distribution de Kaspersky Endpoint Security est optimisé pour l'utilisation de Kaspersky Security Network. Si vous avez refusé de participer au Kaspersky Security Network, mettez à jour Kaspersky Endpoint Security directement à l'issue de l'installation.

Suppression de l'application

Cette section explique comment supprimer Kaspersky Endpoint Security de l'ordinateur.

A propos des méthodes de suppression de l'application

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

Il existe plusieurs méthodes pour supprimer l'application Kaspersky Endpoint Security d'un ordinateur :

- Localement en mode interactif à l'aide de l'Assistant d'installation
- Localement en mode non interactif, depuis la ligne de commande
- à distance à l'aide de la suite logicielle Kaspersky Security Center (les informations sont fournies dans l'aide de Kaspersky Security Center) ;
- à distance via l'éditeur de gestion des stratégies de groupe Microsoft Windows (cf. la documentation qui accompagne le système d'exploitation).

Suppression de l'application à l'aide de l'Assistant d'installation de l'application

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

1. Ouvrez la fenêtre **Panneau de configuration** d'une des méthodes suivantes :
   - Si vous utilisez Windows 7, sélectionnez **Panneau de configuration** dans le menu **Démarrer**.
   - Si vous utilisez Windows 8/Windows 8.1, appuyez sur la combinaison de touches **Win+I** et choisissez l'option **Panneau de configuration**.
   - Si vous utilisez Windows 10, appuyez sur la combinaison de touches **Win+X** et choisissez l'option **Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, choisissez l'option **Applications et modules**.
3. Dans la liste des applications installées, sélectionnez **Kaspersky Endpoint Security for Windows**.
4. Cliquez sur le bouton **Modifier/Désinstaller**.
   L'Assistant d'installation de l'application sera lancé.
5. Dans la fenêtre **Modification, restauration ou suppression de l'application** de l'Assistant d'installation, cliquez sur le bouton **Supprimer**.
6. Suivez les instructions de l'Assistant d'installation.

Étape 1. Enregistrement de données pour une réutilisation

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

Pour enregistrer les données de l'application en vue de leur réutilisation,

cochez les cases en regard des données à enregistrer :

- **Date d'activation** - données qui éliminent le besoin d'activer l'application que vous installez à l'avenir. Il est activé automatiquement sous la licence actuelle, tant que la licence n'a pas expiré au moment de l'installation.
- **Fichiers de la sauvegarde** : fichiers analysés par l'application et placés dans la Sauvegarde.

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

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

- **Paramètres de fonctionnement de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.
- **Stockage local des clés de chiffrement** : données qui garantissent un accès direct aux fichiers et appareils chiffrés avant la suppression de l'application. Après la réinstallation de l'application avec la fonctionnalité de chiffrement des données, l'accès aux fichiers et périphériques chiffrés sera direct.

  Cette case est cochée par défaut.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**. Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Annuler**.

Étape 2. Confirmation de la suppression de l'application

Comme la suppression de l'application met en danger la protection de l'ordinateur, vous êtes invité à confirmer votre intention de supprimer l'application. Pour ce faire, cliquez sur le bouton **Supprimer**.

Pour arrêter la suppression de l'application à tout moment, vous pouvez annuler cette opération en cliquant sur le bouton **Annuler**.

Étape 3. Suppression de l'application. Fin de la suppression

Cette étape de l'Assistant d'installation de l'application correspond à la suppression de l'application de l'ordinateur de l'utilisateur. Attendez la fin de la suppression de l'application.

La suppression de l'application peut requérir le redémarrage du système d'exploitation. Si vous décidez de reporter le redémarrage, la fin de la procédure de suppression de l'application sera reportée jusqu'au moment où le système d'exploitation sera redémarré ou quand l'ordinateur sera éteint et allumé de nouveau.

Suppression de l'application via la ligne de commande

Vous pouvez lancer la suppression de l'application depuis la ligne de commande en exécutant la commande depuis le dossier qui contient le paquet de la distribution. La suppression peut se dérouler en mode interactif ou en mode silencieux (sans lancement de l'Assistant d'installation de l'application).

Pour lancer la suppression de l'application en mode interactif,

dans la ligne de commande, tapez `setup_kes.exe /x` ou `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}`.

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

Pour lancer la suppression de l'application en mode silencieux,

dans la ligne de commande, tapez `setup_kes.exe /s /x` ou `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} /qn`.

La suppression de l'application en mode silencieux démarre (sans lancement de l'Assistant d'installation).

Si l'opération de suppression de l'application est protégée par un mot de passe, il faudra indiquer le nom d'utilisateur et le mot de masse correspondant dans la ligne de commande.

Pour supprimer l'application via la ligne de commande en mode interactif lorsqu'un nom d'utilisateur et un mot de passe doivent être saisis afin de confirmer l'autorisation de suppression/modification/restauration de Kaspersky Endpoint Security,

dans la ligne de commande, tapez `setup_kes.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /x` ou

`msiexec.exe KLLOGIN=<nom d'utilisateur> KLPASSWD=***** /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}`.

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

Pour supprimer l'application via la ligne de commande en mode silencieux lorsqu'un nom d'utilisateur et un mot de passe doivent être saisis afin de confirmer l'autorisation de suppression/modification/restauration de Kaspersky Endpoint Security,

dans la ligne de commande, tapez `setup_kes.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /s /x` ou

`msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} KLLOGIN=<nom d'utilisateur> KLPASSWD=<mot de passe> /qn`.

Suppression des objets et données restants au terme du fonctionnement test de l'Agent d'authentification

Si, pendant le processus de suppression de l'application, Kaspersky Endpoint Security détecte des objets et données restés sur le disque dur système après le fonctionnement test de l'Agent d'authentification, la suppression de l'application est interrompue et ne reprendra que lorsque ces objets et données auront été supprimés.

Après le fonctionnement test de l'Agent d'authentification, les objets et données peuvent rester sur le disque dur système uniquement dans les situations d'exception. Par exemple, si après la mise en œuvre de la stratégie de Kaspersky Security Center selon les paramètres de chiffrement, l'ordinateur n'a jamais été redémarré ou encore après le fonctionnement test de l'Agent d'authentification.

Vous pouvez supprimer les objets et les données demeurés sur le disque dur système après le fonctionnement test de l'Agent d'authentification d'une des deux manières suivantes :

- avec la stratégie du Kaspersky Security Center ;
- à l'aide de l'utilitaire de restauration.

Pour supprimer les objets et données restants au terme du fonctionnement test de l'Agent d'authentification à l'aide des stratégies de Kaspersky Security Center, procédez comme suit :

1. Appliquez à l'ordinateur la stratégie de Kaspersky Security Center avec les paramètres établis pour déchiffrer tous les disques durs de l'ordinateur.
2. Lancez Kaspersky Endpoint Security.

Pour supprimer les données sur l'incompatibilité de l'application avec l'Agent d'authentification,

saisissez la commande `avp pbatestreset` dans la ligne de commande.

L'installation des modules de chiffrement est requise pour exécuter la commande `avp pbatestreset`.

Activation de l'application

Pour pouvoir utiliser les fonctions de l'application et les services complémentaires associés à l'application, il faut activer l'application.

Si vous n'avez pas activé l'application durant l'installation, vous pouvez le faire plus tard. Les notifications de Kaspersky Endpoint Security dans la zone de notification de la barre d'état vous rappellent la nécessité d'activer l'application.

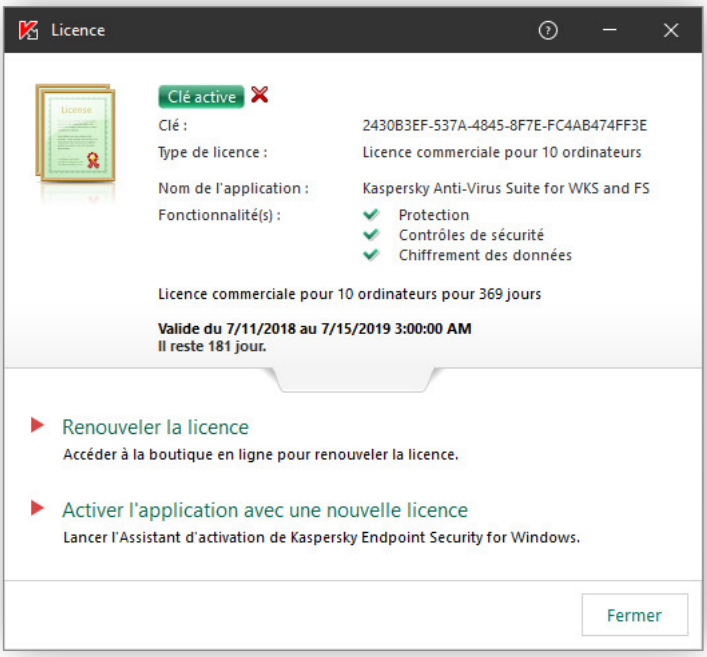
Cette section fournit des informations sur l'activation de l'application et d'autres instructions liées à la licence.

Consultation des informations relatives à la licence

Pour consulter les informations sur la licence,

cliquez sur / sous la fenêtre principale de l'application.

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



Fenêtre Licence

La fenêtre **Licence** contient les informations suivantes :

- **État de la clé**. Il peut y avoir plusieurs clés sur l'ordinateur. Une clé peut être active ou complémentaire. L'application ne peut compter qu'une seule clé active. Une clé supplémentaire peut devenir active uniquement lorsque la clé active expire ou si vous avez supprimé la clé active à l'aide du bouton ×.
- **Clé**. La *clé* est une succession unique de caractères alphanumériques, formée au départ du code d'activation ou du fichier clé.
- **Type de licence**. Les types de licence suivants sont prévus : évaluation et commercial.
- **Nom de l'application**. Le nom complet du produit de Kaspersky acheté.
- **Fonctionnalité(s)**. Les fonctions de l'application accessibles sous votre licence. Les fonctions suivantes sont prévues : Protection, Contrôles de sécurité, Chiffrement des données, Endpoint Sensor et d'autres. La liste des fonctions accessibles figure également dans le certificat de licence.
- **Informations complémentaires sur la licence**. Le type de licence, la quantité d'ordinateurs couverts par la licence, la date de début et la date et l'heure de fin de la durée de validité de la licence(seulement pour la clé active).

  L'heure de la fin de la durée de validité de la licence est exprimée dans le fuseau horaire configuré dans le système d'exploitation.

Les actions suivantes sont également disponibles dans la fenêtre Licence :

- **Acheter une licence** / **Renouveler la licence**. Ouvre le site Internet de la boutique en ligne de Kaspersky où vous pouvez acheter une licence ou renouveler la licence existante. Pour ce faire, il faut saisir les données de l'entreprise et payer la commande.
- **Activer l'application avec une nouvelle licence**. L'Assistant d'activation de l'application est lancé. L'assistant permet d'ajouter une clé avec l'aide du code d'activation ou le fichier clé. L'assistant d'activation de l'application

permet d'ajouter une clé active et une seule clé complémentaire.

Achat d'une licence

Vous pouvez acheter une licence après avoir installé l'application. L'achat de la licence vous permet de recevoir un code d'activation ou un fichier clé pour activer l'application.

Pour acheter une licence, procédez comme suit :

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

   La fenêtre **Licence** s'ouvre.

2. Dans la fenêtre **Licence**, réalisez une des opérations suivantes :

   - Cliquez sur le bouton **Acheter une licence** si aucune clé n'a été installée ou si une clé pour licence d'évaluation a été installée.
   - Cliquez sur le bouton **Renouveler la licence** si vous avez ajouté une clé pour licence commerciale.

   Le site Internet du magasin en ligne de Kaspersky où vous pouvez acheter la licence s'ouvre.

Renouvellement de l'abonnement

Si vous utilisez l'application par abonnement, Kaspersky Endpoint Security se connecte automatiquement au serveur d'activation à des intervalles définis jusqu'à la fin de l'abonnement.

Si vous utilisez l'application sous un abonnement illimité, Kaspersky Endpoint Security vérifie automatiquement en arrière-plan la présence éventuelle d'une clé mise à jour sur le serveur d'activation. Si la clé se trouve sur le serveur d'activation, l'application l'ajoute en mode de remplacement de la clé précédente. C'est ainsi que l'abonnement illimité à Kaspersky Endpoint Security se renouvelle sans votre participation.

Si vous utilisez l'application avec un abonnement limité, Kaspersky Endpoint Security vous préviendra le jour de l'expiration de l'abonnement ou de la période de grâce après l'expiration de l'abonnement et les tentatives de renouvellement automatique seront interrompues. Le comportement de Kaspersky Endpoint Security dans ce cas est identique à celui observé à l'échéance de la licence commerciale de l'application : l'application fonctionne sans mises à jour et Kaspersky Security Network est inaccessible.

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

Vous pouvez mettre à jour l'état de l'abonnement manuellement dans la fenêtre **Licence**. Cette opération peut être requise si l'abonnement est renouvelé après l'expiration de la période de grâce et que l'application a arrêté de mettre à jour automatiquement l'état de l'abonnement.

Accès au site Internet du fournisseur de services

Pour accéder au site Internet du fournisseur de services à partir de l'interface de l'application, procédez comme suit :

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

La fenêtre **Licence** s'ouvre.

2. Dans la fenêtre **Licence**, cliquez sur le bouton **Contacter le fournisseur de l'abonnement**.

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

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

1. Cliquez sur le bouton / situé dans la partie inférieure de la fenêtre principale de l'application.
   La fenêtre **Licence** s'ouvre.
2. Dans la fenêtre **Licence** qui s'ouvre, cliquez sur le bouton **Activer l'application avec une nouvelle licence**.
   L'Assistant d'activation de l'application sera lancé.
3. Suivez les instructions de l'Assistant d'activation de l'application.

Vous trouvez de plus amples informations sur la procédure d'activation de l'application dans la section consacrée à l'Assistant de configuration initiale de l'application.

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

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

tapez `avp.com license /add <code d'activation ou fichier clé> /password=<mot de passe>` dans la ligne de commande.

Interface de l'application

Cette section présente les éléments fondamentaux de l'interface de l'application.

Icône de l'application dans la zone de notification

Dès que Kaspersky Endpoint Security a été installé, l'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows.

L'icône de l'application remplit les fonctions suivantes :

- elle indique le fonctionnement de l'application ;
- elle permet d'accéder au menu contextuel de l'icône de l'application et à la fenêtre principale de l'application.

Indication du fonctionnement de l'application

L'icône de l'application indique l'état de fonctionnement de l'application :

- L'icône indique que tous les modules de protection de l'application sont activés.
- L'icône signifie que des événements importants nécessitant votre attention se sont produits lors du fonctionnement de Kaspersky Endpoint Security. Par exemple, le module Protection contre les fichiers malicieux est désactivé ou les bases de l'application sont dépassées.
- L'icône indique que des événements critiques se sont produits durant le fonctionnement de Kaspersky Endpoint Security. Par exemple, échec d'un module, bases de l'application endommagées.

Menu contextuel de l'icône de l'application

Le menu contextuel de l'icône de l'application reprend les options suivantes :

- **Kaspersky Endpoint Security for Windows**. Ouvre la fenêtre principale de l'application. Cette fenêtre permet de gérer le fonctionnement des modules et des tâches de l'application, et de consulter les statistiques relatives aux fichiers traités et aux menaces détectées.
- **Configuration**. Ouvre la fenêtre **Configuration**. L'onglet **Paramètres** vous permet de modifier les paramètres par défaut de l'application.
- **Suspension de la protection et du contrôle** / **Rétablissement de la protection et du contrôle**. Suspend temporairement ou rétablit le fonctionnement des modules de protection et des modules de contrôle de l'application. Cette option du menu contextuel n'a aucune influence sur l'exécution de la mise à jour et des analyses. Elle est uniquement accessible lorsque la stratégie de Kaspersky Security Center est désactivée.

  Kaspersky Security Network est utilisé dans le cadre du fonctionnement de Kaspersky Endpoint Security sans tenir compte de la suspension/de la reprise du fonctionnement des modules de protection et des modules de contrôle.

- **Désactivation de la stratégie** / **Activation de la stratégie**. Désactive ou active la stratégie de Kaspersky Security Center. Cette option du menu contextuel est accessible si l'ordinateur doté de Kaspersky Endpoint Security fonctionne dans le cadre d'une stratégie et que le mot de passe pour la désactivation d'une stratégie de Kaspersky Security Center a été défini dans les paramètres de la stratégie.
- **À propos de l'application**. Ouvre une fenêtre contenant des informations sur l'application.
- **Quitter**. Entraîne l'arrêt de Kaspersky Endpoint Security. Si vous choisissez cette option du menu contextuel, l'application est déchargée de la mémoire vive de l'ordinateur.

Menu contextuel de l'icône de l'application

Pour ouvrir le menu contextuel de l'icône de l'application, placez le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows, puis cliquez avec le bouton droit de la souris.

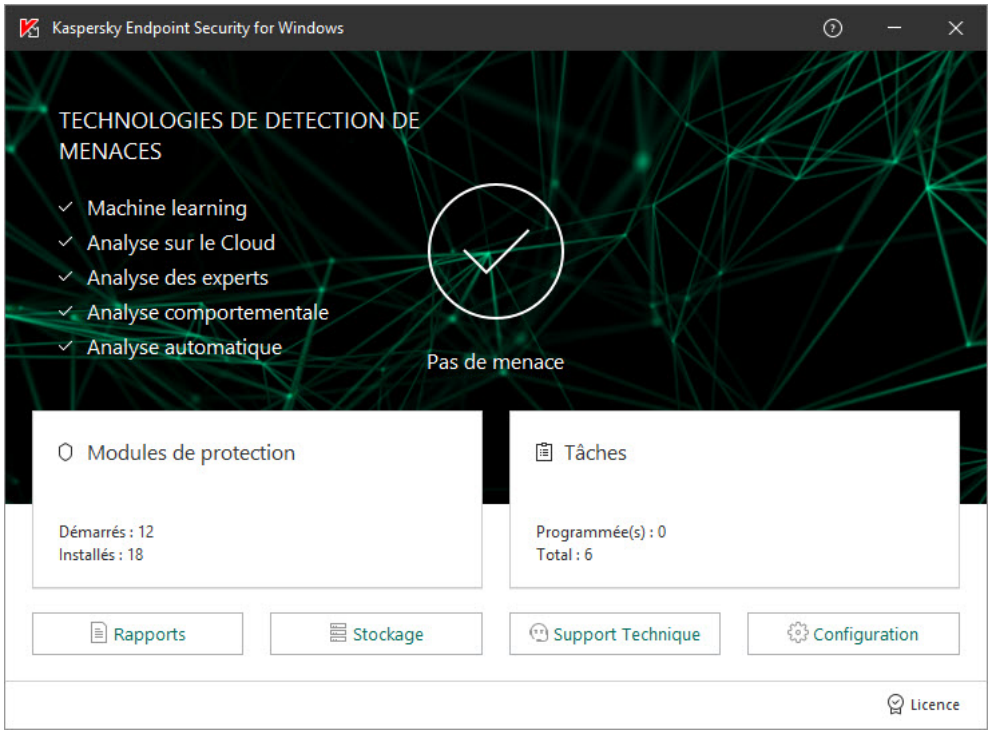
Fenêtre principale de l'application

La fenêtre principale de Kaspersky Endpoint Security réunit les éléments de l'interface qui vous permettent d'accéder aux principales fonctionnalités de l'application.

La fenêtre principale de l'application contient les éléments suivants :

- Lien **Kaspersky Endpoint Security for Windows**. Cliquez sur ce lien pour ouvrir la fenêtre **À propos de l'application** qui contient des informations sur la version de l'application.
- Bouton . Cliquez sur ce bouton pour accéder à l'aide de Kaspersky Endpoint Security.
- Groupe **Technologies de détection des menaces** Le groupe contient les informations suivantes :
  - La partie gauche du groupe affiche la liste des technologies de détection de menaces. A droite du nom de chacune de ces technologies de détection de menaces, vous voyez le nombre de menaces détectées.
  - Un des messages suivants s'affiche au centre du groupe en fonction de la présence de menaces actives :
    - **Aucune menace**. Si ce message apparaît, quand vous cliquez sur le groupe **Technologies de détection des menaces**, vous ouvrez la fenêtre **Technologies de détection des menaces** qui contient une brève description des technologies de détection des menaces ainsi que l'état et des statistiques générales de l'infrastructure des services Cloud Kaspersky Security Network.
    - **N menaces actives**. Si ce message apparaît, quand vous cliquez sur le groupe **Technologies de détection des menaces**, vous ouvrez la fenêtre **Menaces actives** qui reprend une liste des événements liés aux fichiers infectés qui, pour une raison ou l'autre, n'ont pas été traités.
- Groupe **Modules de protection**. Cliquez sur ce groupe pour ouvrir la fenêtre **Modules de protection**. Cette fenêtre permet de consulter l'état du fonctionnement des modules installés. Cette fenêtre permet également d'ouvrir pour n'importe quel module installé, à l'exception des modules de chiffrement, une sous-section dans la fenêtre **Paramètres** qui contient les paramètres de ce module.
- Groupe **Tâches**. Cliquez sur ce groupe pour ouvrir la fenêtre **Tâches**. Cette fenêtre permet de gérer les tâches de Kaspersky Endpoint Security qui garantissent l'actualité des bases et des modules de l'application, la recherche de virus et d'autres programmes dangereux et la vérification de l'intégrité.
- Bouton **Rapports**. Cliquez sur ce bouton pour ouvrir la fenêtre **Rapports** qui contient les informations relatives aux événements survenus dans le cadre du fonctionnement de l'application dans son ensemble, du fonctionnement de certains modules et de l'exécution de tâches.
- Bouton **Stockages**. Bouton qui ouvre la fenêtre **Sauvegarde**. Cette fenêtre permet de consulter la liste des copies de fichiers infectés qui ont été supprimés lors du fonctionnement de l'application.
- Bouton **Support Technique**. Cliquez sur ce bouton pour ouvrir la fenêtre **Support Technique** contenant les informations relatives au système d'exploitation, à la version actuelle de Kaspersky Endpoint Security et des liens vers des ressources d'informations de Kaspersky.
- Bouton **Configuration**. Cliquez sur ce bouton pour ouvrir la fenêtre **Configuration** qui permet de modifier les paramètres de l'application définis par défaut.
- Bouton / / . Cliquez sur le bouton pour ouvrir la fenêtre **Événements** contenant les informations sur les mises à jour disponibles, ainsi que les demandes d'accès aux fichiers chiffrés et aux appareils.

- Lien **Licence**. Cliquez sur ce lien pour ouvrir la fenêtre **Licence** contenant les informations relatives à la licence active.



Fenêtre principale de l'application

Pour ouvrir la fenêtre principale de Kaspersky Endpoint Security, réalisez une des opérations suivantes :

- Cliquez sur l'icône de l'application dans la zone de notification de la barre de tâches de Microsoft Windows.
- Sélectionnez **Kaspersky Endpoint Security for Windows** dans le menu contextuel de l'icône de l'application.

Renouvellement de la licence

Quand la durée de validité d'une licence est sur le point d'expirer, vous pouvez la renouveler. Ainsi, la protection de l'ordinateur ne sera pas interrompue entre la fin de la validité de la licence active et l'activation de l'application à l'aide d'une nouvelle licence.

Pour renouveler la licence, procédez comme suit :

1. Recevez un nouveau code d'activation d'application ou un fichier clé.
2. Ajoutez une clé supplémentaire avec le code d'activation ou le fichier clé que vous avez reçu.

   Ceci a pour effet d'ajouter une clé supplémentaire. Elle est activée à l'expiration de la licence.

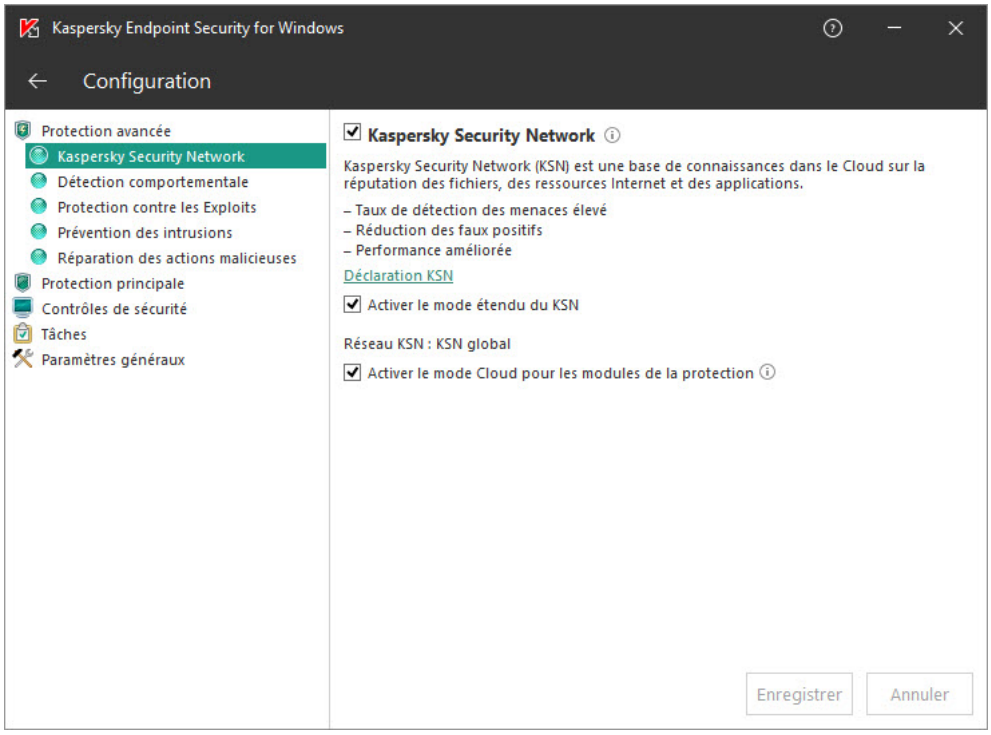
La mise à jour de la clé depuis le statut complémentaire vers le statut actif peut être effectuée avec un retard aléatoire lié à la diffusion de la charge sur les serveurs d'activation de Kaspersky.

Fenêtre Configuration des paramètres de l'application

La fenêtre de configuration des paramètres de Kaspersky Endpoint Security permet de configurer les paramètres de fonctionnement de l'application dans son ensemble, de ses modules distincts, des rapports et des stockages, des tâches d'analyse et de la tâche de mise à jour. Elle permet également de configurer la communication avec les serveurs de Kaspersky Security Network.

La fenêtre de configuration des paramètres de l'application comprend deux parties (cf. ill. ci-après) :

- la partie gauche contient les modules de l'application, les tâches et la section des paramètres complémentaires composée de plusieurs sous-sections ;
- La partie droite contient les éléments d'administration qui permettent de configurer les paramètres du module ou les tâches choisies dans la partie gauche de la fenêtre, ainsi que les paramètres complémentaires.



Fenêtre Configuration des paramètres de l'application

Pour ouvrir la fenêtre de configuration des paramètres de l'application, réalisez une des opérations suivantes :

- Dans la fenêtre principale de l'application, sélectionnez l'onglet **Paramètres**.
- Dans le menu contextuel de l'icône de l'application, sélectionnez **Paramètres**.

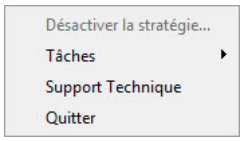
Interface de l'application simplifiée

Si l'ordinateur client doté de l'application Kaspersky Endpoint Security est soumis à une stratégie de Kaspersky Security Center qui prévoit l'affichage de l'interface tronquée de l'application, la fenêtre principale de l'application n'est pas accessible sur ce poste client. D'un clic droit, l'utilisateur peut ouvrir le menu contextuel de l'icône de Kaspersky Endpoint Security (cf. ill. ci-dessous) qui contient les options suivantes :

- **Désactivation de la stratégie**. Désactive la stratégie de Kaspersky Security Center sur l'ordinateur client doté de l'application Kaspersky Endpoint Security. De plus, l'application sollicite le mot de passe d'accès à Kaspersky Endpoint Security (mot de passe du compte utilisateur ou mot de passe temporaire). Après la désactivation de la stratégie, l'utilisateur de l'ordinateur client peut accéder à tous les paramètres de l'application, y compris les paramètres accompagnés d'un cadenas (🔒) dans la stratégie. L'utilisateur a également accès au menu contextuel complet de l'application au lieu de son interface simplifiée. Cette option du menu contextuel est

accessible si l'ordinateur fonctionne dans le cadre d'une stratégie et que le mot de passe d'accès à Kaspersky Endpoint Security a été défini dans les paramètres de la stratégie et que l'accès aux opérations de désactivation d'une stratégie de Kaspersky Security Center est limité.

- **Tâches**. Liste déroulante contenant les éléments suivants :
  - **Mise à jour**.
  - **Restauration de la dernière mise à jour**.
  - **Analyse complète**.
  - **Analyse personnalisée**.
  - **Analyse des zones critiques**.
  - **Vérification de l'intégrité**.
- **Support Technique**. Ouverture de la fenêtre **Support Technique** qui contient les informations requises pour contacter le Support Technique de Kaspersky.
- **Quitter**. Arrêt du fonctionnement de Kaspersky Endpoint Security.



Menu contextuel de l'icône de l'application lors de l'affichage de l'interface simplifiée de l'application

Lancement et arrêt de l'application

Cette section explique comment configurer le lancement automatique de l'application, comment lancer et arrêter l'application manuellement et comment suspendre et rétablir le fonctionnement des modules de protection et des modules de contrôle.

Activation et désactivation du lancement automatique de l'application

Le concept de lancement automatique de l'application désigne le lancement de Kaspersky Endpoint Security sans intervention de l'utilisateur après le démarrage du système d'exploitation. Cette option de lancement de l'application est définie par défaut.

La première fois, l'application Kaspersky Endpoint Security est lancée automatiquement après son installation.

Le chargement des bases antivirus de Kaspersky Endpoint Security après le chargement du système d'exploitation peut durer jusqu'à deux minutes en fonction des performances (capacités techniques) de l'ordinateur. Pendant cette période, le niveau de la protection de l'ordinateur est réduit. Le chargement des bases antivirus au lancement de l'application Kaspersky Endpoint Security quand le système d'exploitation est déjà chargé n'entraîne pas de réduction du niveau de la protection de l'ordinateur.

Pour activer ou désactiver le lancement automatique de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.
3. Exécutez une des actions suivantes :
   - Si vous voulez activer le lancement automatique de l'application, cochez la case **Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur**.
   - Si vous voulez désactiver le lancement automatique de l'application, décochez la case **Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement et arrêt manuels de l'application

Les experts de Kaspersky déconseillent de quitter Kaspersky Endpoint Security car cela exposerait votre ordinateur et vos données à des risques. Le cas échéant, vous pouvez suspendre la protection de l'ordinateur pendant l'intervalle que vous souhaitez, sans quitter l'application.

Le lancement manuel de Kaspersky Endpoint Security s'impose si vous avez désactivé le lancement automatique de l'application.

Pour démarrer l'application manuellement,

sélectionnez dans le menu **Démarrer** l'option **Applications** → **Kaspersky Endpoint Security for Windows**.

Pour arrêter l'application manuellement, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Sélectionnez **Quitter** dans le menu contextuel.

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

Les experts de Kaspersky déconseillent de quitter Kaspersky Endpoint Security car cela exposerait votre ordinateur et vos données à des risques. Le cas échéant, vous pouvez suspendre la protection de l'ordinateur pendant l'intervalle que vous souhaitez, sans quitter l'application.

Pour quitter l'application via la ligne de commande, il faut décocher la case **Désactiver la gestion externe des services systèmes**.

Vous pouvez lancer la suppression de l'application au départ de la ligne de commande.

Pour démarrer ou quitter l'application via la ligne de commande, il faut le fichier klpsm.exe qui figure dans le kit de distribution de Kaspersky Endpoint Security.

Pour lancer l'application, procédez comme suit :

Saisissez dans la ligne de commande klpsm.exe start_avp_service.

Pour arrêter l'application,

Saisissez dans la ligne de commande klpsm.exe stop_avp_service.

Suspension et rétablissement de la protection et du contrôle de l'ordinateur

Par suspension de la protection de l'ordinateur et du contrôle, il faut entendre la désactivation pendant un certain temps de tous les modules de protection et de tous les modules de contrôle de Kaspersky Endpoint Security.

L'état de l'application est illustré par l'icône de l'application dans la zone de notifications de la barre de tâches :

- L'icône signale la suspension de la protection et du contrôle de l'ordinateur.
- L'icône indique que la protection et le contrôle de l'ordinateur sont désactivés.

La suspension et le rétablissement de la protection de l'ordinateur et du contrôle n'ont aucune influence sur l'exécution des tâches d'analyse et de mise à jour de l'application.

Si des connexions réseau étaient ouvertes au moment de la suspension et du rétablissement du contrôle de l'ordinateur, un message s'affiche pour indiquer l'interruption de ces connexions.

Pour rétablir la protection et le contrôle de l'ordinateur, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Sélectionnez **Suspension de la protection et du contrôle** dans le menu contextuel.

   La fenêtre **Suspension de la protection** s'ouvre.
3. Choisissez l'une des options suivantes :

   - **Suspendre pendant la période indiquée** : la protection de l'ordinateur et le contrôle seront activés à l'issue de l'intervalle de temps défini dans la liste déroulante en dessous.
   - **Suspendre jusqu'au redémarrage** : la protection de l'ordinateur et le contrôle sont activés après le redémarrage de l'application ou du système d'exploitation. Pour pouvoir utiliser cette fonctionnalité, le lancement automatique de l'application doit être activé.
   - **Suspendre** : la protection et le contrôle de l'ordinateur sont activés quand vous décidez de les rétablir.
4. Si vous aviez choisi l'option **Suspendre pendant la période indiquée** à l'étape précédente, choisissez l'intervalle nécessaire dans la liste déroulante.

Pour rétablir la protection de l'ordinateur et le contrôle, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

2. Sélectionnez **Rétablissement de la protection et du contrôle** dans le menu contextuel.

Vous pouvez rétablir la protection et le contrôle de l'ordinateur à n'importe quel moment, quelle que soit l'option de suspension de la protection et du contrôle de l'ordinateur vous aviez choisi auparavant.

Kaspersky Security Network

Cette section contient des informations relatives à la participation au Kaspersky Security Network et explique comment activer ou désactiver l'utilisation de Kaspersky Security Network.

A propos de la participation au Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. *Kaspersky Security Network* est conçu pour recevoir ces données.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

En fonction de l'emplacement de l'infrastructure, on distingue le KSN global (infrastructure hébergée sur les serveurs de Kaspersky) et le KSN privé.

Après la modification de la licence d'utilisation du KSN local, il faut transmettre les informations relatives à la nouvelle clé au fournisseur de service. Si cette opération n'est pas effectuée, l'échange d'informations avec le KSN privé n'est pas possible.

La participation des utilisateurs à Kaspersky Security Network permet à Kaspersky de récupérer efficacement des informations sur les types et les sources de menaces, de développer des moyens de neutralisation de celles-ci et de réduire le nombre de faux positifs pour les modules de l'application.

Pendant l'utilisation du mode étendu du KSN, l'application envoie automatiquement à KSN les informations statistiques obtenues lors de son fonctionnement. L'application peut également envoyer à Kaspersky des fichiers (ou partie de fichier) pour vérification complémentaire. Il s'agit de fichiers que des individus malintentionnés pourraient utiliser pour nuire à l'ordinateur ou aux données.

Vous pouvez lire des informations plus détaillées sur l'envoi à Kaspersky, le stockage et la destruction des informations statistiques obtenues lors de l'utilisation de KSN dans la Déclaration de Kaspersky Security Network et sur le site Internet de Kaspersky. Le fichier ksn_<ID de la langue>.txt qui contient la Déclaration de Kaspersky Security Network figure dans le kit de distribution.

Pour réduire la charge sur les serveurs de KSN, les spécialistes de Kaspersky peuvent lancer des bases antivirus de l'application qui désactivent temporairement ou limitent en partie la communication dans Kaspersky Security Network. Dans ce cas, l'état de la connexion à KSN apparaît comme *Activé avec des restrictions*.

Les ordinateurs des utilisateurs qui sont administrés par le serveur d'administration Kaspersky Security Center peuvent interagir avec KSN à l'aide du service KSN Proxy.

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur de l'utilisateur peut interroger KSN et transmettre à KSN des informations, même s'il n'a pas d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Pour en savoir plus sur le service KSN Proxy *consultez l'* *aide de Kaspersky Security Center* .

Les paramètres du service KSN Proxy peuvent être configurés dans les propriétés de la stratégie de *Kaspersky Security Center*.

L'utilisation de Kaspersky Security Network est volontaire. L'application propose d'utiliser le KSN pendant la configuration initiale de l'application. Vous pouvez commencer à utiliser le KSN ou arrêter de l'utiliser à n'importe quel moment.

A propos de la collecte des données dans le cadre de l'utilisation de Kaspersky Security Network

En acceptant la Déclaration de Kaspersky Security Network, vous acceptez de transmettre automatiquement les informations suivantes :

- Si la case **Kaspersky Security Network** est cochée alors que la case **Activer le mode étendu du KSN** est décochée, les informations suivantes sont transmises :
  - informations relatives à la mise à jour de la configuration de KSN : identifiant de la configuration active, identifiant de la configuration reçue, code d'erreur de mise à jour de la configuration ;
  - informations sur les fichiers et les adresses Internet analysés : sommes de contrôle du fichier analysé (MD5, SHA2-256, SHA1) et profils de fichier (MD5), taille du profil, type de menace détectée et son nom conformément à la classification du Titulaire des droits, identifiant des bases antivirus, adresse Internet pour laquelle la réputation est sollicitée, adresse Internet depuis laquelle l'accès à l'adresse Internet à analyser a eu lieu, identifiant du protocole de connexion et numéro du port utilisé ;
  - identifiant de la tâche d'analyse dont l'exécution a détecté la menace ;
  - informations sur les certificats numériques utilisés requises pour vérifier leur authenticité : sommes de contrôle du certificat (SHA256) utilisé pour signer l'objet à analyser, clé publique du certificat ;
  - identificateur du composant de l'application qui exécute l'analyse ;
  - identificateurs des bases antivirus et enregistrements dans les bases antivirus ;
  - informations relatives à l'application du Titulaire des droits : type de l'application Kaspersky Endpoint Security, version du protocole de connexion aux services de Kaspersky utilisé ;
  - informations relatives à l'activation de l'application sur l'ordinateur ; en-tête signé du ticket du service d'activation (identificateur du centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identificateur unique du ticket, version du ticket, état de la licence, date et heure du début de fin de validité du ticket, identificateur unique de licence, version de la

licence), identificateur du certificat utilisé pour signer les en-têtes du ticket, somme de contrôle (MD5) du fichier clé.

- Si en plus de la case **Kaspersky Security Network** vous cochez la case **Activer le mode étendu du KSN**, les informations suivantes sont envoyées en plus :

  - informations sur les résultats du classement en catégories des ressources Internet sollicitées. Celui contient l'adresse Internet à analyser et l'adresse IP de l'hôte, la version du composant de l'application qui réalise le classement en catégories, le mode de classement utilisé et la sélection de catégories définies pour la ressource Internet ;

  - informations sur l'application installée sur l'Ordinateur : nom de l'application et son éditeur, clés de registre utilisée et leurs valeurs, informations relatives aux fichiers des modules de l'application installée (sommes de contrôle (MD5, SHA2-256, SHA1), nom, chemin du fichier sur l'Ordinateur, taille, version et signature numérique) ;

  - informations sur l'état de la protection antivirus de l'Ordinateur : versions, dates et heures d'émission des bases antivirus utilisées, identificateur de la tâche qui réalise l'analyse ;

  - Informations sur les fichiers téléchargés par l'Utilisateur : URL et adresses IP depuis lesquelles le téléchargement a eu lieu et adresse Internet de la page de transfert à la page de téléchargement du fichier, identifiant du protocole de téléchargement et numéro du port de connexion, indice de caractère malveillant des adresses, attributs et taille du fichier ainsi que ses sommes de contrôle (MD5, SHA2-256, SHA1), informations sur le processus qui a chargé le fichier (sommes de contrôle (MD5, SHA2-256, SHA1), date et heure de création et d'association, indice de présence dans le démarrage automatique, attributs, nom des compacteurs, informations relatives à la signature, indice du fichier exécutable, identifiant du format, type du compte utilisateur sous lequel le processus a été lancé), informations sur le fichier du processus (nom, chemin du fichier et taille), nom du fichier, chemin d'accès au fichier sur l'Ordinateur, signature numérique du fichier et informations sur l'exécution de la signature, adresse Internet où a eu lieu la détection, nombre de scripts suspects sur la page considérée comme suspecte ou malveillante ;

  - informations sur les applications lancées et leurs modules : données sur les processus exécutés dans le système (identifiant du processus dans le système (PID), nom du processus, données relatives au compte utilisateur sous lequel le processus a été lancé, données relatives à l'application et à la commande qui a lancé le processus, ainsi que l'indice de confiance de l'application ou du processus, chemin d'accès complet aux fichiers du processus et leur somme de contrôle (MD5, SHA2-256, SHA1), ligne de commande de lancement, niveau d'intégrité du processus, description du produit auquel se rapporte le processus (nom du produit et données relatives à l'éditeur), données relatives aux certificats numériques utilisés et informations indispensables à la vérification de leur authenticité ou données relatives à l'absence de signature numérique du fichier), informations sur les modules chargés dans le processus (nom, taille, type, date de création, attributs, sommes de contrôle (MD5, SHA2-256, SHA1), chemin d'accès), informations de l'en-tête des fichiers PE, nom du compacteur (si le fichier était compacté) ;

  - informations relatives à l'ensemble des objets et actions potentiellement malveillants : nom de l'objet détecté et chemin d'accès complet à l'objet sur l'Ordinateur, sommes de contrôle des fichiers traités (MD5, SHA2-256, SHA1), date et heure de la détection, nom et taille des fichiers traités et chemin d'accès à ceux-ci, code du modèle de chemin d'accès, indice de fichier exécutable, identification de l'objet en tant que conteneur ou non, nom du compacteur (si le fichier a été compacté), code du type de fichier, identifiant du format de fichier, identificateurs des bases antivirus et des enregistrements dans ces bases sur la base desquels l'application a été mise en évidence, indice d'objet potentiellement malveillant, nom de la menace détectée conformément à la classification du Titulaire des droits, état et mode de détection, cause de l'inclusion dans le contexte à analyser et position du fichier dans le contexte, sommes de contrôle (MD5, SHA2-256, SHA1), nom et attributs du fichier exécutable de l'application via laquelle le message infecté ou le lien est arrivé, adresses IP(IPv4 et IPv6) de l'hôte de l'objet bloqué, entropie du fichier, indice de la présence du fichier dans le démarrage automatique, heure de la première détection du fichier dans le système, nombre de lancements du fichier depuis le dernier envoi des statistiques, type de compilateur, informations relatives au nom, aux sommes de contrôle (MD5, SHA2-256, SHA1) et à la taille du client de messagerie via lequel l'objet malveillant a été reçu, identifiant de la tâche de l'application qui a réalisé l'analyse, indice de vérification de la réputation ou signature du fichier, résultats de l'analyse statistique du contenu de l'objet,

résultats du traitement du fichier, profils de l'objet et taille du profil en octets, caractéristiques techniques des technologies de détection appliquée ;

- informations sur les objets analysés : groupe de confiance attribué dans lequel le fichier est placé et/ou hors duquel il est déplacé, cause du placement du fichier dans cette catégorie, identifiant de la catégorie, informations relatives à la source des catégories et à la version des bases de catégories, indice de la présence dans le fichier d'un certificat de confiance, nom de l'éditeur du fichier, version du fichier, nom et version de l'application dont le fichier fait partie ;

- informations sur les vulnérabilités détectées : identifiant de la vulnérabilité dans la base des vulnérabilités, classe du danger de la vulnérabilité ;

- informations sur l'exécution de l'émulation du fichier exécutable : taille du fichier et ses sommes de contrôle (MD5, SHA2-256, SHA1), version du composant d'émulation, profondeur de l'émulation, vecteur des caractéristiques des blocs logiques et des fonctions à l'intérieur des blocs logiques obtenu lors de l'émulation, données issues de la structure de l'en-tête PE du fichier exécutable ;

- Informations sur les attaques réseau : adresses IP de l'ordinateur attaquant (IPv4 et IPv6), numéro de port de l'Ordinateur ciblé par l'attaque réseau, identifiant du protocole du paquet IP dans lequel l'attaque a été enregistrée, cible de l'attaque (nom de l'organisation, le site Internet), l'indicateur de réaction à l'attaque, la pondération de l'attaque, la valeur du niveau de confiance ;

- informations relatives aux attaques liées à la substitution de ressources réseau, DNS et adresses IP (IPv4 ou IPv6) des sites Internet visités ;

- adresses Internet et adresses IP (IPv4 ou IPv6) de la ressource Internet sollicitée, informations relatives au fichier et/ou au client Internet qui a contacté la ressource Internet : nom, taille, sommes de contrôle (MD5, SHA2-256, SHA1) du fichier, chemin d'accès complet à celui-ci et code du modèle de chemin d'accès, résultat de la vérification de sa signature numérique et son état dans KSN ;

- informations sur l'exécution du retour à l'état antérieur aux actions du programme malveillant : données relatives au fichier, activité soumise à la tâche (nom du fichier, son chemin d'accès complet, sa taille et les sommes de contrôle (MD5, SHA2-256, SHA1)), données sur les actions réussies ou non au niveau de la suppression, du changement de nom et de la copie des fichiers et de la restauration des valeurs dans le registre (nom des clés du registre et leurs valeurs), informations sur les fichiers système modifiés par le programme malveillant avant et après le retour à l'état antérieur ;

- informations sur les exclusions pour les règles du module Contrôle évolutif des anomalies : identificateur et état de la règle déclenchée, action de l'application lors du déclenchement de la règle, type de compte utilisateur sous lequel le processus ou le flux exécute les actions suspectes, informations sur le processus qui exécute les actions suspectes (identificateur du script ou nom du fichier du processus, chemin d'accès complet du processus, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du processus), informations sur l'objet au nom duquel les actions suspectes ont été réalisées et sur l'objet sur lequel les actions suspectes ont été réalisées (nom de la clé du registre ou nom du fichier, chemin du fichier complet, code du modèle de chemin et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier) ;

- informations relatives aux modules de l'application à charger : nom, taille et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du module, son chemin d'accès complet et code du modèle de chemin d'accès, paramètres de la signature numérique du fichier du module, date et heure de création de la signature, nom du sujet et de l'organisation qui ont signé le fichier du module, identifiant du processus dans lequel le module a été chargé, nom du fournisseur du module, numéro de position du module dans la file de chargement ;

- informations sur les exclusions pour les règles du module Contrôle évolutif des anomalies : date et heure de début et de fin de la période de collecte des statistiques, informations sur la qualité des requêtes et de la connexion avec chacun des services de KSN utilisés (identificateur du service KSN, nom de requêtes réussies, nombre de requêtes avec des réponses issues du cache, nombre de requêtes en échec (problèmes de réseau, désactivation de KSN dans les paramètres de l'application, parcours incorrect), répartition dans le temps des requêtes qui ont réussi, répartition dans le temps des requêtes qui ont été annulées, répartition

dans le temps des requêtes qui ont dépassé le délai d'attente, nombre de connexion au KSN tirées du cache, nombre de connexions à KSN réussies, nombre de connexions à KSN ratées, nombre de transactions réussies, nombre de transactions ratées, répartition dans le temps des connexions à KSN réussie, répartition dans le temps des connexions à KSN ratées, répartition dans le temps des transactions réussies, répartition dans le temps des transactions ratées) ;

- en cas de détection d'un objet potentiellement malveillant, les informations relatives aux données dans la mémoire des processus sont transmises : éléments de la hiérarchie des objets système (ObjectManager), données de la mémoire UEFI BIOS, noms des clés de registre et leurs valeurs ;

- informations relatives aux événements dans les journaux système : heure de l'événement, nom du journal dans lequel l'événement est détecté, type et catégorie de l'événement, nom de la source de l'événement et sa description ;

- informations sur les connexions réseau : version et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du processus qui a ouvert le port, chemin d'accès au fichier du processus et sa signature numérique, adresses IP locales et distantes, numéros des ports local et distant de connexion, état de la connexion, heure d'ouverture du port ;

- informations sur la date d'installation et d'activation de l'application sur l'Ordinateur : identificateur du partenaire qui a vendu la licence, numéro de série de la licence, identificateur unique de l'installation de l'application sur l'ordinateur, type et identificateur de l'application utilisée pour la mise à jour, identificateur de la tâche de mise à jour ;

- informations sur l'ensemble des mises à jour installées ainsi que sur l'ensemble des dernières mises à jour installées et/ou supprimées, type d'événement ayant provoqué l'envoi des informations relatives aux mises à jour, durée écoulée depuis l'installation de la dernière mise à jour, informations relatives aux bases antivirus téléchargées au moment de la remise des informations ;

- Information sur le fonctionnement de l'application sur l'Ordinateur : données sur l'utilisation du processeur (CPU), donnée sur l'utilisation de la mémoire (Private Bytes, Non-Page Pool, Paged Pool), nombre de flux actifs dans le processus de l'application et de flux en attente, durée de fonctionnement de l'application jusqu'à l'erreur, indice de fonctionnement de l'application en mode interactif ;

- nombre de plantages de l'application et de plantages du système (BSOD) depuis l'installation de l'application et depuis la dernière mise à jour, identifiant et version du module de l'application dans lequel l'échec s'est produit, pile de la mémoire dans le processus de produit et informations relatives aux bases antivirus au moment de l'échec ;

- données relatives au plantage du système (BSOD) : indice de l'apparition du BSOD sur l'Ordinateur, nom du pilote qui a provoqué le BSOD, adresse et pile de la mémoire dans le pilote, indice de la longueur de la session du système d'exploitation avant le BSOD, pile de la mémoire de chute du pilote, type de dump de mémoire conservé, indice que la session du système d'exploitation avant le BSOD avait duré plus de 10 minutes, identifiant unique du dump, date et heure du BSOD ;

- données sur les erreurs ou les problèmes de performances survenus pendant le fonctionnement des modules de l'application : identificateur de l'état de l'application, code et cause de l'erreur, ainsi que son heure d'apparition, identificateurs du composant, du module et du processus de l'application dans lequel l'erreur s'est produite, identificateur de la tâche ou de la catégorie de mise à jour au cours de laquelle l'erreur s'est produite, journaux des pilotes utilisés par l'application (code d'erreur, nom du module, nom du fichier source et ligne sur laquelle l'erreur s'est produite) ;

- données relatives aux mises à jour des bases antivirus et des modules de l'application : noms, dates et heures des fichiers d'index chargés suite à la dernière mise à jour et présents dans la mise à jour actuelle ;

- informations sur les pannes de l'application : date et heure de création du dump, son type, type d'événement à l'origine de l'arrêt accidentel de l'application (coupure accidentelle de l'alimentation, plantage de l'application d'un éditeur tiers), date et heure de la coupure accidentelle de l'alimentation ;

- informations sur la compatibilité des pilotes de l'application avec la configuration matérielle et logicielle : informations sur les propriétés du système d'exploitation qui imposent des limites sur les fonctions des modules de l'application (Secure Boot, KPTL, WHQL Enforce, BitLocker, Case Sensitivity), type de chargement de l'application intégré (UEFL BIOS), indice de la présence d'un module de plateforme de confiance (Trusted Platform Module, TPM), version de la spécification de la TPM, informations sur l'unité centrale (CPU) installée sur l'ordinateur, mode et paramètres de fonctionnement de Code Integrity et Device Guard, mode de fonctionnement des pilotes et raison de l'utilisation du mode actif, version des pilotes de l'application, état de la prise en charge des outils logiciels et matériel de virtualisation de l'Ordinateur par les pilotes ;

- informations sur les applications tierces qui ont provoqué l'erreur : leur nom, version et localisation, code d'erreur et informations à son sujet tirées du journal système des applications, adresse où l'erreur est apparue et pile de mémoire de l'application tierce, signe d'apparition de l'erreur dans le composant de l'application, durée de fonctionnement de l'application avant l'erreur, sommes de contrôle (MD5, SHA2-256, SHA1) de l'image du processus de l'application dans lequel l'erreur s'est produite, chemine d'accès à cette image du processus de l'application et code du modèle de chemin, informations du journal système du système d'exploitation avec la description de l'erreur liée à l'application, les informations sur le module de l'application dans lequel l'erreur s'est produite (identifiant de l'erreur, adresse de l'erreur comme déplacement dans le module, nom et version du module, identifiant de la panne de l'application dans le plug-in du Titulaire de droit et pile de la mémoire de cette panne, durée de fonctionnement de l'application jusqu'à l'erreur) ;

- version du composant de la mise à jour de l'application, nombre d'arrêts sur échec du composant de mise à jour de l'application lors de l'exécution des tâches de mise à jour après le fonctionnement du composant, identifiant du type de tâche de mise à jour, nombre d'échecs de tâches de mise à jour du composant de mise à jour de l'application ;

- informations sur le fonctionnement des modules de surveillance du système : versions complètes des modules, date et heure de lancement des modules, code de l'événement qui a fait déborder la file d'attente d'événement et le nombre de ces événements, total des débordements de la file d'attente d'événement, informations sur le fichier du processus à l'origine de l'événement (nom du fichier et son chemin d'accès sur l'Ordinateur, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du processus lié au fichier, version du fichier), identificateur de l'interception de l'événement réalisée, version complète du filtre de l'intercepteur, identificateur du type d'événement intercepté, taille de la file d'attente d'événements et nombre d'événements entre le premier de la file et l'actuel, nombre d'événements dépassés dans la file d'attente, informations sur le processus à l'origine de l'événement actuel (nom du fichier du processus et son chemin sur l'Ordinateur, code du modèle de chemin, sommes de contrôle (MD5, SHA2-256, SHA1) du processus), durée de traitement de l'événement, durée maximale autorisée pour le traitement de l'événement, valeur de la probabilité d'envoi des données, informations sur les événements du système d'exploitation pour lesquels l'application a dépassé la limite du délai d'attente (date et heure de la réception de l'événement, nombre d'initialisations répétées des bases antivirus, date et heure de la dernière initialisation répétée des bases antivirus après leur mise à jour, durée du retard de traitement des événements par chaque module de surveillance du système, nombre d'événements en attente, nombre d'événements traités, nombre d'événements du type actuel retenus, total du retard pour les événements du type actuel, total du retard pour tous les événements) ;

- informations sur l'outil de trace des événements Windows (Event Tracing for Windows, ETW) lors de problèmes de performances de l'application, fournisseurs d'événements SysConfig/SysConfigEx/WinSATAssessment de Microsoft : données sur l'ordinateur (modèle, fabricant, facteur de forme, version), données sur les indicateurs de performance Windows (données de l'évaluation WinSAT, indice de performance Windows), nom du domaine, données sur les processus physiques et logiques (nombre de processeurs physiques et logiques, fabricant, modèle, stepping, nombre de noyaux, fréquence d'horloge, identificateur de processeur (CPUID), caractéristiques du cache, caractéristiques du processeur logique, indice de prise en charge des modes et des instructions), données sur les modules de la mémoire vive (type, facteur de forme, fabricant, modèle, volume, granularité de l'allocation de la mémoire), données sur les interfaces réseau (adresses IP et MAC, nom, description, configuration des interfaces réseau, répartition du nombre et du volume de paquets réseau par type, vitesse de l'échange réseau, distribution du nombre d'erreurs réseau par type), configuration du contrôleur IDE, adresses IP des serveurs DNS, données sur la carte vidéo (modèle, description, fabricant, compatibilité, volume de mémoire vidéo, résolution de l'écran, nombre de bits par pixel, version du BIOS), données sur les périphériques Plug-and-Play

(nom, description, identificateur de périphérique [PnP, ACPI], données relatives aux disques et supports (nombre de disques ou de clés USB, fabricant, modèle, volume de disque, nombre de tambours, nombre de pistes par tambour, nombre de partitions par piste, volume de secteur, caractéristiques du cache, numéro de séquence, nombre de partitions, configuration du contrôleur SCSI), données sur les disques logiques (numéro de séquence, volume de la partition, taille du volume, lettre du volume, type de partition, type de système de fichiers, nombre de clusters, taille du cluster, nombre de secteurs dans un cluster, nombre de clusters occupés et disponibles, lettre du volume d'amorçage, déplacement de la partition par rapport au début du disque), données sur le BIOS de la carte-mère (fabricant, date de fabrication, version), données sur la mémoire physique (volume total et disponible), données sur les services du système d'exploitation (nom, description, état, tag, données sur les processus [nom et identificateur PID]), paramètres de consommation de l'ordinateur, configuration du contrôleur d'interruptions, chemin d'accès aux dossiers système Windows (Windows et System32), données sur le système d'exploitation (version, build, date d'édition, nom, type, date d'installation), taille du fichier de débogage, données sur les écrans (nombre, fabricant, résolution de l'écran, pouvoir de résolution, type), données sur le pilote de la carte vidéo (fabricant, date de sortie, version) ;

- informations fournies par ETW, fournisseurs d'événements EventTrace/EventMetadata de Microsoft : données sur la séquence des événements système (type, heure, date, fuseau horaire), métadonnées du fichier avec les résultats du traçage (nom, structure, paramètres de traçage, distribution du nombre d'opérations de traçage par type), données sur le système d'exploitation (nom, type, version, build, date de publication, heure de lancement) ;

- informations fournies par l'ETW, fournisseurs d'événements Process / Microsoft-Windows-Kernel-Process / Microsoft-Windows-Kernel-Processor-Power de Microsoft : données sur les processus à lancer et à arrêter (nom, identificateur PID, paramètres de lancement, ligne de commande, code de retour, paramètres d'administration de l'alimentation, heure de lancement et de fin, type de marqueur d'accès, identificateur de sécurité SID, identificateur de séance SessionID, nombre de descripteurs installés), données sur la modification des priorités de flux (identificateur de flux TID, priorité, heure), données sur les opérations du processus sur le disque (type, heure, volume, nombre), historique de la modification de la structure et volume de processus utilisé ;

- informations fournies par ETW, fournisseurs d'événements StackWalk / Perfinfo de Microsoft : données des compteurs de performance (performances de segments distincts du code, séquence des appels de fonction, identificateur du processus PID, identificateur du flux TID, adresses et attributs des gestionnaires d'interruption ISR et des appels différés des procédures DPC) ;

- informations fournies par ETW, fournisseur d'événements KernelTraceControl-ImageID de Microsoft : données sur les fichiers exécutables et les bibliothèques dynamiques (nom, taille de l'image, chemin d'accès complet), données sur les fichiers PDB (nom, identificateur), données de la ressource VERSIONINFO du fichier exécutable (nom, description, éditeur, locale, version et identificateur de l'application, version et identificateur du fichier) ;

- informations fournies par ETW, fournisseurs d'événements FileIo / DiskIo / Image / Windows-Kernel-Disk de Microsoft : données sur les opérations relatives aux fichiers et aux disques (type, volume, heure de début, heure de fin, durée, état de l'arrêt, identificateur de processus PID, identificateur de flux TID, adresses des appels de fonction du pilote, paquet de requête d'E/S (IRP), attributs d'objet de fichier Windows), données sur les fichiers impliqués dans les opérations relatives aux fichiers et aux disques (nom, version, taille, chemin d'accès complet, attribut, déplacement, somme de contrôle de l'image, options d'ouverture et d'accès) ;

- informations fournies par ETW, fournisseur d'événements PageFault de Microsoft : données sur les erreurs d'accès aux pages de la mémoire (adresse, heure, volume, identificateur du processus PID, identificateur de flux TID, attributs de l'objet de fichier Windows, paramètres d'allocation de mémoire) ;

- informations fournies par ETW, fournisseur d'événements Thread de Microsoft : données sur la création/la fin de flux, données sur les flux lancés (identificateur de processus PID, identificateur de flux TID, taille de la pile, priorité et distribution des ressources de l'unité centrale, ressources d'entrée et de sortie, pages de mémoire entre les flux, adresse de la pile, adresse de la fonction initiale, adresse du bloc d'environnement de flux (Thread Environment Block, TEB), tag du service Windows) ;

- informations fournies par ETW, fournisseur d'événements Microsoft-Windows-Kernel-Memory de Microsoft : données sur les opérations d'administration de la mémoire (état de la fin, heure, nombre, identificateur de processus PID), structure de distribution de la mémoire (type, volume, identificateur de session SessionID, identificateur de processus PID) ;

- informations sur le fonctionnement de l'application en cas de problème de productivité : identificateur d'installation de l'application, type et valeur de réduction des performances, données sur la séquence des événements internes de l'application (heure, fuseau horaire, type, état d'arrêt, identificateur de module de l'application, identificateur de scénario de fonctionnement de l'application, identificateur de flux TID, identificateur de processus PID, adresses d'appels de fonctions), données sur les fichiers PDB (nom, identificateur, taille de l'image du fichier exécutable), données sur les fichiers à analyser (nom, chemin complet, somme de contrôle), paramètres de surveillance des performances de l'application ;

- informations sur le dernier redémarrage en échec du système d'exploitation : nombre de redémarrages en échec depuis l'installation du système d'exploitation, données relatives au crash du système (code et paramètres de l'erreur, nom, version et somme de contrôle (CRC32) du module ayant entraîné l'erreur dans le fonctionnement du système d'exploitation, adresse de l'erreur comme déplacement dans le module, sommes de contrôle (MD5, SHA2-256, SHA1) du vidage du système) ;

- informations de vérification de l'authenticité des certificats qui signent les fichiers : empreinte du certificat, algorithme de calcul de la somme de contrôle, clé publique et numéro de série du certificat, nom de l'autorité de certification, résultat du contrôle du certificat et identifiant de la base de certificats ;

- informations sur le processus à l'origine de l'attaque contre l'auto-défense de l'application : nom et taille du fichier du processus, ses sommes de contrôle (MD5, SHA2-256, SHA1), chemin d'accès complet à celui-ci et modèle de chemin, date et heure de création et de configuration du fichier du processus, code du type de fichier de processus, indice de fichier exécutable, attribut de fichier du processus, informations relatives au certificat utilisé pour signer le fichier du processus, type du compte utilisateur sous lequel le processus ou le flux réalise l'action suspecte, identifiant des opérations réalisées pour accéder au processus, type de ressource à partir de laquelle l'opération a été réalisée (processus, fichier, objet du registre, fenêtre de recherche à l'aide de la fonction FindWindow), nom de la ressource depuis laquelle l'opération est exécutée, indice de réussite de l'opération, état du fichier du processus et sa signature dans KSN ;

- informations relatives à l'application du Titulaire des droits : locale et état de fonction de la version de l'application utilisée, version des modules de l'application installés et état de leur fonctionnement, données sur les mises à jour de l'application installée ainsi que la valeur du filtre TARGET ;

- informations sur le matériel installé sur l'Ordinateur : type, nom, modèle, version du micrologiciel, caractéristiques des appareils intégrés et connectés, identifiant unique de l'Ordinateur sur lequel est installée l'application ;

- informations relatives à la version du système d'exploitation installée sur l'Ordinateur et aux paquets de mises à jour installés, version, rédaction et paramètres du mode de fonctionnement du système d'exploitation, version et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier du noyau du système d'exploitation et date et heure de lancement du système d'exploitation ;

- les fichiers exécutables et non exécutables, dans leur intégralité ou en partie, y compris les fichiers de confiance ;

- des parties de la mémoire RAM de l'Ordinateur ;

- les secteurs impliqués dans le processus d'amorçage du système d'exploitation ;

- les paquets de données du trafic réseau ;

- les pages Web et les e-mails contenant des objets malveillants et suspects ;

- la description des classes et instances de classes du référentiel WMI ;

- Ces rapports d'activités des applications contiennent les données suivantes sur les fichiers et processus : nom, taille, version, description et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier envoyé, identifiant du format du fichier, nom de l'éditeur du fichier, nom du produit auquel le fichier appartient, chemin d'accès complet sur l'Ordinateur, code de modèle du chemin d'accès au fichier, date et heure de création et de modification du fichier ; date et heure de début et de fin de validité du certificat (si le fichier possède une signature numérique), date et heure de la signature, nom de l'émetteur du certificat, informations relatives au détenteur du certificat, empreinte, clé publique et algorithmes appropriés du certificat, numéro de série du certificat ; nom du compte à partir duquel le processus est exécuté ; sommes de contrôle (MD5, SHA2-256, SHA1) du nom de l'Ordinateur sur lequel le processus est en cours d'exécution ; titres des fenêtres de processus ; identifiant des bases antivirus, nom de la menace détectée selon la classification du Détenteur des droits ; données relatives à la licence installée : identifiant, type et date d'expiration ; heure locale de l'Ordinateur au moment de la fourniture des informations , noms et chemins d'accès des fichiers auxquels le processus a accédé , noms et valeurs des clés de registre auxquelles le processus a accédé , URL et adresses IP auxquelles le processus a accédé , URL et adresses IP à partir desquelles le fichier en exécution a été téléchargé.

Activation et désactivation de l'utilisation de Kaspersky Security Network

Pour activer ou désactiver l'utilisation de Kaspersky Security Network, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection avancée → Kaspersky Security Network**.
3. Cochez la case **Kaspersky Security Network** si vous souhaitez que Kaspersky Endpoint Security exploite les informations sur la réputation des fichiers, des sites Internet et des applications fournies par les bases de Kaspersky Security Network.

   Kaspersky Endpoint Security affichera la Déclaration de Kaspersky Security Network. Si vous êtes d'accord avec le contenu, acceptez les conditions d'utilisation de KSN.

   Par défaut, Kaspersky Endpoint Security utilise le mode étendu du KSN. Le *mode étendu du KSN* est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Endpoint Security envoie des données supplémentaires à Kaspersky.
4. Si nécessaire, décochez la case **Activer le mode étendu du KSN**.
5. Enregistrez vos modifications.

Activation et désactivation du mode Cloud pour les modules de protection

Lors de l'utilisation de Kaspersky Private Security Network, la fonction du mode Cloud est accessible à partir de la version Kaspersky Private Security Network 3.0.

Pour activer ou désactiver le mode cloud pour les modules de la protection, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Kaspersky Security Network**.

   Les paramètres de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer le mode Cloud pour les modules de protection**.

     Si la case est cochée, Kaspersky Endpoint Security utilise la version allégée des bases antivirus, ce qui réduit la charge sur les ressources du système d'exploitation.

     Kaspersky Endpoint Security télécharge la version allégée des bases antivirus lors de la première mise à jour après que la case a été cochée.

     Si la version simplifiée des bases antivirus ne peut être utilisée, Kaspersky Endpoint Security passe automatiquement à l'utilisation de la version complète des bases antivirus.

   - Décochez la case **Activer le mode Cloud pour les modules de protection**.

     Si la case est décochée, Kaspersky Endpoint Security utilise la version complète des bases antivirus.

     Kaspersky Endpoint Security télécharge la version complète des bases antivirus lors de la première mise à jour après que la case a été décochée.

   La case est accessible si la case **Kaspersky Security Network** est cochée.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Vérification de la connexion à Kaspersky Security Network

Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le groupe **Technologies de détection des menaces**.

   La partie inférieure de la fenêtre **Technologies de détection des menaces** reprend les informations suivantes sur le fonctionnement de Kaspersky Security Network :

   - Sous la ligne **KASPERSKY SECURITY NETWORK (KSN)** figure un des états suivants de la connexion de Kaspersky Endpoint Security à Kaspersky Security Network :

     - *Activé. Disponible*.

       Cet état signifie que Kaspersky Security Network intervient dans le fonctionnement de Kaspersky Endpoint Security et les serveurs KSN sont accessibles.

     - *Activé. Non disponible*.

       Cet état signifie que Kaspersky Security Network intervient dans le fonctionnement de Kaspersky Endpoint Security et les serveurs KSN ne sont pas accessibles.

     - *Désactivé*.

       Cet état signifie que Kaspersky Security Network n'intervient pas dans le fonctionnement de Kaspersky Endpoint Security.

   - Les lignes **Objets inoffensifs**, **Objets dangereux**, **Menaces neutralisées par jour** reprennent les statistiques globales de l'infrastructure des services cloud Kaspersky Security Network.

- La ligne **Dernière synchronisation** affiche la date et l'heure de la dernière synchronisation de Kaspersky Endpoint Security avec les serveurs KSN.

  L'application obtient les données statistiques sur l'utilisation de KSN à l'ouverture de la fenêtre **Technologies de détection des menaces**. La mise à jour en temps réel des statistiques globales de l'infrastructure des services cloud Kaspersky Security Network et du contenu de la ligne **Dernière synchronisation** n'a pas lieu.

  Si le temps écoulé depuis la dernière synchronisation avec les serveurs KSN est supérieur à 15 minutes ou si l'état *Inconnu* est affiché, l'état de la connexion de Kaspersky Endpoint Security à Kaspersky Security Network prend la *valeur Activé. Non disponible*.

  La connexion avec les serveurs de Kaspersky Security Network peut être interrompue pour une des raisons suivantes :

  - L'ordinateur n'est pas connecté à Internet.
  - L'application n'est pas activée.
  - La durée de validité de la licence est écoulée.
  - Problèmes liés à la clé (par exemple, la clé figure dans une liste noire de clés).

  En cas d'échec du rétablissement de la connexion aux serveurs de Kaspersky Security Network, il est conseillé de contacter le Support Technique ou le prestataire de services.

Vérification de la réputation d'un fichier dans Kaspersky Security Network

Le service KSN permet de recevoir des informations sur les applications qui figurent dans les bases de données de réputation de Kaspersky. Cela permet de réaliser une gestion flexible des stratégies de lancement des applications au niveau de l'entreprise en empêchant le lancement d'applications publicitaires ou d'applications légitimes que des individus malintentionnés pourraient utiliser pour nuire à l'ordinateur ou aux données de l'utilisateur.

Pour vérifier la réputation d'un fichier dans Kaspersky Security Network, procédez comme suit :

1. D'un clic droit, ouvrez le menu contextuel du fichier dont vous souhaitez vérifier la réputation.
2. Sélectionnez l'option **Consulter la réputation dans KSN**.

   Cette option est disponible si vous avez accepté les conditions de la Déclaration de Kaspersky Security Network.

   Cette action ouvre la fenêtre **<Nom du fichier> : réputation dans KSN**. La fenêtre **<Nom du fichier> : réputation dans KSN** affiche les informations suivantes à propos du fichier en cours de vérification :

   - **Emplacement**. Le chemin d'accès au fichier sur le disque.
   - **Version**. La version de l'application (les informations s'affichent uniquement pour les fichiers exécutables).

- **Signature numérique**. Existence d'une signature numérique pour le fichier.
- **Date de signature**. La date de la signature du certificat par la signature numérique.
- **Date de création**. La date de création du fichier.
- **Date de modification**. La date de la dernière modification du fichier.
- **Taille**. L'espace occupé par le fichier sur le disque.
- Les informations relatives au nombre d'utilisateurs qui font confiance au fichier ou qui le bloquent.

Détection comportementale

Cette section contient des informations sur la Détection comportementale et les instructions sur la configuration des paramètres du module.

A propos de la Détection comportementale

Le module Détection comportementale récupère des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent intervenir avec plus d'efficacité.

Le module Détection comportementale utilise des modèles de comportement d'applications dangereux. Les modèles comprennent les séries d'actions des applications que Kaspersky Endpoint Security considère comme dangereuses. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Endpoint Security exécute la réaction choisie. La fonction de Kaspersky Endpoint Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

Activation et désactivation de la Détection comportementale

Par défaut, la Détection comportementale est activée et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver la Détection comportementale.

Il est déconseillé de désactiver la Détection comportementale sans nécessité car cela réduit l'efficacité des modules de la protection. Les modules de protection peuvent solliciter des informations récupérées par la Détection comportementale pour détecter les menaces.

Pour activer ou désactiver la Détection comportementale, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Détection comportementale**.

   Les paramètres du module Détection comportementale s'affichent dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

- Cochez la case **Détection comportementale** si vous souhaitez que Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation à l'aide des modèles de comportement dangereux.

- Décochez la case **Détection comportementale** si vous ne souhaitez pas que Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation à l'aide des modèles de comportement dangereux.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection de l'action à exécuter en cas de détection d'une activité malveillante d'une application

Lors de la détection de l'activité d'une application malveillante, Kaspersky Endpoint Security crée l'enregistrement *Un objet malveillant a été détecté* dans les rapports de l'application (**Rapports → Détection comportementale**).

Pour choisir l'action à exécuter en cas de détection de l'activité malveillante d'une application, procédez comme suit :

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

2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Détection comportementale**.

   Les paramètres du module Détection comportementale s'affichent dans la partie droite de la fenêtre.

3. Sélectionnez l'action requise dans la liste déroulante **En cas de détection de l'activité d'une application malveillante** :

   - **Supprimer le fichier**.

     Si cet élément est sélectionné, Kaspersky Endpoint Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application.

   - **Arrêter le programme**.

     Si cet élément est sélectionné, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application.

   - **Notifier**.

     Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la protection des dossiers partagés contre le chiffrement externe

Le composant assure le suivi des opérations uniquement pour les fichiers qui se trouvent sur des périphériques de stockage de masse avec système de fichiers NTFS et qui ne sont pas chiffrés par le système EFS.

La fonction de protection des dossiers partagés contre le chiffrement externe garantit l'analyse de l'activité dans les dossiers partagés. Si l'activité correspond à un modèle de comportement dangereux caractéristique du chiffrement externe, Kaspersky Endpoint Security exécute l'action choisie.

Vous pouvez exécuter les actions suivantes pour configurer la protection du dossier partagé contre le chiffrement externe :

- sélectionner l'action à exécuter en cas de détection du chiffrement externe d'un dossiers partagé ;
- configurer les adresses des exclusions de la protection des dossiers partagés contre le chiffrement externe.

Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe

La protection des dossiers partagés contre le chiffrement externe est désactivée par défaut.

Après l'installation de Kaspersky Endpoint Security, la fonction de protection des dossiers partagés contre le chiffrement externe est limitée avant le redémarrage de l'ordinateur.

Pour activer ou désactiver la protection des dossiers partagés contre le chiffrement externe, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Détection comportementale**.

   Les paramètres du module Détection comportementale s'affichent dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Dans la section **Protection des dossiers partagés contre le chiffrement externe**, cochez la case **Activer la protection des dossiers partagés contre le chiffrement externe** si vous voulez que Kaspersky Endpoint Security analyse l'activité typique d'un chiffrement externe.
   - Dans la section **Protection des dossiers partagés contre le chiffrement externe**, décochez la case **Activer la protection des dossiers partagés contre le chiffrement externe** si vous ne voulez pas que Kaspersky Endpoint Security analyse l'activité typique d'un chiffrement externe.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection de l'action à exécuter en cas de détection du chiffrement externe de dossiers partagés

En cas de détection d'une tentative de modification des fichiers dans les dossiers partagés, Kaspersky Endpoint Security crée dans le journal un enregistrement qui contient les informations sur la tentative de modification des fichiers dans les dossiers partagés.

Pour choisir l'action à exécuter en cas de détection du chiffrement externe de dossiers partagés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Détection comportementale**.

   Les paramètres du module Détection comportementale s'affichent dans la partie droite de la fenêtre.
3. Dans la liste déroulante **En cas de détection du chiffrement externe de dossiers partagés** du groupe **Protection des dossiers partagés contre le chiffrement externe**, choisissez l'action requise :

   - **Bloquer la connexion**.

     Si vous avez choisi cette option, en cas de détection d'une tentative de modification des fichiers dans des dossiers partagés, Kaspersky Security Center bloque l'activité réseau de l'ordinateur qui a réalisé la modification, crée une copie de sauvegarde des fichiers endommagés par la modification, ajoute un enregistrement aux rapports de l'interface locale de l'application et envoie les informations relatives à la détection de l'activité malveillante à Kaspersky Security Center. Si le composant Réparation des actions malicieuses est activé, l'application restaure les fichiers modifiés au départ des copies de sauvegarde.

     Si vous avez choisi l'option **Bloquer la connexion**, vous pouvez indiquer dans le champ **Bloquer la connexion pendant** la durée en minutes pendant laquelle la connexion réseau va être bloquée.

   - **Notifier**.

     Si vous avez choisi cette option, en cas de détection d'une tentative de modification de fichiers dans des dossiers partagés, Kaspersky Endpoint Security ajoute un enregistrement dans les rapports de l'interface locale de l'application, ajoute un enregistrement à la liste des menaces actives et envoie les informations relatives à la détection d'une activité malveillante à Kaspersky Security Center.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration des adresses des exclusions de la protection des dossiers partagés contre le chiffrement externe

Pour pouvoir profiter de la fonction d'exclusion des adresses de la protection des dossiers partagés contre le chiffrement externe, il faut activer le service d'Audit de l'accès au système. Ce service est désactivé par défaut (pour en savoir plus sur l'activation du service d'audit de l'accès au système, consultez le site de Microsoft).

La fonction des exclusions des adresses de la protection des dossiers partagés n'est pas disponible sur un ordinateur distant si celui-ci a été allumé avant le lancement de Kaspersky Endpoint Security. Vous pouvez redémarrer cet ordinateur distant après le lancement de Kaspersky Endpoint Security pour garantir le fonctionnement de l'exclusion des adresses de la protection des dossiers partagés sur cet ordinateur distant.

Pour exclure de la protection des ordinateurs distants qui réalisent le chiffrement externe des dossiers partagés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Détection comportementale**.

   Les paramètres du module Détection comportementale s'affichent dans la partie droite de la fenêtre.
3. Dans le groupe **Protection des dossiers partagés contre le chiffrement externe**, cliquez sur le bouton **Exclusions**.

   La fenêtre **Exclusions** s'ouvre.
4. Exécutez une des actions suivantes :

   - Si vous voulez ajouter l'adresse IP ou le nom de l'ordinateur à la liste des exclusions, cliquez sur le bouton **Ajouter**.
   - Si vous souhaitez modifier l'adresse IP ou le nom de l'ordinateur, sélectionnez l'élément dans la liste des exclusions et cliquez sur le bouton **Modifier**.

   La fenêtre **Ordinateur** s'ouvre.
5. Saisissez l'adresse IP ou le nom de l'ordinateur pour lequel les tentatives de chiffrement externe ne doivent pas être traitées.
6. Cliquez sur le bouton **OK** dans la fenêtre **Ordinateur**.
7. Dans la fenêtre **Exclusions**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection contre les Exploits

Cette section contient des informations sur la Protection contre les Exploits et les instructions sur la configuration du module.

A propos de la Protection contre les Exploits

Le module Protection contre les Exploits traque les fichiers exécutables lancés par les applications vulnérables. S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier. Les informations relatives à l'interdiction du lancement du fichier exécutable sont consignées dans le rapport sur le fonctionnement de la Protection contre les Exploits.

Activation et désactivation de la Protection contre les Exploits

Par défaut, la Protection contre les Exploits est activée et fonctionne dans le mode recommandé par les experts de Kaspersky. Vous pouvez désactiver la Protection contre les Exploits le cas échéant.

Pour activer ou désactiver la Protection contre les exploits, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les Exploits**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les Exploits.
3. Exécutez une des actions suivantes :

   - Cochez la case **Protection contre les Exploits** si vous voulez que Kaspersky Endpoint Security surveille les fichiers exécutables lancés par les applications vulnérables.

     Si Kaspersky Endpoint Security détecte qu'un fichier exécutable de l'application vulnérable n'a pas été lancé par l'utilisateur, il exécute l'action sélectionnée dans la liste déroulante **En cas de détection d'un exploit**.
   - Décochez la case **Protection contre les Exploits** si vous ne voulez pas que Kaspersky Endpoint Security surveille les fichiers exécutables lancés par les applications vulnérables.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la Protection contre les Exploits

Vous pouvez exécuter les opérations suivantes pour configurer le fonctionnement du module Protection contre les exploits :

- sélectionner l'action à exécuter en cas de détection d'un exploit ;
- activer ou désactiver la protection de la mémoire des processus système.

Sélection de l'action à exécute en cas de détection d'un exploit

Par défaut, quand Kaspersky Endpoint Security détecte un exploit, il en bloque les opérations.

Pour choisir l'action à exécuter en cas de détection d'un exploit, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les Exploits**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les Exploits.
3. Sélectionnez dans la liste déroulante **En cas de détection d'un exploit** l'action requise :

   - **Bloquer l'opération**.

     Si vous avez choisi cette option, Kaspersky Endpoint Security, après la détection d'un exploit, bloque l'opération de ce code d'exploitation et crée dans le journal une entrée qui reprend des informations relatives à ce code d'exploitation.
   - **Notifier**.

     Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert un exploit, crée une entrée dans le journal qui reprend les informations relatives à l'exploit et ajoute les informations relatives à l'exploit dans la liste des menaces actives.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation ou désactivation de la protection de la mémoire des processus système

La protection de la mémoire des processus système est activée par défaut.

Pour activer ou désactiver la protection de la mémoire des processus système, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les Exploits**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les Exploits.
3. Exécutez une des actions suivantes :

   - Dans le groupe **Protection de la mémoire des processus système**, cochez la case **Activer la protection de la mémoire des processus système** si vous voulez que Kaspersky Endpoint bloque les processus tiers qui tentent d'accéder aux processus système.
   - Dans le groupe **Protection de la mémoire des processus système**, décochez la case **Activer la protection de la mémoire des processus système** si vous ne voulez pas que Kaspersky Endpoint bloque les processus tiers qui tentent d'accéder aux processus système.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Prévention des intrusions

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Windows pour serveurs de fichiers.

Cette section contient des informations sur la Prévention des intrusions et les instructions sur la configuration du module.

Présentation de la Prévention des intrusions

Le module Prévention des intrusions empêche l'exécution des actions dangereuses pour le système et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles.

Le module contrôle les applications, y compris l'accès des applications aux ressources protégées (fichiers et dossiers, clés du registre), à l'aide des *privilèges des applications*. Les privilèges des applications représentent un ensemble de restrictions pour différentes actions des applications dans le système d'exploitation et un ensemble de droits d'accès aux ressources de l'ordinateur.

Le module Pare-feu contrôle l'activité réseau des applications.

Au premier lancement de l'application sur l'ordinateur, le module Prévention des intrusions vérifie le niveau de danger de l'application et la place dans un des groupes de confiance. Le groupe de confiance définit les privilèges que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications.

Pour contribuer au fonctionnement plus efficace du module Prévention des intrusions, il est conseillé de participer au Kaspersky Security Network. Les données obtenues à l'aide de Kaspersky Security Network permettent de référer plus précisément les applications à un groupe de confiance ou à un autre, et aussi appliquer les paramètres optimaux pour les privilèges des applications.

Lors du prochain lancement de l'application, la Prévention des intrusions analyse l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les privilèges des applications existants. En cas de modification de l'application, la Prévention des intrusions l'analyse comme s'il s'agissait de sa première exécution.

Restrictions sur le contrôle des appareils audio et vidéo

A propos de la protection du signal audio

La fonction de protection du signal audio possède les caractéristiques suivantes :

- Pour que la fonction soit opérationnelle, le module Prévention des intrusions doit être activé.
- Si l'application a commencé à recevoir le signal audio avant le lancement de la Prévention des intrusions, Kaspersky Endpoint Security permet à l'application de recevoir le signal audio et n'affiche aucune notification.
- Si vous avez placé l'application dans le groupe **Douteuses** ou **Restrictions élevées** après que l'application a commencé à recevoir le signal audio, Kaspersky Endpoint Security permet à l'application de recevoir le signal audio et n'affiche aucune notification.
- En cas de modification des paramètres d'accès de l'application aux dispositifs d'enregistrement (par exemple, la réception du signal audio par l'application a été interdite dans la fenêtre des paramètres de la Prévention des intrusions), il faut relancer l'application afin qu'elle arrête de recevoir le signal audio.
- Le contrôle de la réception du signal audio depuis le dispositif d'enregistrement ne dépend pas des paramètres de l'accès des applications à la webcam.
- Kaspersky Endpoint Security protège uniquement l'accès aux microphones intégrés et externes. Les autres dispositif de transmission du son ne sont pas pris en charge.
- Kaspersky Endpoint Security ne garantit pas la protection du signal audio transmis par des appareils comme les appareils photo reflex numériques, les caméras vidéo portables ou les caméras sportives.

Caractéristiques du fonctionnement des appareils audio et vidéo pendant l'installation et la mise à jour de Kaspersky Endpoint Security

Au premier lancement de l'application Kaspersky Endpoint Security après son installation, la reproduction ou l'enregistrement audio ou vidéo peuvent être interrompus dans les applications de d'enregistrement ou de lecture audio et vidéo. Ceci est nécessaire pour activer la fonction du contrôle de l'accès des applications aux dispositifs d'enregistrement audio. Le service système d'administration des outils de manipulation du son sera redémarré au premier lancement de l'application Kaspersky Endpoint Security.

A propos de l'accès des applications aux webcams

La fonction de protection de l'accès à la webcam possède les particularités et les restrictions suivantes :

- L'application contrôle les images dynamiques et statiques reçues à la suite du traitement des données de la webcam.
- L'application contrôle le signal audio afin de déterminer s'il appartient au flux vidéo de la webcam.
- L'application contrôle uniquement les webcams connectées via l'interface USB ou IEEE1394 et affichées dans le Gestionnaire de périphériques Windows comme **Périphérique d'acquisition d'image** (Imaging Device).

Webcam prises en charge

Kaspersky Endpoint Security est compatible avec les webcams suivantes :

- Logitech HD Webcam C270 ;
- Logitech HD Webcam C310 ;
- Logitech Webcam C210 ;
- Logitech Webcam Pro 9000 ;
- Logitech HD Webcam C525 ;
- Microsoft LifeCam VX-1000 ;
- Microsoft LifeCam VX-2000 ;
- Microsoft LifeCam VX-3000 ;
- Microsoft LifeCam VX-800 ;
- Microsoft LifeCam Cinema.

Kaspersky ne garantit pas la prise en charge des webcams qui ne figurent pas dans cette liste.

Activation et désactivation de la Prévention des intrusions

Par défaut, le module Prévention des intrusions est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver le module Prévention des intrusions.

Pour activer ou désactiver le module Prévention des intrusions, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :

   - Cochez la case **Prévention des intrusions** si vous voulez activer le module Prévention des intrusions.
   - Décochez la case **Prévention des intrusions** si vous voulez désactiver le module Prévention des intrusions.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des groupes de confiance d'applications

Au premier lancement de chaque l'application, le module Prévention des intrusions vérifie le niveau de danger de l'application et la place dans un des groupes de confiance.

A la première étape de l'analyse de l'application, Kaspersky Endpoint Security cherche l'enregistrement sur l'application dans la base interne des applications connues et envoie simultanément une demande à la base de Kaspersky Security Network (s'il existe une connexion à Internet). L'application est placée dans un groupe de confiance sur la base des résultats de l'analyse selon la base interne et selon la base de Kaspersky Security Network. À chaque lancement de l'application, Kaspersky Endpoint Security envoie une nouvelle demande à la base KSN et déplace l'application dans un autre groupe de confiance si la réputation de l'application dans la base KSN a changé.

Vous pouvez choisir le groupe de confiance dans lequel Kaspersky Endpoint Security va mettre automatiquement les applications inconnues. Les applications, lancées avant Kaspersky Endpoint Security, sont placées automatiquement dans le groupe de confiance indiqué dans la fenêtre **Sélection du groupe de confiance**.

S'agissant des applications lancées avant Kaspersky Endpoint Security, le contrôle porte uniquement sur leur activité réseau. Le contrôle s'opère selon les règles réseau définies dans les paramètres du Pare-feu.

Configuration des paramètres de répartition des applications par groupe de confiance

Si la participation à Kaspersky Security Network est activée, Kaspersky Endpoint Security envoie la demande sur la réputation de l'application à KSN à chaque lancement de l'application. En fonction de la réponse reçue, l'application peut être déplacée dans un groupe de confiance différent de celui désigné dans les paramètres du module Prévention des intrusions.

Kaspersky Endpoint Security place toujours les applications signées par des certificats Microsoft ou des certificats Kaspersky dans le groupe "De confiance".

Pour configurer les paramètres de la répartition des applications selon les groupes de confiance, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module **Prévention des intrusions** s'affichent dans la partie droite de la fenêtre.
3. Si vous voulez placer automatiquement les applications avec une signature numérique de fournisseur de confiance dans le groupe De confiance, cochez la case **Faire confiance aux applications dotées d'une signature numérique**.

   Les *éditeurs de confiance* sont les éditeurs d'applications qui sont inclus par Kaspersky dans le groupe de confiance. Vous pouvez également ajouter manuellement le certificat de l'éditeur au stockage système sécurisé des certificats.
4. Pour placer tous les programmes inconnus dans le groupe de confiance indiqué, choisissez le groupe de confiance souhaité dans la liste déroulante **Les applications dont le groupe de confiance n'a pas pu être déterminé sont placées automatiquement dans**

   > Pour garantir votre sécurité, le groupe **De confiance** ne figure pas les valeurs du paramètre **Les applications dont le groupe de confiance n'a pas pu être déterminé sont placées automatiquement dans**.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du groupe de confiance

A la première exécution de l'application, Kaspersky Endpoint Security place automatiquement l'application dans un groupe de confiance ou l'autre. Le cas échéant, vous pouvez manuellement déplacer l'application dans un autre groupe de confiance.

> Les experts de Kaspersky déconseillent de déplacer les applications du groupe de confiance défini automatiquement dans un autre groupe de confiance. Au lieu de cela, modifiez le cas échéant les privilèges de l'application en question.

Pour modifier le groupe de confiance où Kaspersky Endpoint Security a placé automatiquement l'application à son premier lancement, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Privilèges des applications** de la fenêtre **Prévention des intrusions** s'ouvre.
4. Sélectionnez sous l'onglet **Privilèges des applications** l'application requise.
5. Exécutez une des actions suivantes :

- Cliquez-droit pour ouvrir le menu contextuel de l'application. Dans le menu contextuel de l'application, choisissez l'option **Déplacer dans le groupe → <nom du groupe>**.
- Le lien **De confiance** / **Restrictions faibles**/**Restrictions élevées** / **Douteuses** permet d'ouvrir un menu contextuel. Sélectionnez le groupe de confiance requis dans le menu contextuel.

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection du groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security

S'agissant des applications lancées avant Kaspersky Endpoint Security, le contrôle porte uniquement sur leur activité réseau. Le contrôle s'opère selon les règles réseau définies dans les paramètres du Pare-feu. Pour désigner les règles réseau qui doivent régir le contrôle de l'activité réseau de ces application, il faut choisir un groupe de confiance.

Pour choisir le groupe de confiance pour les applications lancées avant Kaspersky Endpoint Security, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Modifier**.

   La fenêtre **Sélection du groupe de confiance** s'ouvre.
4. Choisissez le groupe de confiance requis.
5. Cliquez sur le bouton **OK**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des privilèges des applications

Par défaut le contrôle de l'application est assuré par les privilèges des applications définis pour le groupe de confiance dans lequel Kaspersky Endpoint Security a mis l'application à son premier lancement. Le cas échéant, vous pouvez modifier les privilèges des applications pour tout le groupe de confiance, pour une application spécifique ou pour un groupe d'applications qui font partie du groupe de confiance.

Les privilèges des applications définis pour une application spécifique ou pour un groupe d'applications qui font partie du groupe de confiance ont une priorité plus élevée que les privilège des applications définis pour le groupe de confiance. Cela veut dire que si les paramètres des privilèges des applications définis pour une application spécifique ou un groupe d'applications qui font partie du groupe de confiance sont différents des paramètres des privilèges des applications définis pour le groupe de confiance, la Prévention des intrusions contrôle l'application ou le groupe d'applications qui font partie du groupe de confiance conformément aux privilèges des applications définis pour l'application ou le groupe d'applications.

Modification des privilèges des applications pour les groupes de confiance et pour les groupe d'applications

Par défaut, les privilèges des applications optimaux ont été créés pour différents groupes de confiance. Les paramètres des privilèges de groupes d'applications qui font partie du groupe de confiance héritent des valeurs des paramètres des privilèges des groupes de confiance. Vous pouvez modifier les privilèges des groupes de confiance prédéfinis et les privilèges des groupes d'applications.

Pour modifier les privilèges du groupe de confiance ou les privilèges du groupe d'applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Privilèges des applications** de la fenêtre **Prévention des intrusions** s'ouvre.
4. Sélectionnez le groupe de confiance ou le groupe d'applications requis.
5. Dans le menu contextuel du groupe de confiance ou du groupe d'applications, sélectionne l'option **Autorisations pour le groupe**.

   La fenêtre **Règles de contrôle du groupe d'applications** s'ouvre.
6. Dans la fenêtre **Règles de contrôle du groupe d'applications**, exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et registre système** pour modifier les privilèges du groupe de confiance ou les privilèges du groupe d'applications qui régissent les privilèges du groupe de confiance ou du groupe d'applications relatives aux opérations avec le registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.
   - Sélectionnez l'onglet **Privilèges** pour modifier les privilèges du groupe de confiance ou les privilèges du groupe d'applications qui régissent les privilèges du groupe de confiance ou du groupe d'applications relatifs à l'accès aux processus et aux objets du système d'exploitation.
7. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.
8. Sélectionnez l'option souhaitée dans le menu contextuel.

   - **Hériter**
   - **Autoriser**

- **Bloquer**
- **Consigner dans le rapport**

> Si vous modifiez les règles de contrôle du groupe de confiance, l'option **Hériter** est inaccessible.

9. Cliquez sur le bouton **OK**.
10. Dans la fenêtre **Prévention des intrusions**, cliquez sur le bouton **OK**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification des privilèges de l'application

Par défaut, les paramètres des privilèges des applications qui font partie du groupe d'applications ou de groupe de confiance héritent des valeurs des paramètres des privilèges du groupe de confiance. Vous pouvez modifier les paramètres des privilèges des applications.

Pour modifier les privilèges d'une application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Privilèges des applications** de la fenêtre **Prévention des intrusions** s'ouvre.
4. Sélectionnez l'application requise.
5. Exécutez une des actions suivantes :

   - Dans le menu contextuel de l'application, sélectionnez l'option **Autorisations des applications**.
   - Cliquez sur le bouton **Avancé** dans le coin inférieur droit de l'onglet **Privilèges des applications**.

   La fenêtre **Autorisations des applications** s'ouvre.
6. Dans la fenêtre **Autorisations des applications**, exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et registre système** pour modifier les privilèges des applications qui régissent les privilèges de l'application relatifs aux opérations sur la base de registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.
   - Sélectionnez l'onglet **Privilèges** pour modifier les règles de contrôle de l'application qui régissent les privilèges de l'application relatifs à l'accès aux processus et à d'autres objets du système d'exploitation.
7. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.

8. Sélectionnez l'option souhaitée dans le menu contextuel.
    - **Hériter**
    - **Autoriser**
    - **Bloquer**
    - **Consigner dans le rapport**
9. Cliquez sur le bouton **OK**.
10. Dans la fenêtre **Applications**, cliquez sur **OK**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Désactivation du téléchargement et de la mise à jour des privilèges des applications depuis la base de Kaspersky Security Network

Par défaut, lors de la détection dans la base de Kaspersky Security Network de nouvelles informations sur l'application, Kaspersky Endpoint Security applique pour cette application les privilèges téléchargés depuis la base de KSN. Ensuite, vous pourrez modifier manuellement les privilèges de l'application.

Si l'application ne figurait pas dans la base de Kaspersky Security Network au moment de la première exécution de l'application, mais que les informations la concernant ont été ajoutées par la suite à la base de Kaspersky Security Network, Kaspersky Endpoint Security met à jour automatiquement par défaut les privilèges de cette application.

Vous pouvez désactiver le téléchargement des privilèges des applications depuis les bases de Kaspersky Security Network et la mise à jour automatique des privilèges pour les applications jusqu'alors inconnues.

Pour désactiver le téléchargement et la mise à jour des privilèges des applications depuis la base de Kaspersky Security Network, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

    Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.
3. Décochez la case **Mettre à jour les autorisations pour les applications inconnues depuis la base KSN**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Désactivation de l'héritage des restrictions du processus parent

L'utilisateur ou une autre application en cours d'exécution peut être à l'origine du lancement d'une application. Si l'application a été lancée par une autre, alors la séquence de lancement est composée des processus parent et fils.

Lorsque l'application tente d'accéder à la ressource contrôlée, le module Prévention des intrusions analyse les privilèges de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource protégée. Dans ce cas, ce sont les privilèges de priorité minimale qui sont appliqués : lorsque les privilèges d'accès de l'application et du processus parent sont comparés, les privilèges d'accès avec la priorité minimale sont appliqués à l'activité de l'application.

Priorité des privilèges d'accès :

1. **Autoriser** Ce droit d'accès a une priorité élevée.

2. **Interdire** Ce privilège d'accès a une priorité faible.

Ce mécanisme empêche l'utilisation d'applications de confiance par des applications douteuses ou dont les privilèges sont réduits pour exécuter des actions avec des privilèges.

Si l'activité de l'application est bloquée en raison de Privilèges insuffisants au niveau d'un des processus parents, vous pouvez modifier ces Privilèges ou désactiver l'héritage des restrictions du processus parent.

Pour désactiver l'héritage des restrictions du processus parent, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Applications**.

   L'onglet **Privilèges des applications** de la fenêtre **Prévention des intrusions** s'ouvre.

4. Sélectionnez l'application requise.

5. Dans le menu contextuel de l'application, sélectionnez l'option **Autorisations des applications**.

   La fenêtre **Autorisations des applications** s'ouvre.

6. Dans la fenêtre **Autorisations des applications** qui s'ouvre, sélectionnez l'onglet **Exclusions**.

7. Cochez la case **Ne pas hériter les restrictions du processus parent (application)**.

8. Cliquez sur le bouton **OK**.

9. Dans la fenêtre **Applications**, cliquez sur **OK**.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Exclusion de certaines actions des applications des privilèges des applications des applications

Pour exclure certaines actions des applications des privilèges des applications, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Applications**.

   L'onglet **Privilèges des applications** de la fenêtre **Prévention des intrusions** s'ouvre.

4. Sélectionnez l'application requise.

5. Dans le menu contextuel de l'application, sélectionnez l'option **Autorisations des applications**.

   La fenêtre **Autorisations des applications** s'ouvre.

6. Sélectionnez l'onglet **Exclusions**.

7. Cochez les cases en regard des actions de l'application à ne pas contrôler.

8. Cliquez sur le bouton **OK**.

9. Dans la fenêtre **Applications**, cliquez sur **OK**.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression des privilèges obsolètes des applications

Kaspersky Endpoint Security surveille le fonctionnement des applications à l'aide des privilèges d'application. Les privilèges d'une application sont déterminés par un groupe de confiance. Kaspersky Endpoint Security place l'application dans un groupe de confiance au premier lancement. Vous pouvez modifier manuellement le groupe de confiance de l'application. Vous pouvez également configurer manuellement les privilèges d'une application distincte. Ainsi, Kaspersky Endpoint Security stocke les informations suivantes sur l'application : groupe de confiance et privilèges de l'application.

Kaspersky Endpoint Security supprime automatiquement les informations sur les applications non utilisées afin d'économiser les ressources de l'ordinateur. Kaspersky Endpoint Security supprime les informations relatives aux applications conformément aux règles suivantes :

- Si le groupe de confiance et les privilèges sont déterminés automatiquement, Kaspersky Endpoint Security supprime les informations relatives à cette application après 30 jours. Il n'est pas possible de modifier la durée de conservation des informations relatives à l'application ou de désactiver la suppression automatique.

- Si vous avez placé manuellement l'application dans un groupe de confiance ou configuré les droits d'accès, Kaspersky Endpoint Security supprime les informations relatives à cette application au bout de 60 jours (valeur par défaut). Vous pouvez modifier la durée de conservation des informations relatives à l'application ou désactiver la suppression automatique (cf. les instructions ci-dessous).

Lorsque vous lancez une application dont les informations ont été supprimées, Kaspersky Endpoint Security examine l'application comme au premier lancement.

Pour configurer la suppression automatique des informations relatives aux applications non utilisées, procédez comme suit :

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

2. Dans la fenêtre des paramètres de l'application, sélectionnez la section **Protection avancée → Prévention des intrusions**.

3. Exécutez une des actions suivantes :

   - Si vous souhaitez configurer la suppression automatique, cochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours** et indiquez le nombre de jours requis.

   - Si vous souhaitez désactiver la suppression automatique, décochez la case **Supprimer les privilèges des applications qui n'ont pas été lancées depuis plus de X jours**.

     Kaspersky Endpoint Security conservera pendant une durée indéterminée les informations relatives aux applications que vous avez placées manuellement dans le groupe de confiance ou pour lesquelles vous avez configuré des privilèges d'accès. Kaspersky Endpoint Security supprime uniquement les informations relatives aux applications pour lesquelles un groupe de confiance et des privilèges sont automatiquement déterminés.

4. Enregistrez vos modifications.

Protection des ressources du système d'exploitation et des données personnelles

Le module Prévention des intrusions gère les privilèges des applications relatifs aux opérations sur différentes catégories de ressources du système d'exploitation et de données personnelles.

Les experts de Kaspersky ont sélectionné des catégories de ressources à protéger. Vous ne pouvez pas modifier ou supprimer les catégories préinstallées de ressources à protéger et des ressources protégées connexes.

Vous pouvez exécuter les opérations suivantes :

- ajouter une nouvelle catégorie de ressources protégées ;
- ajouter une nouvelle ressource protégée ;
- désactiver la protection de la ressource.

Ajout de la catégorie de ressources protégées

Pour ajouter une catégorie des ressources protégées, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Ressources**.

   L'onglet **Ressources protégées** de la fenêtre **Prévention des intrusions** s'ouvre.

4. Sélectionnez dans la partie gauche de l'onglet **Ressources protégées** la section ou la catégorie des ressources protégées dans laquelle vous souhaitez ajouter une nouvelle catégorie des ressources protégées.

5. Cliquez sur le bouton **Ajouter** et dans la liste déroulante choisissez l'option **Catégorie**.

   La fenêtre **Catégorie de ressources protégées** s'ouvre.

6. Saisissez dans la fenêtre **Catégorie de ressources protégées** le nom de la nouvelle catégorie des ressources protégées.

7. Cliquez sur le bouton **OK**.

   Un élément nouveau apparaît dans la liste des catégories des ressources protégées.

8. Dans la fenêtre **Prévention des intrusions**, cliquez sur le bouton **OK**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Après avoir ajouté une catégorie de ressources protégées, vous pouvez la modifier ou la supprimer en cliquant sur les boutons **Modifier** ou **Supprimer** dans la partie supérieure gauche de l'onglet **Ressources protégées**.

Ajout de la ressource protégée

Pour ajouter une ressource protégée, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Ressources**.

   L'onglet **Ressources protégées** de la fenêtre **Prévention des intrusions** s'ouvre.

4. Sélectionnez dans la partie gauche de l'onglet **Ressources protégées** la catégorie des ressources protégées à laquelle vous souhaitez ajouter une nouvelle ressource protégée.

5. Cliquez sur le bouton **Ajouter** et choisissez dans la liste déroulante le type de la ressource que vous voulez ajouter :

   - **Fichier ou dossier**.
   - **Clé de registre**.

   La fenêtre **Ressource protégée** s'ouvre.

6. Saisissez dans la fenêtre **Ressource protégée** dans le champ **Nom** le nom de la ressource protégée.

7. Cliquez sur le bouton **Parcourir**.

8. Définissez dans la fenêtre qui s'ouvre les paramètres requis en fonction du type de la ressource protégée ajoutée et cliquez sur **OK**.

9. Dans la fenêtre **Ressource protégée**, cliquez sur **OK**.

   Un nouvel élément s'affiche dans la liste des ressources protégées de la catégorie sélectionnée sous l'onglet **Ressources protégées**.

10. Dans la fenêtre **Prévention des intrusions**, cliquez sur le bouton **OK**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Après avoir ajouté une ressource protégée, vous pouvez la modifier ou la supprimer en cliquant sur les boutons **Modifier** ou **Supprimer** dans la partie supérieure gauche de l'onglet **Ressources protégées**.

Désactivation de la protection de la ressource

Pour désactiver la protection de la ressource, procédez comme suit :

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

2. Dans la section **Protection avancée** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Prévention des intrusions**.

   Les paramètres du module Prévention des intrusions s'affichent dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

   L'onglet **Ressources protégées** de la fenêtre **Prévention des intrusions** s'ouvre.

4. Exécutez une des actions suivantes :

   - Sélectionnez la ressource dans la liste des ressources protégées de la partie gauche de l'onglet dont vous souhaitez désactiver la protection et décochez la case en regarde de son nom.

   - Cliquez sur le bouton **Exclusions** et procédez comme suit :

     a. Dans la fenêtre **Exclusions**, cliquez sur le bouton **Ajouter**. Dans la liste déroulante, sélectionnez le type de ressource que vous souhaitez ajouter à la liste des exclusions de la protection du module Prévention des intrusions : **Fichier ou dossier** ou **Clé de registre**.

        La fenêtre **Ressource protégée** s'ouvre.

     b. Saisissez dans la fenêtre **Ressource protégée** dans le champ **Nom** le nom de la ressource protégée.

     c. Cliquez sur le bouton **Parcourir**.

     d. Définissez dans la fenêtre qui s'ouvre les paramètres requis en fonction du type de la ressource protégée que vous souhaitez ajouter à la liste des exclusions de la protection du module Prévention des intrusions.

     e. Cliquez sur le bouton **OK**.

     f. Dans la fenêtre **Ressource protégée**, cliquez sur **OK**.

        Dans la liste des ressources exclues de la protection du module Prévention des intrusions, un nouvel élément apparaît.

Après avoir ajouté une ressource à la liste des exclusions de la protection par le module Prévention des intrusions, vous pouvez la modifier ou la supprimer en cliquant sur les boutons **Modifier** ou **Supprimer** dans la partie supérieure de la fenêtre **Exclusions**.

g. Dans la fenêtre **Exclusions**, cliquez sur **OK**.

5. Dans la fenêtre **Prévention des intrusions**, cliquez sur le bouton **OK**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Réparation des actions malicieuses

Cette section contient des informations sur la Réparation des actions malicieuses et les instructions sur l'activation et la désactivation du module.

A propos de la Réparation des actions malicieuses

Le module Réparation des actions malicieuses permet à Kaspersky Endpoint Security d'exécuter le retour à l'état antérieur aux actions des applications malveillantes dans le système d'exploitation.

Lors de la restauration des actions du programme malveillant dans le système d'exploitation, Kaspersky Endpoint Security traite les types suivants d'activité de programme malveillant :

- **Activité de fichiers**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - suppression des fichiers exécutables créés par l'application malveillante (sur tous les supports, sauf les disques réseau) ;
  - suppression des fichiers exécutables créés par les applications dans lesquelles une application malveillante s'est introduite ;
  - restauration des fichiers modifiés ou supprimés par l'application malveillante.

  La fonction de restauration est soumise à une série de restrictions.

- **Activité sur la base de registre**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - suppression des sections et des clés de registre créées par l'application malveillante ;
  - non-restauration des sections et clés de registre modifiées ou supprimées par l'application malveillante.

- **Activité système**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - arrêt des processus lancés par l'application malveillante ;

- arrêt des processus dans lesquels l'application malveillante s'est introduite ;
- non-rétablissement des processus arrêtés par l'application malveillante.

- **Activité réseau**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - interdiction de l'activité réseau de l'application malveillante ;
  - interdiction de l'activité réseau des processus dans lesquels l'application malveillante s'est introduite.

L'annulation des actions de l'application malveillante peut être lancée par le module Protection contre les fichiers malicieux, Détection comportementale ou lors de la recherche de virus.

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cela n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

Restrictions de la fonction de restauration des fichiers

La fonction de restauration des fichiers possède les restrictions suivantes :

- L'application restaure les fichiers uniquement sur les périphériques dotés du système de fichiers NTFS et FAT32.
- L'application restaure les fichiers portant les extensions suivantes : odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Il est impossible de restaurer les fichiers installés sur les disques réseau, ainsi que sur les CD/DVD réinscriptibles.
- Il est impossible de restaurer les fichiers chiffrés à l'aide d'Encryption File System (EFS). Pour en savoir plus sur le fonctionnement d'EFS, consultez le *site de Microsoft*.
- L'application ne contrôle pas les modifications de fichiers exécutées par les procès au niveau du noyau du système d'exploitation.
- L'application ne contrôle pas les modifications des fichiers exécutées via l'interface réseau (par exemple, le fichier se trouve dans un dossier partagé et le procès est lancé à distance depuis un autre ordinateur).

Activation et désactivation de la Réparation des actions malicieuses

Pour activer ou désactiver la Réparation des actions malicieuses, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection avancée contre les menaces** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Réparation des actions malicieuses**.

3. Cochez la case **Réparation des actions malicieuses** dans la partie droite de la fenêtre si vous souhaitez que Kaspersky Endpoint Security annule les actions exécutées par les programmes malveillants dans votre système d'exploitation.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection contre les fichiers malicieux

Cette section contient des informations sur le module Protection contre les fichiers malicieux et les instructions sur la configuration du module.

A propos de la Protection contre les fichiers malicieux

Lors de l'ouverture ou du lancement d'un fichier dont le contenu sur OneDrive, Kaspersky Endpoint Security charge et analyse le contenu de ce fichier.

Le module Protection contre les fichiers malicieux permet d'éviter l'infection du système de fichiers de l'ordinateur. La Protection contre les fichiers malicieux est lancée par défaut au démarrage de Kaspersky Endpoint Security. Elle se trouve en permanence dans la mémoire vive de l'ordinateur et analyse les fichiers ouverts et exécutés sur l'ordinateur ainsi que sur les disques montés. Elle recherche les virus et autres applications présentant une menace. L'analyse est exécutée conformément aux paramètres de l'application.

En cas de détection d'une menace dans un fichier, Kaspersky Endpoint Security exécute les actions suivantes :

1. Détermine le type d'objet détecté dans le fichier (comme un *virus* ou un *cheval de Troie*).

2. L'application affiche une notification sur l'objet malveillant détecté dans le fichier (si les notifications sont configurées), et traite le fichier en prenant l'action précisée dans les paramètres du module Protection contre les fichiers malicieux.

Activation et désactivation de la Protection contre les fichiers malicieux

Par défaut, le module Protection contre les fichiers malicieux est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver la Protection contre les fichiers malicieux.

Pour activer ou désactiver le module Protection contre les fichiers malicieux, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.

3. Exécutez une des actions suivantes :

   - Cochez la case **Protection contre les fichiers malicieux** si vous souhaitez activer la Protection contre les fichiers malicieux.

- Décochez la case **Protection contre les fichiers malicieux** si vous souhaitez désactiver la Protection contre les fichiers malicieux.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suspension automatique de la Protection contre les fichiers malicieux

Vous pouvez configurer la suspension automatique de la Protection contre les fichiers malicieux à l'heure indiquée ou en cas d'utilisation d'applications spécifiques.

La suspension de la Protection contre les fichiers malicieux en cas de conflit avec certaines applications est une mesure extrême. Si des conflits apparaissent pendant l'utilisation du module, veuillez contacter le Support Technique de Kaspersky (https://companyaccount.kaspersky.com). Les experts vous aideront à garantir le fonctionnement de la Protection contre les fichiers malicieux avec d'autres applications sur votre ordinateur.

Pour configurer l'arrêt automatique du module Protection contre les fichiers malicieux, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module **Protection contre les fichiers malicieux**.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.

4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Suspension de la tâche**, procédez comme suit :

   - Cochez la case **Selon la planification** et cliquez sur le bouton **Planification** pour configurer la suspension automatique de la Protection contre les fichiers malicieux à l'heure indiquée.

     La fenêtre **Suspension de la tâche** s'ouvre.

   - Cochez la case **Au lancement des applications** et cliquez sur le bouton **Sélectionner** pour configurer la suspension automatique de la Protection contre les fichiers malicieux au lancement des applications indiquées.

     La fenêtre **Applications** s'ouvre.

6. Exécutez une des actions suivantes :

   - Pour configurer la suspension automatique de la Protection contre les fichiers malicieux à l'heure indiquée, dans la fenêtre **Suspension de la tâche** définissez à l'aide des champs **Suspendre à partir de** et **Reprendre à** la période (au format HH:MM) pendant laquelle il faut suspendre le fonctionnement de la Protection contre les fichiers malicieux. Cliquez sur le bouton **OK**.

   - Pour configurer la suspension automatique de la Protection contre les fichiers malicieux au lancement des applications indiquées, composez dans la fenêtre **Applications** à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer** la liste des applications dont l'utilisation nécessite la suspension de la Protection contre les fichiers malicieux. Cliquez sur le bouton **OK**.

7. Dans la fenêtre **Protection contre les fichiers malicieux** , cliquez sur **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la Protection contre les fichiers malicieux

Vous pouvez exécuter les opérations suivantes pour configurer le fonctionnement du module Protection contre les fichiers malicieux :

- Modifier le niveau de sécurité.

  Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

- Modifier l'action que le module Protection contre les fichiers malicieux exécute en cas de détection d'un fichier infecté.

- Composer la zone de protection du module Protection contre les fichiers malicieux.

  Vous pouvez élargir ou restreindre la zone de protection en ajoutant ou en supprimant des objets ou en modifiant le type de fichiers à analyser.

- Configurer l'utilisation de l'analyse heuristique.

  Pendant qu'il fonctionne, le module Protection contre les fichiers malicieux utilise la méthode d'analyse Machine learning et l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, le module Protection contre les fichiers malicieux compare l'objet trouvé aux signatures des bases antivirus de l'application. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, le module Protection contre les fichiers malicieux analyse l'activité des objets dans le système. L'Analyse heuristique permet de détecter des objets malveillants dont les enregistrements n'ont pas encore été ajoutés aux bases d'analyse contre les virus de l'application.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers avec le module Protection contre les fichiers malicieux : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

  Vous pouvez également activer les technologies iChecker et iSwift qui permettent d'optimiser la vitesse d'analyse des fichiers en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

- Configurer l'analyse des fichiers composés.

- Modifier le mode d'analyse des fichiers.

Modification du niveau de sécurité

Pour protéger le système de fichiers de l'ordinateur, le module Protection contre les fichiers malicieux utilise différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de sécurité*. Il existe trois niveaux prédéfinis de sécurité : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky.

Afin de modifier le niveau de sécurité, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.
3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour appliquer un des niveaux prédéfinis de sécurité (**Élevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Protection contre les fichiers malicieux** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité, le nom du niveau de sécurité des fichiers dans le groupe **Niveau de sécurité** devient **Autre**.
   - Pour sélectionner le niveau de sécurité **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action du module Protection contre les fichiers malicieux sur les objets infectés

Par défaut, le module Protection contre les fichiers malicieux tente de désinfecter tous les fichiers infectés détectés. Si la désinfection est impossible, le module Protection contre les fichiers malicieux supprime ces fichiers.

Pour modifier l'action que le module Protection contre les fichiers malicieux va exécuter sur les fichiers infectés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.
3. Dans le groupe **Action en cas de détection d'une menace** sélectionnez l'option requise :

   - **Désinfecter ; supprimer si la désinfection est impossible**.

     Si vous choisissez cette option, le module Protection contre les fichiers malicieux essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les fichiers malicieux supprime ces fichiers.
   - **Désinfecter ; bloquer si la désinfection est impossible**.

Si vous choisissez cette option, le module Protection contre les fichiers malicieux essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les fichiers malicieux bloque ces fichiers.

- **Interdire**.

  Si cette option est sélectionnée, le module Protection contre les fichiers malicieux bloque automatiquement les fichiers infectés sans tenter de les désinfecter.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition de la zone de protection du module Protection contre les fichiers malicieux

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection du module Protection contre les fichiers malicieux reprennent l'emplacement et le type de fichiers analysés. Par défaut, le module Protection contre les fichiers malicieux analyse uniquement les fichiers infectables et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques réseau de l'ordinateur.

Pour former la zone de protection, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.
4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Types de fichiers**, sélectionnez le type de fichiers que vous souhaitez analyser avec le module Protection contre les fichiers malicieux :

   - Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
   - Sélectionnez **Fichiers analysés par format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
   - Sélectionnez **Fichiers analysés par extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

   Au moment de choisir le type d'objet à analyser, il convient de ne pas oublier les éléments suivants :

   - La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, les formats EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.
   - Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné

l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si l'analyse des fichiers selon le format a été sélectionnée, le module Protection contre les fichiers malicieux analyse les en-têtes de fichier quelle que soit l'extension. Cette analyse peut révéler que le fichier est au format EXE. Un tel fichier est scrupuleusement analysé sur les virus et sur d'autres programmes présentant une menace.

6. La liste **Zone de protection** permet d'effectuer une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** pour ajouter un nouvel objet à la zone d'analyse.
   - Pour modifier l'emplacement de l'objet, sélectionnez-le dans la zone d'analyse et cliquez sur le bouton **Modifier**.

   La fenêtre **Sélection de la zone d'analyse** s'ouvre.

   - Pour supprimer l'objet de la liste des objets analysés, sélectionnez-le dans la liste des objets analysés et cliquez sur le bouton **Supprimer**.

     La fenêtre de confirmation de suppression s'ouvre.

7. Exécutez une des actions suivantes :

   - Pour ajouter un nouvel objet ou modifier l'emplacement de l'objet de la zone d'analyse, sélectionnez-le dans la fenêtre **Sélection de la zone d'analyse** et cliquez sur le bouton **Ajouter**.

     Tous les objets sélectionnés dans la fenêtre **Sélection de la zone d'analyse** sont affichés dans la liste **Zone de protection** dans la fenêtre **Protection contre les fichiers malicieux**.

     Cliquez sur le bouton **OK**.

   - Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

8. Le cas échéant, répétez les points 6-7 pour ajouter, modifier l'emplacement ou supprimer les objets de la liste des objets à analyser.

9. Pour exclure l'objet de la liste des objets analysés, décochez la case en regard de l'objet dans la liste **Zone de protection**. Dans ce cas, l'objet reste dans la liste des objets analysés mais il est exclu de l'analyse du module Protection contre les fichiers malicieux.

10. Dans la fenêtre **Protection contre les fichiers malicieux** , cliquez sur **OK**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les fichiers malicieux

Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les fichiers malicieux, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.

4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Performance**.

5. Dans le groupe **Méthodes d'analyse**, procédez comme suit :

   - Si vous voulez que le module Protection contre les fichiers malicieux utilise l'analyse heuristique, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

   - Si vous ne souhaitez pas que le module Protection contre les fichiers malicieux n'utilise pas l'analyse heuristique, décochez la case **Analyse heuristique**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des technologies d'analyse dans le cadre du fonctionnement du module Protection contre les fichiers malicieux

Pour configurer l'utilisation des technologies d'analyse dans le fonctionnement du module Protection contre les fichiers malicieux, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.

4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Technologies d'analyse**, procédez comme suit :

   - Cochez les cases en regard des noms des technologies que vous voulez utiliser dans le cadre du fonctionnement de la Protection contre les fichiers malicieux.

   - Décochez les cases en regard des noms des technologies que vous ne voulez pas utiliser dans le cadre du fonctionnement de la Protection contre les fichiers malicieux.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Optimisation de l'analyse des fichiers

Pour optimiser l'analyse des fichiers, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.
4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Performance**.
5. Dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données de messagerie est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulés de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limites le cercle des fichiers composés analysés pour accélérer l'analyse.

Le mode de traitement du fichier composé infecté (désinfection ou suppression) dépend du type de fichier.

Le module Protection contre les fichiers malicieux désinfecte les fichiers composés des formats RAR, ARJ, ZIP, CAB, LHA et supprime les fichiers de tous les autres formats (à l'exception des bases de messagerie).

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.
3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.
4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Performance**.
5. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets d'installation ou fichiers au format Office.

6. Pour analyser uniquement les nouveaux fichiers composés ou les fichiers composés modifiés, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

   Le module Protection contre les fichiers malicieux analyse uniquement les nouveaux fichiers composés et les fichiers composés modifiés de tout type.

7. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

8. Dans le groupe **Analyse en arrière-plan**, exécutez une des actions suivantes :

   - Pour empêcher que le module Protection contre les fichiers malicieux ne décompresse les fichiers composés en arrière-plan, décochez la case **Décompresser les fichiers composés en arrière-plan**.
   - Pour autoriser le module Protection contre les fichiers malicieux à décompresser les fichiers composés en arrière-plan, cochez la case **Décompresser les fichiers composés en arrière-plan**, puis indiquez la valeur requise dans le champ **Taille minimale du fichier**.

9. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Pour empêcher que le module Protection contre les fichiers malicieux ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**. Le module Protection contre les fichiers malicieux ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.
   - Pour autoriser le module Protection contre les fichiers malicieux à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

     Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

   Le module Protection contre les fichiers malicieux analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

10. Cliquez sur le bouton **OK**.

11. Dans la fenêtre **Protection contre les fichiers malicieux** , cliquez sur **OK**.

12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du mode d'analyse des fichiers

Le *mode d'analyse* désigne la condition qui doit être remplie pour que le module Protection contre les fichiers malicieux commencer à analyser les fichiers. Par défaut, Kaspersky Endpoint Security utilise le mode intelligent d'analyse des fichiers. Dans ce mode d'analyse des fichiers, le module Protection contre les fichiers malicieux prend une décision sur la base de l'analyse des opérations exécutées par l'utilisateur, par l'application au nom de l'utilisateur (sous les données duquel la connexion au système d'exploitation a eu lieu, ou sous les données d'un autre utilisateur) ou par le système d'exploitation sur les fichiers. Par exemple, dans le cas d'un fichier Microsoft Office Word, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires de réinscription du fichier sont exclues de l'analyse.

Afin de modifier le mode d'analyse des fichiers, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les fichiers malicieux**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les fichiers malicieux.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les fichiers malicieux** s'ouvre.

4. Dans la fenêtre **Protection contre les fichiers malicieux**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Mode d'analyse**, sélectionnez le mode requis :

   - **Intelligente**.
   - **Ouverture et modification**.
   - **A l'accès**.
   - **A l'exécution**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection contre les menaces Internet

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Windows pour serveurs de fichiers.

Cette section contient des informations sur le module Protection contre les menaces Internet et les instructions sur la configuration du module.

A propos de la Protection contre les menaces Internet

Chaque fois que l'utilisateur travaille sur Internet, les informations enregistrées sur son ordinateur sont exposées à un risque d'infection par des virus et par d'autres applications présentant une menace. Ces menaces peuvent s'introduire dans l'ordinateur lors du téléchargement d'applications gratuites ou lors de la consultation de sites Internet, attaqués par des individus malintentionnés, avant la visite de l'utilisateur. Les vers de réseau peuvent s'introduire sur l'ordinateur des utilisateurs avant l'ouverture des pages Internet ou le téléchargement d'un fichier, directement au moment de la connexion à Internet.

Le module Protection contre les menaces Internet protège les informations qui arrivent sur l'ordinateur des utilisateurs et qui sont envoyées depuis celui-ci via les protocoles HTTP et FTP. Il permet également de déterminer si un lien est malveillant ou s'il mène à un site de phishing.

Chaque page Internet ou fichier auquel accède l'utilisateur ou une application via le protocole HTTP ou FTP est intercepté et analysé par le module Protection contre les menaces Internet pour détecter la présence éventuelle de virus et d'autres applications présentant une menace. Ensuite, l'application procède ainsi :

- Si aucun code malveillant n'a été détecté sur la page Internet ou dans le fichier, ils deviennent immédiatement accessibles à l'utilisateur.
- Si la page Internet ou le fichier que souhaite ouvrir l'utilisateur contient un code malveillant, l'application exécute l'action définie dans les paramètres de la Protection contre les menaces Internet.

Activation et désactivation de la Protection contre les menaces Internet

Par défaut, le module Protection contre les menaces Internet est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver le module Protection contre les menaces Internet.

Pour activer ou désactiver le module Protection contre les menaces Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.
3. Exécutez une des actions suivantes :
   - Cochez la case **Protection contre les menaces Internet** si vous voulez activer le module Protection contre les menaces Internet.
   - Décochez la case **Protection contre les menaces Internet** si vous voulez désactiver le module Protection contre les menaces Internet.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la Protection contre les menaces Internet

Vous pouvez exécuter les opérations suivantes pour configurer le module Protection contre les menaces Internet :

- Modifier le niveau de sécurité du trafic Internet.

  Vous pouvez sélectionner un des niveaux prédéfinis de protection du trafic Internet reçus ou envoyés via les protocoles HTTP et FTP, ou personnaliser le niveau de sécurité du trafic Internet.

  Après avoir modifié les paramètres du niveau de sécurité du trafic Internet, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du trafic Internet.
- Modifier l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants du trafic Internet.

  Si l'analyse d'un objet du trafic Internet par le module Protection contre les menaces Internet détermine la présence d'un code malveillant, la suite des opérations du module Protection contre les menaces Internet dépend de l'action que vous avez définie.
- Configurer l'analyse des liens par le module Protection contre les menaces Internet selon les bases des adresses Internet de phishing et malveillantes.
- Configurer l'utilisation de l'analyse heuristique pour rechercher la présence éventuelle de virus et d'autres applications dangereuses dans le trafic Internet.

Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier les menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

- Configurer l'utilisation de l'analyse heuristique lors de la recherche d'éventuels liens de phishing sur les pages Internet.

- Optimiser l'analyse par le module Protection contre les menaces Internet du trafic Internet sortant et entrant via les protocoles HTTP et FTP.

- Composer la liste des URL de confiance.

  Vous pouvez composer une liste des URL dont vous faites confiance au contenu. Le module Protection contre les menaces Internet ne recherche pas la présence éventuelle de virus et d'autres applications présentant une menace dans les informations en provenance des adresses Internet de confiance. Cette fonctionnalité peut être utilisée, par exemple, si le module Protection contre les menaces Internet empêche le téléchargement d'un fichier depuis un site Internet que vous connaissez.

  Le terme URL signifie à la fois l'URL d'une page Internet et celle d'un site Internet.

Modification du niveau de sécurité du trafic Internet

Pour protéger les données reçues ou envoyées via les protocoles HTTP et FTP, le module Protection contre les menaces Internet utilise différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de protection du trafic Internet*. Il existe trois niveaux prédéfinis de protection du trafic Internet : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité du trafic Internet **Recommandé** sont considérés comme optimaux et sont recommandés par les experts de Kaspersky.

Afin de modifier le niveau de sécurité du trafic Internet, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.

3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour définir un des niveaux prédéfinis de protection du trafic Internet (**Élevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.

   - Pour personnaliser le niveau de sécurité du trafic Internet, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Protection contre les menaces Internet** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité du trafic Internet, le nom du niveau de sécurité du trafic Internet dans le groupe **Niveau de sécurité** devient **Autre**.

   - Pour sélectionner le niveau de sécurité du trafic Internet **Recommandé**, cliquez sur le bouton **Par défaut**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action à effectuer sur les objets malveillants du trafic Internet

Par défaut, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet et affiche sur l'écran une fenêtre de notification sur le blocage.

Pour modifier l'action sur les objets malveillants du trafic Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.
3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants du trafic Internet :

   - **Interdire le téléchargement**.

     Si cette option a été sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet, affiche sur l'écran une fenêtre de notification sur le blocage et consigne dans le journal une entrée contenant les informations relatives à l'objet infecté.

   - **Notifier**.

     Si vous choisissez cette option, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet autorise le chargement de cet objet sur l'ordinateur et Kaspersky Endpoint Security ajoute au journal une entrée contenant des informations sur l'objet infecté et ajoute les informations relatives à l'objet infecté à la liste des menaces actives.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des liens par rapport aux bases d'adresses Internet de phishing ou malveillantes à l'aide du module Protection contre les menaces Internet

La vérification des liens pour contrôler leur appartenance aux URL de phishing permet d'éviter les *attaques de phishing*. L'exemple type en est le message électronique prétendument envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel de la banque. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site Internet de phishing peut figurer non seulement dans un message électronique, mais également dans un message ICQ, le module Protection contre les menaces Internet contrôle les tentatives d'accès à un site de phishing au niveau de l'analyse du trafic Internet et bloque l'accès à ces sites Internet. La liste des adresses de phishing est reprise dans la distribution de Kaspersky Endpoint Security.

Pour configurer l'analyse des liens selon les bases des adresses Internet malveillantes ou de phishing à l'aide du module Protection contre les menaces Internet, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces Internet** s'ouvre.

4. Dans la fenêtre **Protection contre les menaces Internet**, sélectionnez l'onglet **Général**.

5. Procédez comme suit :

   - Cochez la case **Analyser les liens selon la base des URL malveillantes** dans groupe **Méthodes d'analyse** si vous souhaitez que le module Protection contre les menaces Internet analyse les liens selon la base des adresses Internet malveillantes.

     Kaspersky Endpoint Security analyse les liens par rapport à la base des adresses Internet malveillantes, même si le trafic réseau est transmis via une connexion sécurisée et si la case **Analyser les connexions sécurisées** est décochée.

   - Cochez la case **Analyser les liens selon la base des URL de phishing** dans le groupe **Paramètres de l'Anti-Phishing**, si vous souhaitez que le module Protection contre les menaces Internet analyse les liens selon la base des adresses Internet de phishing.

   Pour analyser les liens, vous pouvez également utiliser les bases de données de réputation de Kaspersky Security Network.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation de l'analyse heuristique dans le fonctionnement du module Protection contre les menaces Internet

Pour configurer l'utilisation de l'analyse heuristique, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces Internet** s'ouvre.

4. Choisissez l'onglet **Général**.

5. Si vous souhaitez que le module Protection contre les menaces Internet utilise l'analyse heuristique lors de l'analyse du trafic Internet à la recherche de virus et d'autres applications qui constituent une menace, cochez la case **Analyse heuristique pour détecter les virus** pour détecter les virus dans le groupe **Méthodes**

d'analyse et définissez le niveau de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.

6. Si vous voulez que le module Protection contre les menaces Internet utilise l'analyse heuristique pour rechercher la présence éventuelle de liens de phishing dans les pages Internet, cochez la case **Analyse heuristique pour détecter les liens de phishing** dans le groupe **Paramètres de l'Anti-Phishing**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Constitution d'une liste des URL de confiance

Pour composer une liste d'URL de confiance, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces Internet**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces Internet.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces Internet** s'ouvre.

4. Sélectionnez l'onglet **URL de confiance**.

5. Cochez la case **Ne pas analyser le trafic Internet en provenance des adresses URL de confiance**.

6. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable. Pour enrichir la liste, procédez comme suit :

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

      La fenêtre **Adresse Internet/Masque d'adresse Internet** s'ouvre.

   b. Saisissez l'adresse du site Internet/de la page Internet ou le masque d'adresse du site Internet/de la page Internet.

   c. Cliquez sur le bouton **OK**.

      Un nouvel enregistrement apparaîtra dans la liste des adresses Internet de confiance.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection contre les menaces par emails

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Windows pour serveurs de fichiers.

Cette section contient des informations sur le module Protection contre les menaces par emails et les instructions sur la configuration du module.

A propos de la Protection contre les menaces par emails

Le module Protection contre les menaces par emails analyse l'ensemble des messages électroniques entrants et sortants à la recherche d'éventuels virus et d'autres applications présentant une menace. Il démarre au lancement de Kaspersky Endpoint Security, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages reçus ou envoyés via les protocoles POP3, SMTP, IMAP, MAPI et NNTP. Si aucune menace n'a été détectée dans le message électronique, le message devient accessible et/ou est traité.

En cas de détection d'une menace dans le message électronique, le module Protection contre les menaces par emails exécute les actions suivantes :

1. Il attribue l'état *Infecté* au message électronique.

   Cet état est attribué au message électronique dans les cas suivants :

   - Si l'analyse du message électronique a détecté un segment de code d'un virus connu au sujet duquel les bases antivirus de Kaspersky Endpoint Security contiennent des informations.
   - Si le message électronique contient un segment de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

2. Il identifie le type d'objet détecté dans le message électronique (par exemple, virus, *cheval de Troie*).
3. Il bloque le message électronique.
4. Il affiche à l'écran une notification sur la détection d'un objet (si cela a été défini dans les paramètres des notifications).
5. Il exécute l'action définie dans les paramètres du composant Protection contre les menaces par emails.

Le module interagit avec les clients de messagerie installés sur l'ordinateur. Une extension intégrable est disponible pour le client de messagerie Microsoft Office Outlook® qui vous permet d'affiner les paramètres d'analyse des messages. L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

Activation et désactivation de la Protection contre les menaces par emails

Par défaut, le module Protection contre les menaces par emails est activé et fonctionne dans le mode recommandé par les experts de Kaspersky. Le cas échéant, vous pouvez désactiver le module Protection contre les menaces par emails.

Pour activer ou désactiver le module Protection contre les menaces par emails, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.

3. Exécutez une des actions suivantes :

   - Cochez la case **Protection contre les menaces par emails** si vous souhaitez activer la Protection contre les menaces par email.
   - Décochez la case **Protection contre les menaces par emails** pour désactiver la Protection contre les menaces par email.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la Protection contre les menaces par emails

Vous pouvez exécuter les opérations suivantes pour configurer le fonctionnement du module Protection contre les menaces par emails :

- Modifier le niveau de sécurité du courrier.

  Vous pouvez sélectionner un des niveaux de protection prédéfinis pour le courrier ou personnaliser le niveau de sécurité du courrier.

  Après avoir modifié les paramètres du niveau de sécurité du courrier, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité du courrier.

- Modifier l'action que Kaspersky Endpoint Security exécute sur les messages infectés.
- Composer la zone de protection du module Protection contre les menaces par emails.
- Configurer l'analyse des fichiers composés joints aux messages électroniques.

  Vous pouvez activer ou désactiver l'analyse des objets joints aux messages, limiter la taille maximale des objets à analyser joints aux messages et la durée maximale d'analyse des objets joints aux messages.

- Configurer le filtrage selon le type de pièces jointes dans les messages électroniques.

  Le filtrage selon le type de pièces jointes des messages permet de renommer ou de supprimer automatiquement les fichiers des types indiqués.

- Configurer l'utilisation de l'analyse heuristique.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier dans les messages les menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

- Configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook.

  Il existe pour le client de messagerie Microsoft Office Outlook une extension qui permet de configurer facilement les paramètres d'analyse du courrier.

  Lorsqu'il fonctionne avec d'autres clients de messagerie, y compris Microsoft Outlook Express®, Windows Mail et Mozilla™ Thunderbird™, le module Protection contre les menaces par emails analyse le trafic des protocoles de messagerie SMTP, POP3, IMAP et NNTP.

Lorsqu'il s'agit du client de messagerie Mozilla Thunderbird, le module Protection contre les menaces par emails ne recherche pas des virus et d'autres programmes présentant une menace dans les messages transmis via le protocole IMAP en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

Modification du niveau de sécurité du courrier

Le module Protection contre les menaces par emails utilise différents ensembles de paramètres afin de protéger votre courrier. Ces ensembles de paramètres sont appelés *niveaux de protection du courrier*. Il existe trois niveaux prédéfinis de sécurité du courrier : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité du courrier **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky.

Afin de modifier le niveau de sécurité du courrier, exécutez l'opération suivante :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.
3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour définir un des niveaux prédéfinis de protection du courrier (**Élevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité du courrier, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Protection contre les menaces par emails** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité du courrier, le nom du niveau de sécurité du courrier dans le groupe **Niveau de sécurité** devient **Autre**.
   - Pour sélectionner le niveau de sécurité du courrier **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action exécutée sur les messages électroniques infectés

Par défaut, le module Protection contre les menaces par emails tente de désinfecter tous les messages électroniques infectés détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails supprime les messages électroniques infectés.

Pour modifier l'action à exécuter sur les messages électroniques infectés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.

3. Dans le groupe **Action en cas de détection d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un message infecté :

   - **Désinfecter ; supprimer si la désinfection est impossible**.

     Si vous choisissez cette option, le module Protection contre les menaces par emails essaie de désinfecter automatiquement tous les messages électroniques infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails supprime les messages électroniques infectés.

   - **Désinfecter ; bloquer si la désinfection est impossible**.

     Si vous choisissez cette option, le module Protection contre les menaces par emails essaie de désinfecter automatiquement tous les messages électroniques infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails bloque les messages électroniques infectés.

   - **Interdire**.

     Si cette option est sélectionnée, le module Protection contre les menaces par emails bloque automatiquement les messages électroniques infectés sans tenter de les désinfecter.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition de la zone de protection du module Protection contre les menaces par emails

La zone de protection désigne les objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection du module Protection contre les menaces par emails reprennent les paramètres de l'intégration du module Protection contre les menaces par emails, le type de messages électroniques et les protocoles de messagerie dont le trafic est analysé par la Protection contre les menaces par emails. Par défaut, Kaspersky Endpoint Security analyse les messages électroniques entrant et sortant, le trafic des protocoles de courrier électronique POP3, SMTP, NNTP et IMAP, et s'intègre au client de messagerie Microsoft Office Outlook.

Pour former la zone de protection du module Protection contre les menaces par emails, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces par emails** s'ouvre.

4. Choisissez l'onglet **Général**.

5. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :

   - Sélectionnez l'option **Analyser les messages entrants et sortants** si vous souhaitez que le module Protection contre les menaces par emails analyse tous les messages entrants et sortants sur votre ordinateur.

- Sélectionnez l'option **Analyser uniquement les messages entrants** si vous souhaitez que le module Protection contre les menaces par emails analyse uniquement les messages entrants sur votre ordinateur.

  Si vous sélectionnez l'analyse des messages entrants uniquement, il est recommandé d'analyser une fois tous les messages sortants car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

6. Dans le groupe **Intégration au système** procédez comme suit :

   - Cochez la case **Trafic POP3/SMTP/NNTP/IMAP** si vous souhaitez que le module Protection contre les menaces par emails analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur.

     Décochez la case **Trafic POP3/SMTP/NNTP/IMAP** si vous ne souhaitez pas que le module Protection contre les menaces par emails analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur. Dans ce cas, les messages sont analysés par l'extension du module Protection contre les menaces par emails installée dans le client de messagerie Microsoft Office Outlook après réception sur l'ordinateur de l'utilisateur, si la case **Avancé : extension dans Microsoft Office Outlook**.

     Si vous utilisez un autre client de messagerie que Microsoft Office Outlook, quand la case **Trafic POP3/SMTP/NNTP/IMAP** est décochée, le module Protection contre les menaces par emails n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP.

   - Cochez la case **Avancé : extension dans Microsoft Office Outlook** si vous souhaitez donner l'accès à la configuration du module Protection contre les menaces par emails depuis l'application Microsoft Office Outlook et activer l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur à l'aide de l'extension dans l'application Microsoft Office Outlook.

     Décochez la case **Avancé : extension dans Microsoft Office Outlook**, si vous souhaitez bloquer l'accès à la configuration des paramètres du module Protection contre les menaces par emails depuis l'application Microsoft Office Outlook et désactiver l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur à l'aide de l'extension dans l'application Microsoft Office Outlook.

     L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés joints aux messages électroniques

Pour configurer l'analyse des fichiers composés joints aux messages électroniques, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces par emails** s'ouvre.

4. Choisissez l'onglet **Général**.

5. Dans le groupe **Analyse des fichiers composés**, procédez comme suit :

   - Décochez la case **Analyser les archives jointes** si vous ne souhaitez pas que le module Protection contre les menaces par emails analyse les archives jointes aux messages.
   - Décochez la case **Analyser les fichiers joints aux formats Office** si vous ne souhaitez pas que le module Protection contre les menaces par emails analyse les fichiers au format Office joints aux messages.
   - Cochez la case **Ne pas analyser les archives de plus de N Mo** si vous ne souhaitez pas que le module Protection contre les menaces par emails analyse les archives de plus de N Mo jointes aux messages. Si vous avez coché cette case, indiquez la taille maximale des archives dans le champ à côté du nom de la case.
   - Décochez la case **Ne pas analyser les archives pendant plus de** N s si vous souhaitez que le module Protection contre les menaces par emails analyse les archives jointes aux messages si l'opération dure plus de N secondes.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Filtrage des pièces jointes dans les messages électroniques

La fonction de filtrage des pièces jointes ne s'applique pas aux messages électroniques sortants.

Les programmes malveillants peuvent se propager sous la forme des pièces jointes dans des messages électroniques. Vous pouvez configurer le filtrage selon le type des pièces jointes dans les messages de telle sorte qu'il soit possible de renommer ou de supprimer automatiquement les fichiers des types indiqués. En renommant une pièce jointe d'un type en particulier, Kaspersky Endpoint Security peut protéger votre ordinateur contre l'exécution d'un programme malveillant.

Pour configurer le filtrage des pièces jointes, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection contre les menaces par emails**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces par emails.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection contre les menaces par emails** s'ouvre.

4. Dans la fenêtre **Protection contre les menaces par emails**, sélectionnez l'onglet **Filtre des pièces jointes**.

5. Exécutez une des actions suivantes :

- Sélectionnez l'option **Désactiver le filtre** si vous ne souhaitez pas que le module Protection contre les menaces par emails filtre les pièces jointes dans les messages.

- Sélectionnez l'option **Renommer les types de pièces jointes indiqués** si vous souhaitez que le module Protection contre les menaces par emails change les noms des fichiers des **types indiqués** joints aux messages.

N'oubliez pas que le format réel du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

Si vous avez activé le filtrage des pièces jointes dans les messages électroniques, le module Protection contre les menaces par emails peut, à l'issue de celui-ci, renommer ou supprimer les fichiers portant les extensions suivantes :

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64 Ko ;

exe : fichier exécutable, archive autoextractible ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase™, Clipper ou Microsoft Visual FoxPro®, programme de la suite WAVmaker ;

bin : fichier binaire ;

bat : fichier de paquet ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compressée ;

dll : bibliothèque dynamique ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme qui fonctionne en mode de partage du temps ;

drv : pilote d'un périphérique quelconque ;

vxd : pilote d'un périphérique virtuel Microsoft Windows ;

pif : fichier contenant des informations sur un logiciel ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registre de Microsoft Windows ;

ini : fichier de configuration qui contient les données des paramètres pour Microsoft Windows, Windows NT et pour certaines applications ;

cla : classe Java ;

vbs : script Visual Basic® ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer® ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

eml : email de Microsoft Outlook Express ;

nws : nouvel email de Microsoft Outlook Express ;

msg : email de Microsoft Mail ;

plg : email ;

mbx : email Microsoft Office Outlook enregistré ;

doc* : documents Microsoft Office Word, par exemple, doc : document Microsoft Office Word, docx : document Microsoft Office Word 2007 compatible avec XML, docm : document Microsoft Office Word 2007 compatible avec les macros ;

dot* : modèles de document Microsoft Office Word, par exemple, dot : modèle de document Microsoft Office Word, dotx : modèle de document Microsoft Office Word 2007, dotm : modèle de document Microsoft Office Word 2007 compatible avec les macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Windows Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD® ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave® Flash ;

jpg, jpeg : fichier graphique de conservation de données compressées ;

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows. Les fichiers EMF ne sont pas pris en charge par Microsoft Windows 16 bit ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutables Microsoft Office Word ;

xl* : les documents et les fichiers de Microsoft Office Excel, tels que, xla : extension Microsoft Excel, xlc : schéma, xlt : modèle des documents, xlsx : feuille de calcul Microsoft Office Excel 2007, xltm : feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, xlsb : feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), xltx : modèle Microsoft Office Excel 2007, xlsm : modèle Microsoft Office Excel 2007 compatible avec les macros, xlam : modèle externe Microsoft Office Excel 2007 compatible avec les macros ;

pp* : les documents et les fichiers de Microsoft Office PowerPoint®, tels que, pps : diaporama Microsoft Office PowerPoint, ppt : présentation, pptx : présentation Microsoft Office PowerPoint 2007, pptm : présentation Microsoft Office PowerPoint 2007 compatible avec les macros, potx : modèle de présentation Microsoft Office PowerPoint 2007, potm : modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, ppsx : diaporama Microsoft Office PowerPoint 2007, ppsm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, ppam : module externe Microsoft Office PowerPoint 2007 compatible avec les macros ;

md* : documents et fichiers de Microsoft Office Access® tels que, mda : groupe de travail de Microsoft Office Access, mdb : base de données ;

sldx : diaporama Microsoft Office PowerPoint 2007 ;

sldm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros ;

thmx : thème Microsoft Office 2007.

- Sélectionnez l'option **Supprimer les types de pièces jointes indiqués** si vous souhaitez que le module Protection contre les menaces par emails supprime les fichiers des types indiqués joints aux messages.

6. Si à l'étape précédente des instructions vous avez choisi l'option **Renommer les types de pièces jointes indiqués** ou l'option **Supprimer les types de pièces jointes indiqués**, cochez les cases en regard des types de fichier requis.

   Vous pouvez modifier la liste des types de fichiers en utilisant les boutons **Ajouter**, **Modifier** et **Supprimer**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse du courrier dans Microsoft Office Outlook

L'intégration de l'extension du module Protection contre les menaces par emails à l'application Microsoft Office Outlook (ci-après Outlook) s'opère lors de l'installation de Kaspersky Endpoint Security. Cette extension permet de passer à la configuration des paramètres du module Protection contre les menaces par emails depuis l'application Outlook et d'indiquer le moment auquel il convient de rechercher parmi les messages électroniques la présence de virus et d'autres applications présentant une menace. L'extension du module Protection contre les menaces par emails pour Outlook peut analyser les messages entrants et sortants transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI.

L'extension du module Protection contre les menaces par emails prend en charge Outlook 2010, 2013, 2016, 2019.

La configuration du module Protection contre les menaces par emails depuis Outlook est disponible si la case **Avancé : extension dans Microsoft Office Outlook** est cochée dans l'interface de l'application Kaspersky Endpoint Security.

Dans l'application Outlook, les messages entrants sont d'abord analysés par le module Protection contre les menaces par emails (si la case **Trafic POP3/SMTP/NNTP/IMAP** est cochée dans l'interface de Kaspersky Endpoint Security), puis ils sont analysés par l'extension du module Protection contre les menaces par emails pour Outlook. Lorsque le module Protection contre les menaces par emails détecte un objet malveillant dans un message, il vous en avertit.

L'analyse des messages sortants est confiée d'abord à l'extension du module Protection contre les menaces par emails pour Outlook, puis au module Protection contre les menaces par emails.

Configuration de l'analyse du courrier dans l'application Outlook

Pour configurer l'analyse du courrier dans l'application Outlook 2007, procédez comme suit :

1. Ouvrez la fenêtre principale d'Outlook 2007.
2. Dans le menu de l'application, sélectionnez l'option **Service** → **Paramètres**.

   La fenêtre **Paramètres** s'ouvre.
3. Dans la fenêtre **Paramètres**, sélectionnez l'onglet **Protection du courrier**.

Pour configurer l'analyse du courrier dans l'application Outlook 2010/2013/2016, procédez comme suit :

1. Ouvrez la fenêtre principale d'Outlook.

   Dans le coin supérieur gauche, choisissez l'onglet **Fichier**.
2. Cliquez sur le bouton **Paramètres**.

   La fenêtre **Paramètres d'Outlook** s'ouvre.
3. Choisissez la section **Paramètres**.

   Les paramètres configurés dans les plug-ins d'Outlook apparaissent à droite.

4. Cliquez sur le bouton **Paramètres de configuration**.

Configuration de l'analyse du courrier via Kaspersky Security Center

En cas d'analyse du courrier à l'aide de l'extension du module Protection contre les menaces par emails pour Outlook, il est recommandé d'utiliser le Mode Exchange mis en cache (Use Cached Exchange Mode). Vous pouvez obtenir tous les détails sur le mode Exchange mis en cache et sur ses recommandations d'utilisation dans la base de connaissances de Microsoft : https://technet.microsoft.com/fr-fr/library/cc179175.aspx

Pour configurer le mode de fonctionnement de l'extension du module Protection contre les menaces par emails pour Outlook via Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez configurer l'analyse du courrier.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.
6. Dans la section **Protection principale**, sélectionnez la sous-section **Protection contre les menaces par emails**.
7. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.
   La fenêtre **Protection contre les menaces par emails** s'ouvre.
8. Cliquez sur le bouton **Configuration** dans le groupe **Intégration au système**.
   La fenêtre **Protection du courrier** s'ouvre.
9. Dans la fenêtre **Protection du courrier** procédez comme suit :
   - Cochez la case **Analyser à la réception** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages entrants au moment de leur arrivée dans la boîte aux lettres.
   - Cochez la case **Analyser à la lecture** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages entrants quand l'utilisateur les ouvre pour les lire.
   - Cochez la case **Analyser à l'envoi** si vous voulez que l'extension du module Protection contre les menaces par emails pour Outlook analyse les messages sortants au moment de leur envoi.
10. Dans la fenêtre **Protection du courrier**, cliquez sur **OK**.
11. Dans la fenêtre **Protection contre les menaces par emails**, cliquez sur **OK**.

12. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Protection contre les menaces réseau

Cette section contient des informations sur la Protection contre les menaces réseau et les instructions sur la configuration du module.

A propos de la Protection contre les menaces réseau

Le module Protection contre les menaces réseau recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque l'activité réseau de l'ordinateur attaquant. Un message vous avertit après qu'une tentative d'attaque réseau a été effectuée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

L'activité réseau de l'ordinateur à l'origine de l'attaque est bloquée pendant une heure. Vous pouvez modifier les paramètres du blocage de l'ordinateur attaquant.

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Endpoint Security. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la mise à jour des bases et des modules de l'application.

Activation et désactivation de la Protection contre les menaces réseau

Par défaut, la Protection contre les menaces réseau est activée et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver la Protection contre les menaces réseau.

Pour activer ou désactiver le module Protection contre les menaces réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces réseau.
3. Procédez comme suit :

   - Cochez la case **Protection contre les menaces réseau** pour activer la Protection contre les menaces réseau.
   - Décochez la case **Protection contre les menaces réseau** pour désactiver la Protection contre les menaces réseau.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la Protection contre les menaces réseau

Vous pouvez exécuter les opérations suivantes pour configurer le fonctionnement de la Protection contre les menaces réseau :

- configurer les paramètres de blocage de l'ordinateur à l'origine de l'attaque ;
- composer la liste des adresses à exclure du blocage.

Modification des paramètres de blocage de l'ordinateur à l'origine de l'attaque

Pour modifier les paramètres du blocage de l'ordinateur attaquant, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces réseau.
3. Cochez la case **Bloquer l'ordinateur à l'origine de l'attaque pendant**.

   Si cette case est cochée, lors de la détection d'une tentative d'attaque réseau, le module Protection contre les menaces réseau bloque l'activité réseau de l'ordinateur attaquant pendant la durée spécifiée. Cela protège automatiquement l'ordinateur contre d'éventuelles futures attaques réseau à partir de la même adresse.

   Si cette case est décochée, en cas de détection d'une tentative d'attaque réseau, le module Protection contre les menaces réseau n'active pas la protection automatique contre les futures attaques réseau possibles depuis cette adresse.
4. Pour modifier la durée du blocage de l'ordinateur attaquant, dans le champ qui se trouve à droite de la case **Bloquer l'ordinateur à l'origine de l'attaque pendant**.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration des adresses des exclusions du blocage

Pour configurer les adresses des exclusions du blocage, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces réseau.
3. Cliquez sur le bouton **Exclusions**.

   La fenêtre **Exclusions** s'ouvre.

4. Exécutez une des actions suivantes :

   - Si vous souhaitez ajouter une nouvelle adresse IP, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier une adresse IP ajoutée antérieurement, sélectionnez-la dans la liste des adresses, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Adresse IP** s'ouvre.

5. Saisissez l'adresse IP de l'ordinateur à l'origine des attaques réseaux qui ne devront pas être bloquées.
6. Dans la fenêtre **Adresse IP**, cliquez sur **OK**.
7. Dans la fenêtre **Exclusions**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification du mode de fonctionnement de la protection des attaques de type MAC spoofing

Le module Prévention des intrusions surveille les vulnérabilités dans le protocole ARP pour la falsification des adresses MAC des appareils.

Par défaut Kaspersky Endpoint Security ne traque pas les attaques de type MAC spoofing.

Pour modifier le mode de fonctionnement de la protection contre les attaques de type MAC spoofing, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Protection contre les menaces réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Protection contre les menaces réseau.

3. Dans le groupe **Mode de fonctionnement de la protection contre les attaques de type MAC Spoofing**, choisissez une des options suivantes :

   - **Ne pas suivre les attaques de type MAC spoofing**.
   - **Signaler tous les signes d'attaque de type MAC Spoofing**.
   - **Bloquer tous les signes d'attaque de type MAC Spoofing**.

Pare-feu

Cette section contient des informations sur le Pare-feu et les instructions sur la configuration des paramètres du module.

A propos du Pare-feu

Tout ordinateur connecté aux réseaux locaux et à l'Internet risque non seulement une infection par des virus et d'autres applications présentant une menace, mais il est aussi ouvert aux différentes attaques qui exploitent les vulnérabilités des systèmes d'exploitation et du logiciel.

Le Pare-feu garantit la protection des données personnelles stockées sur l'ordinateur de l'utilisateur, car il bloque la majorité des menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local. Le Pare-feu permet de détecter toutes les connexions réseau sur l'ordinateur de l'utilisateur et d'afficher une liste de leurs adresses IP en indiquant l'état de la connexion réseau par défaut.

Le module Pare-feu filtre toutes les activités du réseau en fonction des règles réseau. La configuration des règles réseau permet de définir le niveau de la protection de l'ordinateur qui peut varier entre un blocage complet de l'accès Internet et l'autorisation de l'accès illimité.

Activation et désactivation du Pare-feu

Par défaut, le Pare-feu est activé et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver le Pare-feu.

Pour activer ou désactiver le Pare-feu, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Pare-feu** pour activer le Pare-feu.
   - Décochez la case **Pare-feu** pour désactiver le Pare-feu.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles réseau

Les *règles réseau* sont des actions autorisées ou bloquées qui sont exécutées par le Pare-feu lors de la détection d'une tentative de connexion au réseau.

Le Pare-feu réalise la protection contre les différents types d'attaques réseau sur deux niveaux : niveau de réseau et niveau appliqué. La protection au niveau de réseau est assurée par l'application des règles pour les paquets réseau. La protection au niveau appliqué est garantie grâce à l'application de règles d'utilisation des ressources de réseau pour les applications installées sur l'ordinateur de l'utilisateur.

Les deux niveaux de protection du Pare-feu vous permettent de créer :

- *Règles pour les paquets réseau*. Elles sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Le Pare-feu définit certaines règles pour les paquets réseau par défaut.

- *Règles réseau de l'application* Elles sont utilisées pour limiter l'activité réseau d'une application spécifique. Elles tiennent compte non seulement des caractéristiques du paquet réseau, mais aussi de l'application spécifique destinataire ou expéditeur de ce paquet réseau. Ces règles permettent de configurer en détail le filtrage de l'activité réseau lorsque, par exemple, un type déterminé des connexions réseau est interdit pour certaines applications mais autorisé pour d'autres.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau pour les applications. Si des règles pour les paquets réseau et des règles réseau pour les applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Vous pouvez définir pour chacune des règles pour les paquets réseau et chacune des règles réseau pour les applications une priorité d'exécution spécifique.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau pour les applications. Si des règles pour les paquets réseau et des règles réseau pour les applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Les règles réseau des applications ont une particularité. Une règle réseau des applications comprend les règles d'accès selon l'état du réseau : *public*, *local*, *fiable*. Par exemple, pour le groupe de confiance « Restrictions élevées », toute activité réseau de l'application dans les réseaux de n'importe quel état est interdite. Si une règle réseau est définie pour une application individuelle (application parent), les processus enfants d'autres applications seront exécutés conformément à la règle réseau de l'application parent. S'il n'y a pas de règle réseau pour l'application, les processus enfant seront exécutés conformément à la règle d'accès aux réseaux du groupe de confiance.

Par exemple, vous avez interdit toute activité réseau de toutes les applications quel que soit l'état du réseau, sauf pour le navigateur X. Si vous lancez l'installation du navigateur Y (processus enfant) dans le navigateur X (processus parent), le programme d'installation du navigateur Y aura accès au réseau et téléchargera les fichiers requis. Après l'installation, le navigateur Y se verra refuser toutes les connexions réseau conformément aux paramètres du Pare-feu. Pour interdire l'activité réseau au programme d'installation du navigateur Y en tant que processus enfant, vous devez ajouter une règle réseau pour le programme d'installation du navigateur Y.

A propos des états de la connexion réseau

Le Pare-feu contrôle toutes les connexions réseau sur l'ordinateur de l'utilisateur et attribue automatiquement un état à toutes les connexions détectées.

Il existe les états suivant de la connexion réseau :

- **Réseau public**. Cet état a été développé pour les réseaux non protégés par des applications antivirus quelconques, des pare-feu, des filtres (ex : pour les réseaux des cafés Internet). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur d'accéder aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur. Le Pare-Feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.

  Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.

- **Réseau local**. Cet état a été développé pour les réseaux aux utilisateurs desquels vous faites suffisamment confiance pour autoriser l'accès aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).

- **Réseau de confiance**. Cet état a été développé pour un réseau sûr dont l'utilisation n'expose pas l'ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état n'importe quelle activité réseau dans le cadre de ce réseau.

Modification de l'état de la connexion réseau

Pour modifier l'état d'une connexion réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Réseaux disponibles**.

   La fenêtre **Pare-feu** s'ouvre.
4. Sélectionnez la connexion réseau dont vous souhaitez modifier l'état.
5. Dans le menu contextuel, choisissez l'option état de la connexion réseau :
   - **Réseau public**.
   - **Réseau local**.
   - **Réseau de confiance**.
6. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des règles pour les paquets réseau

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles pour les paquets réseau :

- Créer une nouvelle règle pour les paquets réseau.

  Vous pouvez créer une nouvelle règle pour les paquets réseau en sélectionnant un ensemble des conditions et des actions relatives aux paquets réseau et aux flux de données.
- Activer et désactiver la règle pour les paquets réseau.

  Toutes les règles pour les paquets réseau créés par défaut par le Pare-feu possèdent l'état *Activé*. Si la règle pour les paquets réseau est activée, le Pare-feu applique cette règle.

  Vous pouvez activer toute règle pour les paquets réseau, sélectionnée dans la liste des règles pour les paquets réseau. Si la règle pour les paquets réseau est désactivée, le Pare-feu suspend temporairement l'application de la règle.

  La nouvelle règle pour les paquets réseau créée par l'utilisateur est par défaut ajoutée à la liste des règles pour les paquets réseau avec l'état *Activé*.

- Modifier les paramètres de la règle pour les paquets réseau.

  Après avoir créé une nouvelle règle pour les paquets réseau, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle pour les paquets réseau.

  Dans la liste des règles pour les paquets réseau, vous pouvez modifier l'action que le Pare-feu exécute en cas de détection d'une activité réseau de la règle pour les paquets réseau indiquée.

- Modifier la priorité de la règle pour les paquets réseau.

  Vous pouvez augmenter ou diminuer la priorité de la règle pour les paquets réseau sélectionnée dans la liste.

- Supprimer la règle pour les paquets réseau.

  Vous pouvez supprimer la règle pour les paquets réseau si vous ne souhaitez pas que le Pare-feu applique cette règle en cas de détection d'une activité réseau et qu'elle soit affichée dans la liste des règles pour les paquets réseau avec l'état *Désactivé*.

Création et modification d'une règle pour les paquets réseau

Au moment de créer des règles pour les paquets réseau, il ne faut pas oublier qu'elles ont priorité sur les règles réseau pour les applications.

Pour créer ou modifier une règle pour les paquets réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.
4. La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

   Cet onglet contient la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.
5. Exécutez une des actions suivantes :

   - Si vous voulez créer une nouvelle règle pour les paquets réseau, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle pour les paquets réseau, sélectionnez-la dans la liste des règles pour les paquets réseau et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle réseau** s'ouvre.
6. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :

   - **Autoriser**
   - **Bloquer**

- **Selon les règles de l'application**.

7. Dans le champ **Nom**, indiquez le nom du service réseau d'une des manières suivantes :

   - Cliquez sur l'icône qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service réseau.

     La liste déroulante reprend les services de réseau décrivant les connexions réseau le plus souvent utilisées.

   - Dans le champ **Nom**, saisissez manuellement le nom du service réseau.

8. Indiquez le protocole de transfert des données :

   a. Cochez la case **Protocole**.

   b. Sélectionnez dans la liste déroulante le type de protocole dont il faut contrôler l'activité réseau.

      Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

   Si le service réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et il convient alors de sélectionner dans la liste déroulante à côté de la case le type de protocole qui correspond au service réseau sélectionné. La case **Protocole** est décochée par défaut.

9. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

   Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

   - **Entrant (paquet)**.
   - **Entrant**.
   - **Entrant/Sortant**
   - **Sortant (paquet)**.
   - **Sortant**.

10. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type ICMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code ICMP** et sélectionnez dans la liste déroulante le code ICMP.

11. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les numéros des ports (séparés par une virgule) de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de l'ordinateur de l'utilisateur.

12. Le tableau **Adaptateurs réseau** contient des informations relatives aux adaptateurs réseaux qui peuvent envoyer ou recevoir des paquets réseau. Utilisez pour ce faire les boutons **Ajouter**, **Modifier** et **Supprimer**.

13. Si vous voulez limiter le contrôle des paquets réseau selon leur durée de vie (TTL, Time to Live), cochez la case **TTL** et dans le champ en regard, définissez la plage de valeurs de durée de vie des paquets réseau envoyés et/ou reçus.

    La règle réseau contrôlera le transfert des paquets réseau dont la durée de vie ne dépasse pas la valeur indiquée.

Dans le cas contraire, décochez la case **TTL**.

14. Indiquez les adresses réseau des ordinateurs distants qui peuvent transmettre et/ou recevoir des paquets réseau. Pour ce faire, choisissez une des valeurs suivantes dans la liste **Adresses distantes** :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par les ordinateurs distants depuis n'importe quelle adresse IP.

    - **Adresses du sous-réseau**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par les ordinateurs distants dont les adresses IP appartiennent aux catégories suivantes : **Réseaux de confiance**, **Réseaux locaux**, **Réseaux publics**.

    - **Adresses de la liste**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par des ordinateurs distants dont les adresses IP peuvent être ajoutées à la liste ci-dessous via les boutons **Ajouter**, **Modifier** et **Supprimer**.

15. Indiquez les adresses réseau des ordinateurs dotés de Kaspersky Endpoint Security qui peuvent transmettre et/ou recevoir les paquets réseaux. Pour ce faire, choisissez une des valeurs suivantes dans la liste **Adresses locales** :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau à partir de n'importe quelle adresse IP par les ordinateurs sur lesquels Kaspersky Endpoint Security est installé.

    - **Adresses de la liste**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par des ordinateurs dotés de Kaspersky Endpoint Security et dont les adresses IP peuvent être ajoutées à la liste ci-dessous via les boutons **Ajouter**, **Modifier** et **Supprimer**.

    Il est parfois impossible d'obtenir une adresse locale pour les applications qui travaillent avec les paquets réseau. Dans ce cas, la valeur du paramètre **Adresses locales** est ignorée.

16. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le rapport.

17. Cliquez sur le bouton **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau, elle apparaît sous l'onglet **Règles pour les paquets réseau** de la fenêtre **Pare-feu**. Par défaut, la nouvelle règle réseau est placée en fin de liste.

18. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.

19. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle pour les paquets réseau

Pour activer ou désactiver la règle pour les paquets réseau, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Choisissez dans la liste la règle pour les paquets réseau requise.
5. Exécutez une des actions suivantes :
   - Cochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez désactiver la règle.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action du Pare-feu pour la règle pour les paquets réseau

Pour modifier l'action du Pare-feu pour la règle pour les paquets réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.
4. Choisissez dans la liste la règle pour les paquets réseau pour laquelle vous souhaitez modifier l'action.
5. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :
   - **Autoriser**
   - **Bloquer**
   - **Selon la règle de l'application**
   - **Consigner dans le rapport**
6. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la priorité de la règle pour les paquets réseau

La priorité d'exécution de la règle pour les paquets réseau est définie par l'emplacement de la règle dans la liste des règles pour les paquets réseau. La première règle pour les paquets réseau dans la liste des règles pour les paquets réseau possède la priorité la plus élevée.

Chaque règle pour les paquets réseau que vous avez créée est ajoutée à la fin de la liste des règles pour les paquets réseau et possède la priorité la plus faible.

Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles pour les paquets réseau haut/bas. Suivant chacune des règles pour les paquets réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Pour modifier la priorité de la règle pour les paquets réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.
4. Choisissez dans la liste la règle pour les paquets réseau pour laquelle vous souhaitez modifier la priorité.
5. A l'aide des boutons **Monter** et **Descendre**, déplacez la règle pour les paquets réseau vers la position requise dans la liste des règles pour les paquets réseau.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des règles réseau pour les applications

Kaspersky Endpoint Security regroupe par défaut toutes les applications installées selon le nom de l'éditeur de l'application dont il contrôle l'activité de réseau ou de fichiers. Les groupes d'applications sont à leur tour regroupés en groupes de confiance. Toutes les applications et tous les groupes d'applications héritent des propriétés de leur groupe parent : règles du contrôle des applications, règles réseau de l'application, ainsi que la priorité de leur exécution.

A l'instar du module Prévention des intrusions, le module Pare-feu applique par défaut les règles réseau du groupe d'applications afin de filtrer l'activité réseau de toutes les applications appartenant à ce groupe. Les règles réseau du groupe d'applications définissent les droits d'accès aux différentes connexions réseau attribués aux applications qui font partie du groupe.

Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Endpoint Security a identifié sur l'ordinateur. Vous avez deux options pour modifier l'action du Pare-feu pour les règles réseau du groupe d'applications créées par défaut. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau du groupe d'applications créées par défaut, ni modifier leur priorité.

Vous pouvez également créer une règle réseau pour une application distincte. La priorité de cette règle sera plus élevée que celle de la règle réseau du groupe auquel appartient cette application.

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles réseau de l'application :

- Créer une nouvelle règle réseau.

Vous pouvez créer une règle réseau selon laquelle le Pare-feu va régir l'activité réseau de l'application ou des applications qui font partie du groupe d'applications sélectionné.

- Activer et désactiver la règle réseau.

  Toutes les règles réseau sont ajoutées à la liste des règles réseau pour les applications avec l'état *Activé*. Si la règle réseau est activée, le Pare-feu applique cette règle.

  Vous pouvez désactiver la règle réseau que vous avez créée manuellement. Si la règle réseau est désactivée, le Pare-feu suspend temporairement l'application de la règle.

- Modifier les paramètres de la règle réseau.

  Après avoir créé une nouvelle règle réseau, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle réseau.

  Dans la liste des règles réseau, vous pouvez modifier l'action pour la règle réseau de l'application que le Pare-feu exécute lors de la détection de l'activité réseau de cette application ou de ce groupe d'applications.

- Modifier la priorité de la règle réseau.

  Vous pouvez augmenter ou diminuer la priorité de la règle réseau que vous avez créée manuellement.

- Supprimer la règle réseau.

  Vous pouvez supprimer la règle réseau que vous avez créée manuellement si vous ne souhaitez pas que le Pare-feu applique cette règle réseau à l'application ou au groupe d'applications sélectionnés lors de la détection de l'activité réseau et qu'elle soit affichée sur la liste des règles réseau de l'application.

Création et modification d'une règle réseau des applications

Pour créer ou modifier la règle réseau d'une application ou du groupe d'applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.
3. Cliquez sur le bouton **Règles pour applications**.

   La fenêtre **Pare-feu** s'ouvre sous l'onglet **Règles réseau des applications**.
4. Dans la liste des applications, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez créer ou modifier une règle réseau.
5. Ouvrez le menu contextuel d'un clic droit et en fonction de ce que vous devez faire, choisissez l'option **Autorisations des applications** ou **Autorisations des groupes d'applications**.

   Ce bouton qui ouvre la fenêtre **Autorisations des applications** ou **Privilèges du groupe d'applications**.
6. Choisissez l'onglet **Règles réseau** dans la fenêtre **Autorisations des applications** ou **Autorisations des groupes d'applications**.
7. Exécutez une des actions suivantes :

   - Si vous voulez créer une nouvelle règle réseau, cliquez sur le bouton **Ajouter**.

- Si vous voulez modifier une règle réseau, sélectionnez-la dans la liste des règles réseau et cliquez sur le bouton **Modifier**.

La fenêtre **Règle réseau** s'ouvre.

8. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**
   - **Bloquer**
9. Dans le champ **Nom**, indiquez le nom du service réseau d'une des manières suivantes :
   - Cliquez sur l'icône qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service réseau.

     La liste déroulante reprend les services de réseau décrivant les connexions réseau le plus souvent utilisées.
   - Dans le champ **Nom**, saisissez manuellement le nom du service réseau.
10. Indiquez le protocole de transfert des données :
    a. Cochez la case **Protocole**.
    b. Sélectionnez dans la liste déroulante le type de protocole à utiliser pour le contrôle de l'activité réseau.

       Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE. Si le service réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et il convient alors de sélectionner dans la liste déroulante à côté de la case le type de protocole qui correspond au service réseau sélectionné. La case **Protocole** est décochée par défaut.
11. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

    Le Pare-feu contrôle les connexions réseau avec des directions suivantes :
    - **Entrant**.
    - **Entrant / Sortant**.
    - **Sortant**.
12. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :
    a. Cochez la case **Type ICMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.
    b. Cochez la case **Code ICMP** et sélectionnez dans la liste déroulante le code ICMP.
13. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les numéros des ports (séparés par une virgule) de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée :
    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.
    b. Saisissez dans le champ **Ports locaux** les ports de l'ordinateur de l'utilisateur.
14. Indiquez les adresses réseau des ordinateurs distants qui peuvent transmettre et/ou recevoir des paquets réseau. Pour ce faire, choisissez une des valeurs suivantes dans la liste **Adresses distantes** :

- **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par les ordinateurs distants depuis n'importe quelle adresse IP.

- **Adresses du sous-réseau**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par les ordinateurs distants dont les adresses IP appartiennent aux catégories suivantes : **Réseaux de confiance**, **Réseaux locaux**, **Réseaux publics**.

- **Adresses de la liste**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par des ordinateurs distants dont les adresses IP peuvent être ajoutées à la liste ci-dessous via les boutons **Ajouter**, **Modifier** et **Supprimer**.

15. Indiquez les adresses réseau des ordinateurs dotés de Kaspersky Endpoint Security qui peuvent transmettre et/ou recevoir les paquets réseaux. Pour ce faire, choisissez une des valeurs suivantes dans la liste **Adresses locales** :

    - **Adresse quelconque**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau à partir de n'importe quelle adresse IP par les ordinateurs sur lesquels Kaspersky Endpoint Security est installé.

    - **Adresses de la liste**. La règle réseau contrôle l'envoi et/ou la réception de paquets réseau par des ordinateurs dotés de Kaspersky Endpoint Security et dont les adresses IP peuvent être ajoutées à la liste ci-dessous via les boutons **Ajouter**, **Modifier** et **Supprimer**.

    Il est parfois impossible d'obtenir une adresse locale pour les applications qui travaillent avec les paquets réseau. Dans ce cas, la valeur du paramètre **Adresses locales** est ignorée.

16. Cochez la case **Consigner dans le rapport** si vous souhaitez que l'action de la règle réseau soit consignée dans le rapport.

17. Cliquez sur le bouton **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau, elle apparaît sous l'onglet **Règles réseau**.

18. Cliquez sur le bouton **OK** dans la fenêtre **Privilèges du groupe d'applications** si la règle est destinée à un groupe d'applications ou dans la fenêtre **Autorisations des applications**, si la règle est destinée à une application.

19. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.

20. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la règle réseau des applications

Pour activer ou désactiver la règle réseau des applications, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour applications**.

   La fenêtre **Pare-feu** s'ouvre sous l'onglet **Règles réseau des applications**.

4. Dans la liste, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez créer ou modifier une règle réseau.

5. Ouvrez le menu contextuel d'un clic droit et en fonction de ce que vous devez faire, choisissez l'option **Autorisations des applications** ou **Autorisations des groupes d'applications**.

   Ce bouton qui ouvre la fenêtre **Autorisations des applications** ou **Privilèges du groupe d'applications**.

6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Règles réseau**.

7. Sélectionnez dans la liste des règles réseau du groupe d'applications la règle réseau requise.

8. Exécutez une des actions suivantes :

   - Cochez la case à côté du nom de la règle réseau si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle réseau si vous souhaitez désactiver la règle.

   > Vous ne pouvez pas désactiver la règle réseau du groupe d'applications si elle a été créée par le Pare-feu par défaut.

9. Cliquez sur le bouton **OK** dans la fenêtre **Privilèges du groupe d'applications** si la règle est destinée à un groupe d'applications ou dans la fenêtre **Autorisations des applications**, si la règle est destinée à une application.

10. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action du Pare-feu pour la règle réseau des applications

Vous pouvez modifier l'action du Pare-feu pour toutes les règles réseau d'application ou de groupe d'applications qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle réseau d'une application ou d'un groupe d'applications qui a été créée manuellement.

Pour modifier l'action du Pare-feu pour toutes les règles réseau d'application ou de groupe des applications, procédez comme suit :

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

2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour applications**.

   La fenêtre **Pare-feu** s'ouvre sous l'onglet **Règles réseau des applications**.

4. Sélectionnez dans la liste l'application ou le groupe d'applications si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau créées par défaut. Les règles réseau définies manuellement resteront inchangées.

5. Dans la colonne **Réseau**, cliquez avec le bouton gauche de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

- **Hériter**
- **Autoriser**
- **Bloquer**

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Pour modifier l'action du Pare-feu pour une règle réseau d'une application ou d'un groupe d'applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour applications**.

   La fenêtre **Pare-feu** s'ouvre sous l'onglet **Règles réseau des applications**.
4. Dans la liste, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez modifier l'action d'une règle réseau.
5. Ouvrez le menu contextuel d'un clic droit et en fonction de ce que vous devez faire, choisissez l'option **Autorisations des applications** ou **Autorisations des groupes d'applications**.

   Ce bouton qui ouvre la fenêtre **Autorisations des applications** ou **Privilèges du groupe d'applications**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Règles réseau**.
7. Choisissez la règle réseau pour laquelle vous voulez modifier l'action du Pare-feu.
8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :
   - **Autoriser**
   - **Bloquer**
   - **Consigner dans le rapport**
9. Cliquez sur le bouton **OK** dans la fenêtre **Privilèges du groupe d'applications** si la règle est destinée à un groupe d'applications ou dans la fenêtre **Autorisations des applications**, si la règle est destinée à une application.
10. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la priorité de la règle réseau des applications

La priorité d'exécution de la règle réseau est définie par l'emplacement de la règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Suivant chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau créées manuellement ont une priorité plus élevée que les règles réseau créées par défaut.

Vous ne pouvez pas modifier la priorité des règles réseau d'un groupe d'applications créées par défaut.

Pour modifier la priorité d'une règle réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour applications**.

   La fenêtre **Pare-feu** s'ouvre sous l'onglet **Règles réseau des applications**.
4. Dans la liste des applications, sélectionnez l'application ou le groupe d'applications pour lequel vous souhaitez modifier la priorité de la règle réseau.
5. Ouvrez le menu contextuel d'un clic droit et en fonction de ce que vous devez faire, choisissez l'option **Autorisations des applications** ou **Autorisations des groupes d'applications**.

   Ce bouton qui ouvre la fenêtre **Autorisations des applications** ou **Privilèges du groupe d'applications**.
6. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Règles réseau**.
7. Sélectionnez la règle réseau dont vous souhaitez modifier la priorité.
8. A l'aide des boutons **Monter** et **Descendre**, déplacez la règle réseau vers la position requise dans la liste des règles réseau.
9. Cliquez sur le bouton **OK** dans la fenêtre **Privilèges du groupe d'applications** si la règle est destinée à un groupe d'applications ou dans la fenêtre **Autorisations des applications**, si la règle est destinée à une application.
10. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Surveillance du réseau

Cette section contient des informations sur la surveillance du réseau et explique comment lancer la surveillance de réseau.

A propos de la surveillance du réseau

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de l'ordinateur d'utilisateur en temps réel.

Lancement de la surveillance du réseau

Pour lancer la Surveillance du réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Cliquez sur la section **Modules de protection**.

   La fenêtre **Modules de protection** s'ouvre.
3. Cliquez sur le lien **Surveillance du réseau** dans le bas de la fenêtre.

   La fenêtre **Surveillance du réseau** s'ouvre. Cette fenêtre affiche les informations sur l'activité réseau de l'ordinateur de l'utilisateur sur quatre onglets :

   - L'onglet **Activité réseau** affiche toutes les connexions réseau à l'ordinateur de l'utilisateur qui sont actuellement actives. Il affiche non seulement les connexions réseau ouvertes par l'ordinateur de l'utilisateur, mais aussi les connexions réseau entrantes.
   - L'onglet **Ports ouverts** reprend tous les ports réseau ouverts sur l'ordinateur de l'utilisateur.
   - L'onglet **Trafic réseau** affiche le volume du trafic réseau entrant et sortant entre l'ordinateur de l'utilisateur et les autres ordinateurs du réseau auquel l'utilisateur est connecté actuellement.
   - L'onglet **Ordinateurs bloqués** affiche la liste des adresses IP des ordinateurs distants dont l'activité réseau a été bloquée par le module Protection contre les menaces réseau après une tentative d'attaque réseau effectuée depuis cette adresse IP.

Protection BadUSB

Cette section contient des informations sur le module Protection BadUSB.

Présentation de la Protection BadUSB

Certains virus modifient l'application interne des périphériques USB afin que le système d'exploitation considère le périphérique USB comme un clavier.

Le module Protection BadUSB permet d'empêcher la connexion de périphériques USB infectés qui imitent un clavier.

Quand un périphérique USB est connecté à l'ordinateur et que le système d'exploitation le considère comme un clavier, l'application génère un code numérique qu'elle propose à l'utilisateur de saisir via ce clavier ou via un clavier numérique (si disponible). C'est ce qu'on appelle l'autorisation du clavier. L'application autorise l'utilisation du clavier autorisé et bloque tout clavier qui n'a pas réussi l'autorisation.

Installation du module Protection BadUSB

Si pendant l'installation de Kaspersky Endpoint Security vous avez choisi le type d'installation de base ou standard, le module Protection BadUSB ne sera pas accessible. Pour l'installer, il faut modifier la composition des modules de l'application.

Pour installer le module Protection BadUSB, procédez comme suit :

1. Ouvrez la fenêtre **Panneau de configuration** d'une des méthodes suivantes :
   - Si vous utilisez Windows 7, sélectionnez **Panneau de configuration** dans le menu **Démarrer**.
   - Si vous utilisez Windows 8/Windows 8.1, appuyez sur la combinaison de touches **Win+I** et choisissez l'option **Panneau de configuration**.
   - Si vous utilisez Windows 10, appuyez sur la combinaison de touches **Win+X** et choisissez l'option **Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, choisissez l'option **Applications et modules**.
3. Dans la liste des applications installées, sélectionnez **Kaspersky Endpoint Security for Windows**.
4. Cliquez sur le bouton **Modifier/Désinstaller**.
5. Dans la fenêtre **Modification, restauration ou suppression de l'application** de l'Assistant d'installation de l'application, cliquez sur le bouton **Modification**.

   Cette action ouvre la fenêtre **Installation personnalisée** de l'Assistant d'installation de l'application.
6. Dans le groupe du module **Protection principale** dans le menu contextuel de l'icône située à côté du nom du module **Protection BadUSB**, sélectionnez l'option **Le module sera installé sur un disque dur local**.
7. Cliquez sur le bouton **Suivant**.
8. Suivez les instructions de l'Assistant d'installation.

Activation et désactivation de la Protection BadUSB

Pour activer ou désactiver le module Protection BadUSB, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection BadUSB**.

   La partie droite de la fenêtre affiche les paramètres du module Protection BadUSB.
3. Exécutez une des actions suivantes :
   - Cochez la case **Protection BadUSB** si vous souhaitez activer la Protection BadUSB.
   - Décochez la case **Protection BadUSB** pour désactiver la Protection BadUSB.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Autorisation et interdiction de l'utilisation du clavier virtuel pour l'autorisation

La possibilité d'utiliser le clavier virtuel existe uniquement pour l'autorisation des périphériques USB qui ne prennent pas en charge la saisie de caractères (par exemple, un lecteur de code-barres). Il est déconseillé d'utiliser le clavier virtuel pour autoriser des périphériques USB que vous ne connaissez pas.

Pour autoriser ou interdire l'utilisation du clavier virtuel pour l'autorisation, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Protection BadUSB**.

   Les paramètres du module s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des périphériques USB** si vous souhaitez interdire l'utilisation du clavier virtuel pour l'autorisation.
   - Décochez la case **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des périphériques USB** si vous souhaitez autoriser l'utilisation du clavier virtuel pour l'autorisation.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Autorisation de clavier

Les périphériques USB définis par le système d'exploitation comme des claviers et connectés à l'ordinateur avant l'installation du module Protection BadUSB sont considérés comme autorisés après son installation.

L'application requiert l'autorisation d'un périphérique USB défini comme un clavier par le système d'exploitation si la demande d'autorisation du clavier USB est activée. L'utilisateur ne peut pas utiliser un clavier que si ce dernier a été autorisé.

Si la demande d'autorisation des claviers USB est désactivée, l'utilisateur peut utiliser tous les claviers connectés. Dès l'activation de la demande d'autorisation des claviers USB, l'application demande l'autorisation pour chaque clavier non autorisé connecté à l'ordinateur.

Pour autoriser un clavier, procédez comme suit :

1. Après avoir activé l'autorisation des claviers USB, branchez un clavier au port USB.

   La fenêtre **Autorisation de clavier <nom du clavier>** contenant les informations sur le clavier connecté et le code numérique d'autorisation s'ouvre.
2. Utilisez le clavier connecté ou le clavier virtuel, s'il est disponible, pour saisir le code numérique aléatoire dans la fenêtre d'autorisation.
3. Cliquez sur le bouton **OK**.

Si le code est saisi correctement, l'application enregistre les paramètres d'identification VID/PID du clavier et le numéro de port utilisé pour la connexion dans la liste des claviers autorisés. Il ne sera pas nécessaire d'autoriser à nouveau le clavier lors de la prochaine connexion ou suite au redémarrage du système d'exploitation.

Par contre, si vous connectez un clavier autorisé à un autre port USB, l'application sollicitera à nouveau l'autorisation.

Si le code numérique n'est pas saisi correctement, l'application crée un autre code. Le nombre maximum de tentatives de saisie est limité à trois. Après trois tentatives infructueuses ou si la fenêtre **Autorisation de clavier <nom du clavier>** est fermée, l'application bloque la saisie à l'aide de ce clavier. Si le clavier est reconnecté ou si le système d'exploitation redémarre, l'application proposera à nouveau d'autoriser le clavier.

Fournisseur de protection AMSI

Cette section contient des informations sur le Fournisseur de protection AMSI et les instructions sur la configuration du module.

A propos du fournisseur de protection AMSI

Le fournisseur de protection AMSI est prévu pour la prise en charge de l'interface Antimalware Scan Interface de Microsoft. L'*interface Antimalware Scan Interface (AMSI)* permet à une application tierce compatible avec AMSI d'envoyer des objets à Kaspersky Endpoint Security en vue d'une analyse complémentaire (par exemple, des scripts PowerShell) et d'obtenir les résultats de l'analyse de ces objets. Pour en savoir plus sur l'interface AMSI, consultez la *documentation de Microsoft*.

Le fournisseur d'événements de protection AMSI peut uniquement détecter une menace et la signaler à l'application tierce. Il ne peut pas la traiter. Après la réception de la notification sur la menace, l'application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt le fonctionnement). Si l'objet est ajouté à l'exclusion de l'analyse, le Fournisseur de protection AMSI n'exécute pas l'analyse à la réception de la demande de l'application tierce.

Le composant Fournisseur de protection AMSI peut rejeter la demande d'une application tierce, par exemple, si cette application a excédé le nombre maximum de demande pour l'intervalle défini. Kaspersky Endpoint Security envoie les informations relatives au rejet de la demande de l'application tierce au Serveur d'administration. Le composant Fournisseur de protection AMSI ne rejette pas les demandes des applications tierces pour lesquelles la case **Ne pas bloquer l'interaction avec le fournisseur de protection AMSI** a été cochée.

Le module Fournisseur de protection AMSI est disponible pour les systèmes d'exploitation suivants pour postes de travail et serveurs de fichiers :

- Windows 10 Home / Pro / Education / Enterprise (32 / 64 bits) ;
- Windows Server 2016 (64 bits) ;
- Windows Server 2019 (64 bits) ;

Activation et désactivation du Fournisseur de protection AMSI

Le Fournisseur de protection AMSI est activé par défaut. Vous pouvez désactiver le Fournisseur de protection AMSI le cas échéant.

Pour activer ou désactiver le Fournisseur de protection AMSI, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Protection principale** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Fournisseur de protection AMSI**.

   La partie droite de la fenêtre affiche les paramètres du module Fournisseur de protection AMSI.
3. Exécutez une des actions suivantes :

   - Cochez la case **Fournisseur de protection AMSI** si vous voulez activer le Fournisseur de protection AMSI.
   - Décochez la case **Fournisseur de protection AMSI** si vous voulez désactiver le Fournisseur de protection AMSI.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés par le Fournisseur de protection AMSI

L'insertion de virus dans des fichiers composés tels que des archives est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulés de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter la sélection de types de fichiers composés à analyser pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés par le Fournisseur de protection AMSI, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section Fournisseur de protection AMSI.

   La partie droite de la fenêtre affiche les paramètres du module Fournisseur de protection AMSI.
3. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets de distribution ou fichiers au format Office.
4. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Pour empêcher que le module Fournisseur de protection AMSI ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**. Le module Fournisseur de protection AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.
   - Pour autoriser le module Fournisseur de protection AMSI à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

Le module Fournisseur de protection AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle des applications

Cette section contient des informations sur le Contrôle des applications et les instructions sur la configuration des paramètres du module.

Présentation du Contrôle des applications

Le composant Contrôle des applications surveille les tentatives de démarrage des applications par les utilisateurs et régit le démarrage des applications à l'aide des *règles de Contrôle des applications*.

Le lancement des applications dont aucun paramètre ne respecte les règles de Contrôle des applications est régi par le mode sélectionné de fonctionnement du module. Le mode *Liste noire* est sélectionné par défaut. Ce mode permet à n'importe quel utilisateur de lancer n'importe quelle application. Quand l'utilisateur tente de lancer une application interdite par les règles de Contrôle des applications, Kaspersky Endpoint Security bloque le lancement de cette application (si l'action **Appliquer les règles** a été choisie) ou enregistre les informations relatives au lancement de l'application dans le rapport (si l'action **Tester les règles** a été choisie).

Toutes les tentatives de l'utilisateur visant à lancer des applications sont consignées dans des rapports.

Activation et désactivation du Contrôle des applications

Le Contrôle des applications est désactivé par défaut. Le cas échéant, vous pouvez activer le Contrôle des applications.

Pour activer ou désactiver le Contrôle des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Contrôle des applications** pour activer le Contrôle des applications.
   - Décochez la case **Contrôle des applications** pour désactiver le Contrôle des applications.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Restrictions sur le fonctionnement du Contrôle des applications

Le fonctionnement du module Contrôle des applications est restreint dans les cas suivants :

- Lors de la mise à jour de la version de l'application, l'importation des paramètres du module Contrôle des applications n'est pas prise en charge.
- Lors de la mise à jour de la version de l'application, l'importation des paramètres du composant Contrôle des applications est pris en charge uniquement lors de la mise à jour depuis la version Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes vers Kaspersky Endpoint Security 11.1.1 for Windows.

  Lors de a mise à jour des versions de l'application différentes de Kaspersky Endpoint Security 10 Service Pack 2 for Windows, il faut à nouveau configurer les paramètres du composant afin de rétablir son fonctionnement.

- En l'absence de connexion avec les serveurs de KSN, Kaspersky Endpoint Security reçoit les informations sur la réputation des applications et de leurs modules uniquement depuis des bases locales.

  La liste des applications pour lesquelles Kaspersky Endpoint Security définit la catégorie KL **Applications de confiance selon la réputation dans KSN**, en présence d'une connexion avec les serveurs KSN, peut différer de la liste des applications pour lesquelles Kaspersky Endpoint Security définit la catégorie KL **Applications de confiance conformément à la réputation dans KSN** en l'absence d'une connexion à KSN.

- La base de données de Kaspersky Security Center peut contenir les informations sur 150 000 fichiers traités. Une fois que ce nombre d'enregistrements a été atteint, les nouveaux fichiers ne seront pas traités. Pour rétablir le fonctionnement de l'inventaire, il faut supprimer les fichiers repris dans la base de données de Kaspersky Security Center antérieurement suite à l'inventaire sur l'ordinateur doté de l'application Kaspersky Endpoint Security.
- Le module ne contrôle pas le lancement des scripts si le script est transmis à l'interprète par une méthode autre que la ligne de commande.

  Si le lancement de l'interpréteur est autorisé par les règles du Contrôle des applications, le module ne bloque pas le script lancé via cet interpréteur.

  Si le lancement d'au moins un des scripts indiqués dans la ligne de commande de l'interpréteur est bloqué par les règles de Contrôle des applications, le composant bloque tous les scripts indiqués dans la ligne de commande de l'interpréteur.

- Le module ne contrôle pas le lancement des scripts depuis des interprètes qui ne sont pas pris en charge par l'application Kaspersky Endpoint Security.

  Kaspersky Endpoint Security est compatible avec les interprètes suivants :

  - Java ;
  - PowerShell.

  Les types d'interprète suivants sont pris en charge :

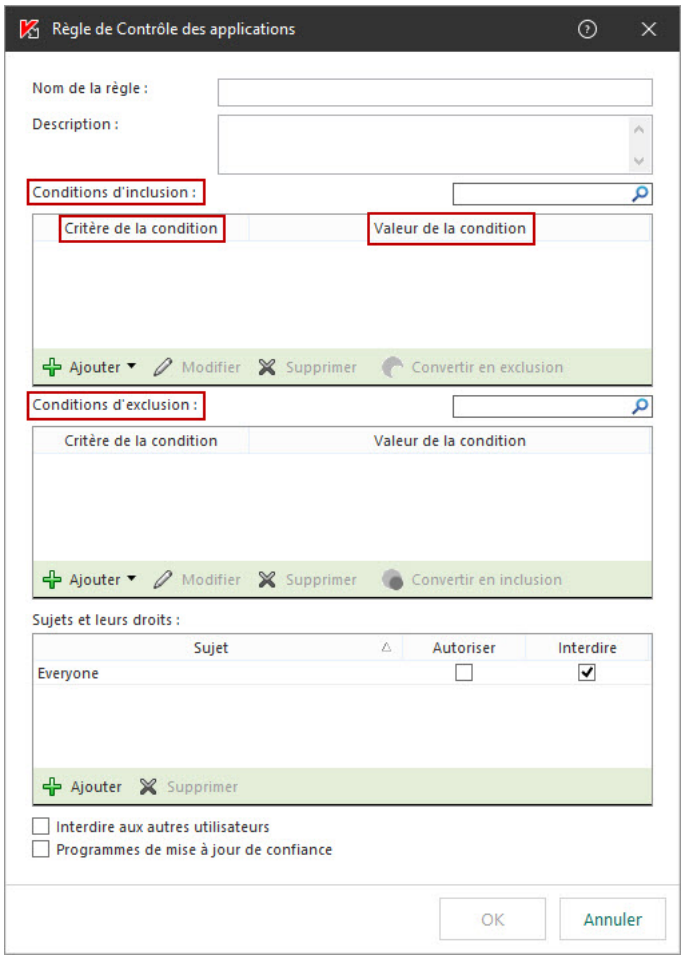
- %ComSpec%
- %SystemRoot%\\system32\\regedit.exe
- %SystemRoot%\\regedit.exe
- %SystemRoot%\\system32\\regedt32.exe
- %SystemRoot%\\system32\\cscript.exe
- %SystemRoot%\\system32\\wscript.exe
- %SystemRoot%\\system32\\msiexec.exe
- %SystemRoot%\\system32\\mshta.exe
- %SystemRoot%\\system32\\rundll32.exe
- %SystemRoot%\\system32\\wwahost.exe
- %SystemRoot%\\syswow64\\cmd.exe
- %SystemRoot%\\syswow64\\regedit.exe
- %SystemRoot%\\syswow64\\regedt32.exe
- %SystemRoot%\\syswow64\\cscript.exe
- %SystemRoot%\\syswow64\\wscript.exe
- %SystemRoot%\\syswow64\\msiexec.exe
- %SystemRoot%\\syswow64\\mshta.exe
- %SystemRoot%\\syswow64\\rundll32.exe
- %SystemRoot%\\syswow64\\wwahost.exe

A propos des règles de Contrôle des applications

Kaspersky Endpoint Security utilise des règles pour contrôler le lancement des applications par l'utilisateur. La règle du Contrôle des applications contient les conditions de déclenchement et l'action exécutée par le module Contrôle des applications en cas de déclenchement de la règle (autoriser ou non les utilisateurs à démarrer l'application).

Condition de déclenchement de la règle

La condition de déclenchement de la règle est une équivalence "type de condition – critères de la condition – valeur de la condition" (cf. ill. ci-après). Sur la base des conditions de déclenchement de la règle Kaspersky Endpoint Security applique ou non la règle à l'application.



Règle de Contrôle des applications. Paramètres des conditions de déclenchement de la règle

Les règles reposent sur des règles d'inclusion et d'exclusion :

- *Conditions d'inclusion*. Kaspersky Endpoint Security applique la règle à l'application si l'application remplit au moins une des conditions d'inclusion.
- *Conditions d'exclusion*. Kaspersky Endpoint Security n'applique pas la règle à l'application si l'application remplit au moins une des conditions d'exclusion ou ne remplit aucune des conditions d'inclusion.

Les conditions de déclenchement de la règle sont définies à l'aide de critères. Les critères suivants interviennent dans la composition des conditions dans Kaspersky Endpoint Security :

- chemin d'accès au dossier contenant le fichier exécutable de l'application ou le chemin d'accès au fichier exécutable de l'application ;
- métadonnées : nom du fichier exécutable de l'application, version du fichier exécutable de l'application, nom de l'application, version de l'application, éditeur de l'application ;
- hash du fichier exécutable de l'application ;
- certificat : éditeur, le sujet, empreinte ;
- appartenance de l'application à une catégorie KL ;
- emplacement du fichier exécutable de l'application sur le disque amovible.

Il faut définir la valeur de chaque critère utilisé dans une condition. Si les paramètres de l'application lancée correspondent aux valeurs des critères repris dans les conditions d'inclusion, la règle se déclenche. Dans ce cas, le Contrôle des applications exécute l'action définie dans la règle. Si les paramètres de l'application correspondent aux valeurs des critères repris dans les conditions d'exclusion, le Contrôle des applications ne contrôle pas le lancement de l'application.

Décisions du Contrôle des applications en cas de déclenchement de la règle

En cas de déclenchement de la règle, le Contrôle des applications, conformément à la règle établie, permet ou non à l'utilisateur (ou à un groupe d'utilisateurs) de lancer l'application. Vous pouvez sélectionner des utilisateurs individuels ou des groupes d'utilisateurs autorisés ou non à lancer les applications qui déclenchent la règle.

Si la règle ne désigne aucun utilisateur autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'interdiction*.

Si la règle ne désigne aucun utilisateur non autorisé à lancer les applications qui satisfont à la règle, cette règle est une règle *d'autorisation*.

Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Par exemple, si une règle d'autorisation de Contrôle des applications a été définie pour un groupe d'utilisateurs et qu'un des membres de ce groupe est soumis à une règle d'interdiction de Contrôle des applications, ce membre n'est pas autorisé à exécuter l'application.

État de fonctionnement de la règle

Les règles de Contrôle des applications peuvent avoir un des états de fonctionnement suivant :

- **Activé**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
- **Désactivée**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.
- **Test**. L'état signifie que Kaspersky Endpoint Security autorise le lancement des applications soumises à la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

Administration des règles du Contrôle des applications

Vous pouvez réaliser les opérations suivantes au niveau des règles de Contrôle des applications :

- Ajouter une nouvelle règle.
- Créer ou modifier les conditions du fonctionnement de la règle.
- Modifier l'état de fonctionnement de la règle.

  La règle de Contrôle des applications peut être activée, désactivée ou sélectionnée pour un test. Par défaut, après sa création, la règle de Contrôle des applications est activée.
- Supprimer la règle.

Ajout et modification d'une règle de Contrôle des applications

Pour ajouter ou modifier une règle de Contrôle des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.
4. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Pour modifier une règle existante, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle de Contrôle des applications** s'ouvre.
5. Définissez ou modifiez les paramètres de la règle :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom de la règle**.

   b. Dans le tableau **Conditions d'inclusion** dressez ou modifiez la liste des conditions d'inclusion du déclenchement de la règle à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**, **Convertir en exclusion**.

   c. Dans le tableau **Conditions d'exclusion** dressez ou modifiez la liste des conditions d'exception du déclenchement de la règle à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**, **Convertir en inclusion**.

   d. Le cas échéant, modifiez le type de condition de déclenchement de la règle :

      - Pour faire passer une condition du type inclusion en type exception, sélectionnez la condition dans le tableau **Conditions d'inclusion**, puis cliquez sur **Convertir en exclusion**.
      - Pour faire passer une condition du type exception au type inclusion, sélectionnez la condition dans le tableau **Conditions d'exclusion**, puis cliquez sur le bouton **Convertir en inclusion**.

   e. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés ou non à lancer les applications qui répondent aux conditions de déclenchement de la règle. Pour ce faire, cliquez sur le bouton **Ajouter** dans le tableau **Sujets et leurs droits**.

      La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

      La valeur **Tous** est ajoutée par défaut à la liste des utilisateurs. La règle s'applique à tous les utilisateurs.

      > Si aucun utilisateur n'est repris dans le tableau, la règle ne peut pas être enregistrée.

   f. Dans le tableau **Sujets et leurs droits**, cochez les cases **Autoriser** ou **Interdire** en regard des utilisateurs et/ou des groupes d'utilisateurs pour définir leur droit au lancement des programmes.

      La case cochée par défaut dépend du mode du Contrôle des applications.

g. Cochez la case **Interdire aux autres utilisateurs** si vous voulez que l'application interdise le lancement des applications qui répondent aux conditions du fonctionnement de la règle à tous les utilisateurs qui ne figurent pas dans la colonne **Sujet** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans la colonne **Sujet**.

Si la case **Interdire aux autres utilisateurs** est décochée, Kaspersky Endpoint Security ne contrôle pas le lancement des applications par les utilisateurs qui ne figurent pas dans le tableau **Sujets et leurs droits** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans le tableau **Sujets et leurs droits**.

h. Cochez la case **Programmes de mise à jour de confiance** si vous souhaitez que les applications qui répondent aux conditions de déclenchement de la règle soient considérées comme des applications de mise à jour de confiance par Kaspersky Endpoint Security et qu'il les autorise à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.

Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutables créés par les programmes de mise à jour de confiance migre également.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Ajout d'une condition de déclenchement de la règle de Contrôle des applications

Pour ajouter une nouvelle condition de déclenchement à la règle de Contrôle des applications, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.

4. Exécutez une des actions suivantes :

   - Si vous souhaitez créer une règle et y ajouter une condition de déclenchement, cliquez sur le bouton **Ajouter**.

   - Si vous souhaitez ajouter une condition de déclenchement à une règle existante, sélectionnez la règle dans la liste des règles, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Règle de Contrôle des applications** s'ouvre.

5. Dans le tableau **Conditions d'inclusion** ou **Conditions d'exclusion**, cliquez sur le bouton **Ajouter**.

Les options de la liste déroulante sous le bouton **Ajouter** permettent d'ajouter à la règle différentes conditions de déclenchements (cf. instructions ci-dessous).

Pour ajouter une condition de déclenchement de la règle sur la base des propriétés des fichiers du dossier indiqué, procédez comme suit :

1. Dans la liste déroulante sous le bouton **Ajouter**, choisissez l'option **Conditions à partir des propriétés du fichier du dossier indiqué**.

   La fenêtre standard de Microsoft Windows **Sélection du dossier** s'ouvre.

2. Dans la fenêtre **Sélection du dossier**, sélectionnez le dossier contenant les fichiers exécutables des applications dont vous souhaitez utiliser les propriétés pour composer une ou plusieurs conditions de déclenchement de la règle.

3. Cliquez sur le bouton **OK**.

   La fenêtre **Ajout des conditions** s'ouvre.

4. Dans la liste déroulante **Afficher les critères**, sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Hash du fichier**, **Certificat**, **Catégorie KL**, **Métadonnées** ou **Chemin d'accès au dossier**.

   Kaspersky Endpoint Security ne prend pas en charge le hash MD5 du fichier et ne contrôle pas le lancement des applications sur la base du hash MD5. Le hash SHA256 fait office de condition de déclenchement de la règle.

5. Si vous choisissez l'option **Métadonnées** dans la liste **Afficher les critères**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom du fichier**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Éditeur**.

   Si aucune des propriétés indiquées n'est sélectionnée, la règle ne peut pas être enregistrée.

6. Si dans la liste déroulante **Afficher les critères** vous avez choisi l'option **Certificat**, cochez les cases en regard des paramètres que vous souhaitez utiliser dans les conditions de déclenchement de la règle : **Éditeur**, **Sujet**, **Empreinte**.

   Si aucun des paramètres indiqués n'est sélectionné, la règle ne peut pas être enregistrée.

   Il est déconseillé d'utiliser uniquement **Éditeur** et **Sujet** en tant que condition de déclenchement des règles. L'utilisation de ces critères n'est pas fiable.

7. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

8. Cliquez sur le bouton **Suivant**.

   La liste des conditions de déclenchement de la règle définies s'affiche.

9. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de Contrôle des applications.

10. Cliquez sur le bouton **Terminer**.

Pour ajouter une condition de déclenchement de règle sur la base des propriétés des applications exécutées sur l'ordinateur, procédez comme suit :

1. Dans la liste déroulante sous le bouton **Ajouter**, sélectionnez l'option **Conditions à partir des propriétés des applications lancées**.

2. Dans la liste déroulante **Afficher les critères** de la fenêtre **Ajout des conditions**, choisissez le critère sur la base duquel vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Hash du fichier**, **Certificat**, **Catégorie KL**, **Métadonnées** ou **Chemin d'accès au dossier**.

   Kaspersky Endpoint Security ne prend pas en charge le hash MD5 du fichier et ne contrôle pas le lancement des applications sur la base du hash MD5. Le hash SHA256 fait office de condition de déclenchement de la règle.

3. Si vous choisissez l'option **Métadonnées** dans la liste **Afficher les critères**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom du fichier**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Éditeur**.

   Si aucune des propriétés indiquées n'est sélectionnée, la règle ne peut pas être enregistrée.

4. Si dans la liste déroulante **Afficher les critères** vous avez choisi l'option **Certificat**, cochez les cases en regard des paramètres que vous souhaitez utiliser dans les conditions de déclenchement de la règle : **Éditeur**, **Sujet**, **Empreinte**.

   Si aucun des paramètres indiqués n'est sélectionné, la règle ne peut pas être enregistrée.

   Il est déconseillé d'utiliser uniquement **Éditeur** et **Sujet** en tant que condition de déclenchement des règles. L'utilisation de ces critères n'est pas fiable.

5. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

6. Cliquez sur le bouton **Suivant**.

   La liste des conditions de déclenchement de la règle définies s'affiche.

7. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de Contrôle des applications.

8. Cliquez sur le bouton **Terminer**.

Pour ajouter une condition de déclenchement de la règle sur la base des catégories KL, procédez comme suit :

1. Dans la liste déroulante sous le bouton **Ajouter**, choisissez l'option **Conditions "Catégorie KL"**.

   Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe® Acrobat® et d'autres.

2. Dans la fenêtre **Conditions "Catégorie KL"**, cochez les cases en regard des noms de catégories KL qui vont servir de base à la création de la condition de déclenchement de la règle.

   Vous pouvez cliquer sur le bouton à gauche du nom des catégories KL afin de sélectionner les sous-catégories.

3. Cliquez sur le bouton **OK**.

Pour ajouter une condition de déclenchement de la règle créée manuellement, procédez comme suit :

1. Dans la liste déroulante sous le bouton **Ajouter**, choisissez l'option **Condition manuelle**.

2. Cliquez sur le bouton **Sélectionner** dans la fenêtre **Condition personnalisée** et indiquez le chemin d'accès au fichier exécutable de l'application.

3. Choisissez le critère sur la base duquel vous souhaitez créer une condition de déclenchement de la règle : **Hash du fichier**, **Certificat**, **Métadonnées** ou **Chemin d'accès au fichier ou au dossier**.

   Kaspersky Endpoint Security ne prend pas en charge le code de hachage de fichier MD5 et ne contrôle pas le démarrage des applications basées sur un hachage MD5. Le hash SHA256 fait office de condition de déclenchement de la règle.

   Si vous utilisez un lien symbolique dans le champ **Chemin d'accès au fichier ou au dossier** , il est conseillé de développer le lien symbolique pour garantir le bon fonctionnement de la règle de Contrôle du lancement des applications. Pour ce faire, cliquez sur le bouton **Résoudre le lien symbolique**.

4. Configurez les paramètres du critère choisi.

5. Cliquez sur le bouton **OK**.

Pour ajouter une condition de déclenchement sur la base des informations relatives au support du fichier exécutable de l'application, procédez comme suit :

1. Dans la liste déroulante sous le bouton **Ajouter**, choisissez l'option **Condition d'après le lecteur de fichiers**.

2. Dans la fenêtre **Condition d'après le lecteur de fichiers**, sélectionnez le type de périphérique de stockage sur lequel le lancement d'applications constituera une condition de déclenchement de la règle dans la liste déroulante **Support**.

3. Cliquez sur le bouton **OK**.

Modification de l'état de la règle de Contrôle des applications

Pour modifier l'état de la règle de Contrôle des applications, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.

4. Dans la colonne **État**, cliquez-gauche pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :

   - **Activé**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
   - **Désactivée**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.
   - **Test**. L'état signifie que Kaspersky Endpoint Security autorise toujours le lancement des applications soumises à cette règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

L'état **Test** permet de désigner l'action semblable à l'option **Tester les règles** pour une partie des règles quand l'option **Appliquer les règles** a été choisie dans la liste déroulante **Action**.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Test des règles du Contrôle des applications

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles.

Pour analyser le fonctionnement des règles de Contrôle des applications, il faut étudier les événements sur la base des résultats du fonctionnement du module Contrôle des applications survenus dans Kaspersky Security Center. Si aucune des applications indispensables au travail de l'utilisateur de l'ordinateur n'affiche des événements d'interdiction de lancement en mode test, les règles créées sont correctes. Dans le cas contraire, il est conseillé de préciser les paramètres des règles que vous avez créées, de créer des règles complémentaires ou de supprimer des règles existantes.

L'action **Appliquer les règles** est sélectionnée par défaut pour les règles du Contrôle des applications.

Pour activer le test des règles de Contrôle des applications ou pour sélectionner une règle d'interdiction du Contrôle des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.
4. Dans la liste déroulante **Mode de contrôle** choisissez une des options suivantes :

   - **Liste noire**, si vous voulez autoriser le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'interdiction ;
   - **Liste blanche**, si vous voulez interdire le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'autorisation.
5. Exécutez une des actions suivantes :

   - Si vous voulez activer le mode de test pour les règles de Contrôle des applications, choisissez l'option **Tester les règles** dans la liste **Action**.
   - Si vous voulez activer le mode d'interdiction pour les règles de Contrôle des applications, choisissez l'option **Appliquer les règles** dans la liste **Action**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Kaspersky Endpoint Security ne bloquera pas les applications dont le lancement est interdit par le module Contrôle des applications, mais enverra des notifications de lancement au Serveur d'administration.

Règles de création de masques de noms de fichiers ou de dossiers

Le *masque du nom de fichier ou de dossier* est une représentation du nom du dossier ou du nom et de l'extension du fichier à l'aide de caractères génériques.

Vous pouvez utiliser les caractères suivants pour créer un masque de nom de fichier ou de dossier :

- Le caractère `*` (astérisque), qui prend la place de tout ensemble de caractères (y compris un ensemble vide). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension `.txt` situés dans des dossiers sur le disque (C:).

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

Modification des modèles de messages du Contrôle des applications

Quand l'utilisateur tente de lancer une application interdite par la règle de Contrôle des applications, Kaspersky Endpoint Security affiche un message sur le blocage du lancement. Si l'utilisateur estime que le blocage du lancement de l'application n'a pas lieu d'être, il peut cliquer sur un lien dans la notification afin d'envoyer un message à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage du lancement de l'application et pour les messages destinés à l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier le modèle de message, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.

4. Cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.

5. Exécutez une des actions suivantes :

   - Si vous souhaitez modifier le modèle de la notification relative au blocage du lancement de l'application, choisissez l'onglet **Blocage**.

   - Pour modifier le modèle de message pour l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Message pour l'administrateur**.

6. Modifiez le modèle de message de blocage ou destiné à l'administrateur. Pour ce faire, utilisez les boutons **Par défaut** et **Variable**.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des modes de fonctionnement du Contrôle des applications

Le module Contrôle des applications peut fonctionner selon deux modes :

- **Liste noire**. Dans ce mode, le Contrôle des applications permet à tous les utilisateurs de démarrer toutes les applications, à l'exception des applications spécifiées dans les règles de blocage du Contrôle des applications.

  Il s'agit du mode de fonctionnement du Contrôle des applications défini par défaut.

- **Liste blanche**. Mode selon lequel le Contrôle des applications interdit à tous les utilisateurs de lancer n'importe quelle application, à l'exception de celles qui figurent dans les règles d'autorisation de Contrôle des applications.

  Si les règles d'autorisation de Contrôle des applications sont les plus strictes, le module interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

  Vous pouvez prendre connaissance des recommandations sur la configuration des règles de Contrôle des applications en mode de liste blanche.

Chaque mode propose deux actions à réaliser sur les applications lancées selon les conditions des règles de Contrôle des applications : Kaspersky Endpoint Security peut bloquer le lancement des applications ou notifier l'utilisateur du lancement des applications.

La configuration du Contrôle des applications pour le fonctionnement dans ces modes est possible à partir de l'interface locale de Kaspersky Endpoint Security ou via Kaspersky Security Center.

Ceci étant dit, Kaspersky Security Center propose des outils qui ne sont pas accessibles dans l'interface locale de Kaspersky Endpoint Security et qui sont indispensables pour réaliser les tâches suivantes :

- Création des catégories d'applications.

  Les règles de Contrôle des applications créées dans la Console d'administration de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.

- Récupération des informations relatives aux applications installées sur les ordinateurs du réseau local de l'entreprise.

C'est pour cette raison qu'il est conseillé de configurer le fonctionnement du module Contrôle des applications via Kaspersky Security Center.

Sélection du mode du Contrôle des applications

Pour sélectionner le mode du Contrôle des applications, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

3. Cochez la case **Contrôle des applications** afin de pouvoir modifier les paramètres du module.

4. Dans la liste déroulante **Mode de contrôle** choisissez une des options suivantes :

   - **Liste noire**, si vous voulez autoriser le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'interdiction ;
   - **Liste blanche**, si vous voulez interdire le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'autorisation.

     Le mode de la liste blanche prévoie au départ la règle **Système d'exploitation et ses modules** qui autorise le lancement des applications qui appartiennent à la catégorie KL « Applications S.E. » ainsi que la règle **Programmes de mise à jour de confiance** qui autorise le lancement des applications qui appartiennent à la catégorie KL Programmes de mise à jour de confiance. La catégorie KL Applications S.E. reprend les applications qui garantissent le fonctionnement normal du système d'exploitation. La catégorie « Programmes de mise à jour de confiance » des catégories KL reprend les programmes de mise à jour des applications des éditeurs les plus connus. Vous ne pouvez pas supprimer ces règles. Les paramètres de ces règles ne peuvent pas être modifiés. Par défaut, la règle **Système d'exploitation et ses modules** est activée tandis que la règle **Programmes de mise à jour de confiance** est désactivée. Le lancement des applications, correspondant aux conditions de déclenchement de ces règles, est autorisé pour tous les utilisateurs.

   Toutes les règles créées dans le mode sélectionné sont enregistres après le changement de mode afin de pouvoir les utiliser à nouveau. Pour revenir à l'utilisation de ces règles, il suffit de choisir le mode requis dans la liste déroulante **Mode de contrôle**.

5. Dans la liste déroulante **Action**, choisissez l'action que le module devra exécuter si l'utilisateur tente de lancer une application interdite par les règles de Contrôle des applications.

6. Cochez la case **Contrôler les DLL et les pilotes** si vous voulez que l'application Kaspersky Endpoint Security contrôle le chargement des modules DLL lorsque les utilisateurs lancent des applications.

   Les informations relatives au module et à l'application qui ont chargé ce module seront enregistrées dans le rapport.

   Kaspersky Endpoint Security contrôle uniquement les modules DLL et les pilotes chargés à partir du moment où la case **Contrôler les DLL et les pilotes** a été cochée. Redémarrer l'ordinateur après avoir coché la case **Contrôler les DLL et les pilotes** si vous voulez que l'application Kaspersky Endpoint Security contrôle tous les modules DLL et les pilotes, y compris ceux qui se chargent avant le lancement de Kaspersky Endpoint Security.

   Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut **Système d'exploitation et ses modules** ou toute autre règle qui contient la catégorie KL « Certificats de confiance » est activée dans la section **Contrôle des applications** et qu'elle garantit le chargement des modules DLL et des pilotes de confiance avant le lancement de Kaspersky Endpoint Security. Les règles de Contrôle des applications créées sur la base d'autres catégories KL (à l'exception de la catégorie KL « Certificats de confiance ») ne sont pas appliquées au contrôle du chargement des modules DLL et des pilotes. L'activation du contrôle du chargement des modules DLL et des pilotes lorsque la règle **Système d'exploitation et ses modules** est désactivée peut provoquer l'instabilité du système d'exploitation.

   Il est recommandé d'activer la protection par mot de passe de la configuration des paramètres de l'application afin de pouvoir désactiver les règles d'interdiction qui bloquent le lancement de modules DLL et de pilotes critiques sans modifier les paramètres de la stratégie de Kaspersky Security Center.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle des périphériques

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Windows pour serveurs de fichiers.

Cette section contient des informations sur le Contrôle des périphériques et les instructions sur la configuration du module.

A propos du Contrôle des périphériques

Le Contrôle des périphériques gère l'accès des utilisateurs aux périphériques installés ou connectés à l'ordinateur (par exemple, disques durs, caméra ou module Wi-Fi). Cela permet de protéger l'ordinateur contre l'infection lors de la connexion de ces périphériques et de prévenir la perte ou la fuite de données.

Le Contrôle des périphériques gère l'accès aux niveaux suivants :

- **Type de périphérique**. Par exemple, imprimantes, disques amovibles, lecteurs CD/DVD.

  Vous pouvez configurer l'accès des périphériques de la manière suivante :

  - Autoriser : .
  - Interdire : .
  - Dépend du bus connexion (excepté Wi-Fi) : .
  - Interdit, avec des exceptions (seulement Wi-Fi) : .

- **Bus de connexion**. Un *bus de connexion* est une interface qui permet de connecter des appareils à l'ordinateur (USB, FireWire, etc.). Ainsi, vous pouvez limiter la connexion de tous les périphériques, par exemple, via USB.

  Vous pouvez configurer l'accès des périphériques de la manière suivante :

  - Autoriser : .
  - Interdire : .

- **Périph. de confiance** Les *Périphériques de confiance* sont les périphériques que les utilisateurs définis dans les paramètres du périphérique de confiance peuvent accéder librement à tout moment.

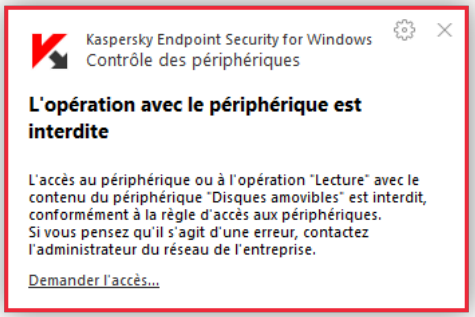
  Vous pouvez ajouter des périphériques de confiance selon les données suivantes :

  - **Identificateur de périphérique**. Chaque périphérique possède un identificateur unique. Vous pouvez consulter l'identificateur dans les propriétés du périphérique à l'aide des outils du système d'exploitation.
  - **Modèle du périphérique**. Chaque périphérique possède les identifiants VID (identificateur du fabricant) et PID (identificateur du produit). Vous pouvez consulter les identificateurs dans les propriétés du périphérique à l'aide des outils du système d'exploitation.
  - **Masque de l'identifiant**. Par exemple, `l'appareil*`.

Le Contrôle des périphériques gère l'accès des utilisateurs aux périphériques à l'aide *de règles d'accès*. Le Contrôle des périphériques permet également d'enregistrer les événements de connexion/déconnexion des périphériques. Pour enregistrer les événements, vous devez configurer l'envoi des événements dans la stratégie.

Si l'accès à l'appareil dépend du bus de connexion (état), Kaspersky Endpoint Security n'enregistre pas l'événement de connexion/de déconnexion de l'appareil. Pour que l'application Kaspersky Endpoint Security enregistre les événements de connexion/de déconnexion de l'appareil, autorisez l'accès au type d'appareil correspondant (état) ou ajoutez l'appareil à la liste des appareils de confiance.

Quand le périphérique se connecte à un ordinateur auquel l'accès est interdit par le Contrôle des périphériques, Kaspersky Endpoint Security bloque l'accès et affiche une notification (cf. ill. ci-dessous).



Notification du Contrôle des périphériques

Activation et désactivation du Contrôle des périphériques

Le Contrôle des périphériques est activé par défaut. Le cas échéant, vous pouvez activer le Contrôle des périphériques.

Pour activer ou désactiver le Contrôle des périphériques, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Contrôle des périphériques** pour activer le Contrôle des périphériques.
   - Décochez la case **Contrôle des périphériques** pour désactiver le Contrôle des périphériques.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles d'accès

Les *règles de l'accès* sont un ensemble de paramètres qui définissent l'accès des utilisateurs aux périphériques installés sur l'ordinateur ou connectés à celui-ci. Il est impossible d'ajouter un périphérique qui n'appartient pas à la classification du Contrôle des périphériques. L'accès à ces périphériques est autorisé pour tous les utilisateurs.

Règles d'accès aux périphériques

Chaque ensemble de paramètres de règle d'accès se distingue en fonction du type de périphériques (cf. le tableau ci-après).

Paramètres de règle d'accès

Périphériques	Accès (Autoriser ✓ / Interdire ⊘ / Dépend du bus ◔)	Planification de l'accès au périphérique	Affectation des utilisateurs/groupes d'utilisateurs	Autorisation en lecture / en écriture
Disques durs	✓	✓	✓	✓
Disques amovibles	✓	✓	✓	✓
Imprimantes	✓	–	–	–
Disquettes	✓	✓	✓	✓
Lecteurs de CD/DVD	✓	✓	✓	✓
modems.	✓	–	–	–
Lecteurs de bande	✓	–	–	–
Périphériques multifonctions	✓	–	–	–
Périphériques de lecture des cartes à puce	✓	–	–	–
Périphériques Windows CE USB ActiveSync	✓	–	–	–
Adaptateurs réseau externes	✓	–	–	–
Périphériques portables (MTP)	✓	✓	✓	✓
Bluetooth	✓	–	–	–
Caméras et scanners	✓	–	–	–

Par défaut, les règles d'accès aux périphériques octroient un accès complet aux périphériques à tous les utilisateurs à tout moment, pour autant que l'accès au bus de connexion pour les types de périphériques correspondants soit autorisé (état ◔).

Règle d'accès aux réseaux Wi-Fi

La règle d'accès aux réseaux Wi-Fi définit l'autorisation (état) ou l'interdiction (état) d'utiliser des réseaux Wi-Fi. Vous pouvez ajouter à la règle un *réseau Wi-Fi de confiance* (état). L'utilisation du réseau Wi-Fi des confiance est autorisée sans restrictions. Par défaut, la règle d'accès aux réseaux Wi-Fi autorise l'accès à n'importe quel réseau Wi-Fi.

Règles d'accès au bus de connexion

Les règles d'accès au bus de connexion déterminent uniquement l'autorisation (état) ou l'interdiction (état) de la connexion de périphériques. Par défaut, les règles qui autorisent l'accès à tous les bus ont été créées pour les bus de connexion de la classification du module Contrôle des périphériques.

A propos des périphériques de confiance

Les *Périphériques de confiance* sont les périphériques que les utilisateurs définis dans les paramètres du périphérique de confiance peuvent accéder librement à tout moment.

Les actions suivantes peuvent être exécutées sur les périphériques de confiance :

- ajout du périphérique à la liste des périphériques de confiance ;
- modification de l'utilisateur et/ou groupe d'utilisateurs qui ont l'accès au périphérique de confiance ;
- suppression du périphérique de la liste des périphériques de confiance.

Si vous avez ajouté un appareil à la liste des appareils de confiance et créé une règle d'accès pour ce type d'appareil qui bloque ou limite l'accès, Kaspersky Endpoint Security décide d'accorder ou non l'accès à l'appareil en fonction de sa présence dans la liste des appareils de confiance. Le fait de figurer dans la liste des appareils de confiance a une priorité plus élevée qu'une règle d'accès.

Décisions types sur l'accès aux périphériques

Une fois que l'utilisateur a connecté un périphérique à l'ordinateur, Kaspersky Endpoint Security prend la décision sur l'accès à ce périphérique.

Décisions types sur l'accès aux périphériques

N°	Conditions d'origine	Étapes intermédiaires avant la prise de décision sur l'accès au périphérique			Décision sur l'accès au périphérique
		Vérification de la présence du périphérique dans la liste des périphériques de confiance	Vérification de l'accès au périphérique sur la base de la règle d'accès	Vérification de l'accès au bus sur la base de la règle d'accès au bus	

1	Le périphérique ne figure pas dans le classement du module Contrôle des périphériques.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante.	Ignoré.	Accès autorisé.
2	Le périphérique est un périphérique de confiance.	Figure sur la liste des périphériques de confiance.	Ignoré.	Ignoré.	Accès autorisé.
3	L'accès au périphérique est autorisé.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé.	Ignoré.	Accès autorisé.
4	Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès autorisé.	Accès autorisé.
5	Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès interdit.	Accès interdit.
6	L'accès au périphérique est autorisé. Règle d'accès au bus inexistante.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé.	Règle d'accès au bus inexistante.	Accès autorisé.
7	Accès au périphérique interdit.	Ne figure pas sur la liste des périphériques de confiance.	Accès interdit.	Ignoré.	Accès interdit.
8	Règle d'accès au périphérique et règle d'accès au bus inexistantes.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante.	Règle d'accès au bus inexistante.	Accès autorisé.
9	Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante.	Accès autorisé.	Accès autorisé.
10	Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante.	Accès interdit.	Accès interdit.

Vous pouvez modifier la règle d'accès au périphérique après sa connexion. Si le périphérique a été connecté et la règle d'accès a autorisé l'accès au périphérique, mais vous avez ensuite modifié la règle d'accès pour interdire l'accès au périphérique, toute tentative d'accès au périphérique pour l'opération de fichiers (consultation de l'arborescence des catalogue, lecture, enregistrement) sera d'ores et déjà bloquée par Kaspersky Endpoint Security. Le blocage du périphérique sans système de fichiers aura lieu uniquement lors de la connexion suivante du périphérique.

Si l'utilisateur de l'ordinateur doté de Kaspersky Endpoint Security doit demander l'accès à un appareil qui, d'après lui, a été bloqué par erreur, transmettez lui l'instruction de demande d'accès.

Modification d'une règle d'accès aux périphériques

En fonction du type de périphérique, vous pouvez modifier différents paramètres d'accès : la liste des utilisateurs ayant accès au périphérique, le calendrier de l'accès et l'autorisation/l'interdiction d'accès.

Pour modifier le privilège d'accès aux périphériques, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Types de périphériques**.

   Sous l'onglet **Types de périphériques** se trouvent les règles d'accès pour tous les périphériques qui figurent dans le classement du module Contrôle des périphériques.
4. Sélectionnez la règle d'accès que vous souhaitez modifier.
5. Cliquez sur le bouton **Modifier**. Le bouton est accessible uniquement pour les types de périphériques avec un système de fichiers.

   La fenêtre **Configuration de la règle d'accès aux périphériques** s'ouvre.

   Par défaut, la règle d'accès aux périphériques autorise un accès libre au type de périphériques à tout moment pour tous les utilisateurs. Dans la liste **Utilisateurs et/ou groupes d'utilisateurs**, cette règle d'accès contient le groupe **Tous**. Dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès**, cette règle d'accès contient la **Planification par défaut** pour l'accès aux appareils, avec le droit d'effectuer tous types d'opérations avec les appareils.
6. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.
7. Procédez comme suit :

   - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :

     1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

        La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

     2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

     3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

        Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

   - Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

     Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.

8. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

9. Dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès**, configurez la programmation de l'accès aux périphériques pour l'utilisateur et/ou le groupe sélectionné d'utilisateurs. Pour ce faire, cochez les cases à côté des noms des programmations de l'accès aux périphériques que vous souhaitez utiliser dans la règle modifiable d'accès aux périphériques.

10. Pour modifier la liste de programmations d'accès aux périphériques, utilisez les boutons **Générer**, **Modifier**, **Copier**, **Supprimer** dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès**.

11. Pour chaque planification de l'accès aux périphériques utilisée dans la règle modifiée, spécifiez les opérations qui sont autorisées dans le cadre de l'utilisation des périphériques. Pour ce faire, dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès** cochez les cases dans les colonnes portant les noms des opérations requises.

12. Cliquez sur le bouton **OK**.

    Une fois que vous avez modifié les valeurs d'origine des paramètres de la règle d'accès aux périphériques, le paramètre d'accès au type de périphérique dans la colonne **Accès** de l'onglet **Types de périphériques** du tableau prend la valeur *Limiter à l'aide de règles*.

13. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de l'enregistrement des événements dans le journal

L'enregistrement des événements dans le journal est accessible seulement pour les opérations sur les fichiers des disques amovibles.

Pour activer ou désactiver l'enregistrement des événements dans le journal, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Types de périphériques**.

   Sous l'onglet **Types de périphériques** se trouvent les règles d'accès pour tous les périphériques qui figurent dans le classement du module Contrôle des périphériques.

4. Choisissez **Disques amovibles** dans le tableau des périphériques.

   Le bouton **Enregistrement des événements dans le journal** est accessible dans partie supérieure du tableau.

5. Cliquez sur le bouton **Enregistrement des événements dans le journal**.

   La fenêtre **Paramètres d'enregistrement des événements dans le journal** s'ouvre.

6. Exécutez une des actions suivantes :

   - Si vous voulez activer l'enregistrement des événements relatifs aux opérations et la suppression des fichiers sur les disques amovibles, cocher la case **Activer l'enregistrement des événements dans le journal**.

Kaspersky Endpoint Security enregistrera l'événement le fichier journal et enverra un message sur le Serveur d'administration de Kaspersky Security Center quand l'utilisateur exécutera des opérations d'écriture ou de suppressions dans les fichiers des disques amovibles.

- Dans le cas contraire, décochez la case **Activer l'enregistrement des événements dans le journal**.

7. Indiquez les informations des opérations qu'il faudra consigner dans le journal. Pour ce faire, exécutez une des actions suivantes :

   - Si vous voulez que Kaspersky Endpoint Security enregistre dans le journal tous les événements, cochez la case **Enregistrer les informations sur tous les fichiers**.

   - Si vous voulez que Kaspersky Endpoint Security enregistre dans le journal uniquement les informations relatives à des fichiers d'un format défini, cochez les cases en regard des formats de fichiers requis dans le groupe **Filtre selon le format des fichiers**.

8. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.

   Quand les utilisateurs indiqués dans le groupe **Utilisateurs** génèreront une entrée dans les fichiers situés sur les disques durs ou lorsqu'ils les supprimeront, Kaspersky Endpoint Security enregistrera les informations sur l'opération réalisées dans le journal des événements et enverra le message au Serveur d'administration de Kaspersky Security Center.

9. Procédez comme suit :

   - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :

     1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

        La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

     2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

     3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

        Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

   - Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

     Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.

10. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

11. Dans la fenêtre **Paramètres d'enregistrement des événements dans le journal**, cliquez sur le bouton **OK**.

12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Vous pouvez consulter les événements liés aux fichiers sur les disques amovibles, dans la Console d'administration de Kaspersky Security Center dans l'espace de travail pour l'entrée **Serveur d'administration** de l'onglet **Événements**. Pour que les événements s'affichent dans le journal local des événements de Kaspersky Endpoint Security, il faut cocher la case **Exécution d'une opération sur un fichier** dans les paramètres des notifications du module Contrôle des périphériques.

Ajout d'un réseau Wi-Fi à la liste des réseaux de confiance

Vous pouvez permettre aux utilisateurs de se connecter aux réseaux Wi-Fi que vous considérés sûr, par exemple au réseau Wi-Fi de l'entreprise. Pour cela, il faut ajouter ce réseau à la liste des réseaux Wi-Fi de confiance. Le Contrôle des périphériques bloquera l'accès à tous les réseaux Wi-Fi, à l'exception de ceux qui figurent dans la liste des réseaux de confiance.

Pour ajouter un réseau Wi-Fi à la liste des réseaux de confiance, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Types de périphériques**.

   Sous l'onglet **Types de périphériques** se trouvent les règles d'accès pour tous les périphériques qui figurent dans le classement du module Contrôle des périphériques.
4. Dans la colonne **Accès** en face du périphérique **Wi-Fi**, invoquez le menu contextuel d'un clic droit de la souris.
5. Choisissez l'option **Interdire avec des exceptions**.
6. Dans la liste des périphériques choisissez **Wi-Fi**, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Réseaux Wi-Fi de confiance** s'ouvre.
7. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Réseau Wi-Fi de confiance** s'ouvre.
8. Dans la fenêtre **Réseau Wi-Fi de confiance**, procédez comme suit :

   - Saisissez dans le champ **Nom du réseau** le nom du réseau Wi-Fi que vous souhaitez ajouter à la liste des réseaux de confiance.
   - Sélectionnez dans la liste déroulante **Type d'authentification** le type d'authentification à utiliser lors de la connexion au réseau Wi-Fi de confiance.
   - Sélectionnez dans la liste déroulante **Type de chiffrement** choisissez le type de chiffrement à utiliser pour la protection du trafic du réseau Wi-Fi de confiance.
   - Vous pouvez saisir dans le champ **Commentaires** n'importe quelle information sur le réseau Wi-Fi ajouté.

   Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.
9. Dans la fenêtre **Réseau Wi-Fi de confiance**, cliquez sur **OK**.
10. Dans la fenêtre **Réseaux Wi-Fi de confiance**, cliquez sur **OK**.

Modification de la règle d'accès au bus de connexion

Pour modifier la règle d'accès au bus de connexion, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez l'onglet **Bus de connexion**.

   Sous l'onglet **Bus de connexion** se trouvent les règles d'accès pour tous les bus de connexion qui existent dans la classification du module Contrôle des périphériques.
4. Sélectionnez la règle d'accès au bus que vous souhaitez modifier.
5. Modifiez la valeur du paramètre d'accès :

   - Pour autoriser l'accès au bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Autoriser**.
   - Pour interdire l'accès au bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Interdire**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Actions avec les périphériques de confiance

Cette section contient des informations sur les actions avec les périphériques de confiance.

Ajout de périphériques à la liste des périphériques de confiance via l'interface de l'application

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

Pour ajouter un périphérique à la liste des périphériques de confiance via l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

4. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des périphériques de confiance** s'ouvre.

5. Cochez la case en regard du nom du périphérique que vous souhaitez ajouter à la liste des périphériques de confiance.

   La liste des périphériques dans la colonne **Périphériques** dépend de la valeur sélectionnée dans la liste déroulante **Afficher les périphériques connectés**.

6. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.

7. Procédez comme suit :

   - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :

     1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

        La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

     2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

     3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

        Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

   - Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

     Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.

8. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

9. Cliquez sur le bouton **OK**.

10. Dans la fenêtre **Sélection des périphériques de confiance**, cliquez **OK**.

    Sous l'onglet **Appareils de confiance** de la fenêtre de configuration du module **Contrôle des appareils** du tableau s'affichera la ligne qui présente les paramètres de l'appareil de confiance ajouté.

11. Répétez les étapes 4 à 7 pour chacun des périphériques que vous souhaitez ajouter à la liste des périphériques de confiance pour des utilisateurs et/ou des groupes d'utilisateurs spécifiques.

12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Ajout de périphériques à la liste des périphériques de confiance en fonction de leur modèle ou de leur identificateur

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

Pour ajouter un périphérique à la liste des périphériques de confiance en fonction de leur modèle ou de leur identificateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez créer une liste d'appareils de confiance.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.
6. Dans la section **Contrôles de sécurité**, sélectionnez **Contrôle des appareils**.
7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.
8. Cliquez sur le bouton **Ajouter**.

   Le menu contextuel du bouton s'ouvre.
9. Dans le menu déroulant du bouton **Ajouter**, exécutez une des actions suivantes :
   - Sélectionnez le bouton **Appareils en fonction de l'identificateur** si vous souhaitez sélectionner des appareils dont l'identifiant unique est connu pour les ajouter à la liste des appareils de confiance.
   - Sélectionnez l'élément **Appareils en fonction du modèle** pour ajouter à la liste les appareils de confiance dont le VID (identifiant du fournisseur) et le PID (identifiant du produit) sont connus.
10. Dans la fenêtre qui s'ouvre, dans la liste déroulante **Type d'appareil**, sélectionnez le type d'appareil à ajouter au tableau plus bas.
11. Cliquez sur le bouton **Actualiser**.

    Le tableau affiche une liste d'appareils dont les identifiants et/ou les modèles sont connus et qui appartiennent au type sélectionné dans la liste déroulante **Type d'appareil**.
12. Cochez les cases en regard des noms des périphériques que vous souhaitez ajouter à la liste des périphériques de confiance.
13. Cliquez sur le bouton **Sélectionner**.

    La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.
14. Procédez comme suit :
    - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :
      1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

         La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

   Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

- Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

  Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.

15. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

16. Cliquez sur le bouton **OK**.

    Des lignes s'affichent avec les paramètres des appareils de confiance qui ont été ajoutés dans le tableau de l'onglet **Appareils de confiance**.

17. Cliquez sur **OK** ou sur **Appliquer** pour enregistrer les modifications.

Ajout de périphériques à la liste des périphériques de confiance en fonction du masque de leur identificateur

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

L'ajout d'appareils à la liste des appareils de confiance selon un masque de leur identificateur est uniquement possible depuis la Console d'administration de Kaspersky Security Center.

Pour ajouter des périphériques à la liste des périphériques de confiance en fonction du masque de leur identificateur, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez créer une liste d'appareils de confiance.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :

   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.

   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.

6. Dans la section **Contrôles de sécurité**, sélectionnez **Contrôle des appareils**.

7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

8. Cliquez sur le bouton **Ajouter**.

   Le menu contextuel du bouton s'ouvre.

9. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'élément **Appareils en fonction du masque de l'identifiant**.

   La fenêtre **Ajout d'appareils de confiance en fonction du masque d'identifiant** s'ouvre.

10. Dans la fenêtre **Ajout de périphériques de confiance en fonction du masque d'identifiant**, saisissez le masque pour les identifiants de l'appareil dans le champ **Masque**.

11. Cliquez sur le bouton **Sélectionner**.

    La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.

12. Procédez comme suit :

    - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :

      1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

         La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

      2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

      3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

         Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

    - Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

      Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.

13. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

14. Cliquez sur le bouton **OK**.

    Dans le tableau de l'onglet **Appareils de confiance** de la fenêtre des paramètres du module **Contrôle des appareils**, une ligne s'affiche avec les paramètres de la règle d'ajout d'appareils à la liste des appareils de confiance en fonction du masque de leurs identifiants.

15. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'accès des utilisateurs au périphérique de confiance

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder. Vous pouvez configurer l'accès des utilisateurs (et des groupes d'utilisateurs) à un périphérique de confiance.

Pour configurer l'accès des utilisateurs au périphérique de confiance, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.
4. Dans la liste des périphériques de confiance, sélectionnez le périphérique dont vous souhaitez modifier les règles d'accès.
5. Cliquez sur le bouton **Modifier**.

   La fenêtre **Configuration de la règle d'accès aux appareils de confiance** s'ouvre.
6. Cliquez sur le bouton **Sélectionner**.

   La fenêtre **Sélection des utilisateurs et/ou des groupes** s'ouvre.
7. Procédez comme suit :

   - Si vous voulez ajouter des utilisateurs et/ou des groupes d'utilisateurs dans le tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, procédez comme suit :

     1. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **Ajouter**.

        La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

     2. Définissez dans la fenêtre Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

     3. Dans la fenêtre Windows **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.

        Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélection des utilisateurs et/ou des groupes** sont affichés dans le champ **Sélection des utilisateurs et/ou des groupes**.

   - Si vous voulez supprimer des utilisateurs et/ou des groupes d'utilisateurs dans tableau de la fenêtre **Sélection des utilisateurs et/ou des groupes**, choisissez une ou plusieurs ligne dans le tableau, puis cliquez sur le bouton **Supprimer**.

     Pour sélectionner plusieurs lignes, choisissez-les en maintenant la touche **CTRL** enfoncée.
8. Dans la fenêtre **Sélection des utilisateurs et/ou des groupes**, cliquez sur le bouton **OK**.
9. Cliquez sur le bouton **OK**.
10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression du périphérique de la liste des périphériques de confiance

Pour supprimer le périphérique de la liste des périphériques de confiance, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

4. Sélectionnez le périphérique que vous souhaitez supprimer de la liste des périphériques de confiance.

5. Cliquez sur le bouton **Supprimer**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

La décision sur l'accès au périphérique que vous avez supprimé de la liste des périphériques de confiance est prise par Kaspersky Endpoint Security sur la base des règles d'accès aux périphériques et sur la base des règles d'accès aux bus de connexion.

Importation de la liste des périphériques de confiance

Pour importer une liste de périphériques de confiance, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

4. Cliquez sur le bouton **Importer**.

   La fenêtre **Sélection du fichier de configuration** s'ouvre.

5. Dans la fenêtre **Sélection du fichier de configuration**, choisissez le fichier au format XML à partir duquel vous voulez importer la liste des périphériques de confiance, puis cliquez sur le bouton **Ouvrir**.

   Si la liste des appareils de confiance contient certains éléments, vous verrez s'afficher une fenêtre intitulée **La liste contient déjà des éléments**. Dans cette fenêtre, vous pouvez effectuer l'une des actions suivantes :

   - Cliquez sur le bouton **Oui** si vous voulez ajouter les éléments importés aux éléments existants.
   - Cliquez sur le bouton **Non** si vous voulez supprimer les éléments existants avant d'ajouter les éléments importés.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Exportation de la liste des périphériques de confiance

Pour exporter une liste de périphériques de confiance, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périph. de confiance**.

4. Choisissez les éléments de la liste que vous voulez exporter.

5. Cliquez sur le bouton **Exporter**.

   La fenêtre **Sélection du fichier de configuration** s'ouvre.

6. Dans la fenêtre **Sélection du fichier de configuration**, indiquez le nom du fichier au format XML dans lequel vous voulez exporter la liste des périphériques de confiance et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier, puis cliquez sur le bouton **Enregistrer**.

Modification des modèles de messages du Contrôle des périphériques

Quand l'utilisateur tente de s'adresser au périphérique bloqué, Kaspersky Endpoint Security affiche le message sur le blocage d'accès au périphérique ou sur l'interdiction de l'opération sur le contenu du périphérique. Si l'utilisateur considère que le blocage de l'accès au périphérique ou l'interdiction de l'opération sur le contenu du périphérique est une erreur, il peut envoyer un message à l'administrateur du réseau local de l'organisation via le lien qui apparaît dans le texte du message relatif au blocage.

Il existe des modèles prévus pour les messages de blocage d'accès au périphérique ou d'interdiction des opérations sur le contenu ainsi que des modèles de messages pour l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier les modèles de message du Contrôle des périphériques, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.

4. Exécutez une des actions suivantes :

   - Pour modifier le modèle du message de blocage d'accès au périphérique ou d'interdiction d'une opération sur le contenu du périphérique, sélectionnez l'onglet **Blocage**.

   - Pour modifier le modèle de message de message pour l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Message pour l'administrateur**.

5. Modifier le modèle de message. De plus vous pouvez utiliser les boutons **Variable**, **Par défaut** et **Lien** (le bouton est disponible uniquement sous l'onglet **Blocage**).

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Anti-Bridging

Cette section contient des informations sur la fonction Anti-Bridging et les instructions sur la configuration de celle-ci.

A propos d'Anti-Bridging

La fonction Anti-Bridging assure la protection contre les ponts réseau en empêchant la possibilité d'établir simultanément plusieurs connexions réseau pour un ordinateur doté de l'application Kaspersky Endpoint Security.

Activation de désactivation d'Anti-Bridging

La fonctionnalité Anti-Bridging est désactivée par défaut. Le cas échéant, vous pouvez activer cette fonction.

Pour activer ou désactiver la fonction Anti-Bridging, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Anti-Bridging**.

   La fenêtre **Anti-Bridging** s'ouvre.
4. Exécutez une des actions suivantes :

   - Cochez la case **Activer l'Anti-Bridging** pour activer la protection contre les ponts réseau.

     Après l'activation de la fonction Anti-Bridging, Kaspersky Endpoint Security bloque les connexions déjà établies conformément aux règles d'établissement des connexions.

   - Décochez la case **Activer l'Anti-Bridging** pour désactiver la protection contre les ponts réseau.
5. Dans la fenêtre **Anti-Bridging**, cliquez sur **OK**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A propos des règles d'établissement d'une connexion

Il existe des règles d'établissement d'une connexion pour les types de périphériques préinstallés suivants :

- adaptateurs réseau ;
- adaptateurs Wi-Fi ;

- Modems

Si la règle d'établissement d'une connexion est activée, Kaspersky Endpoint Security exécute les actions suivantes :

- bloque la connexion active lors de l'établissement d'une nouvelle connexion si le type de périphérique indiqué dans la règle est utilisé pour les deux connexions ;
- bloque les connexions établies ou qui vont être établies à l'aide des types de périphérique soumis à des règles d'une priorité inférieure.

Modification de l'état d'une règle d'établissement de connexion

Pour modifier l'état de la règle d'établissement de la connexion, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Anti-Bridging**.

   La fenêtre **Anti-Bridging** s'ouvre.
4. Sélectionnez la règle dont vous souhaitez modifier l'état.
5. Dans la colonne **Contrôle**, ouvrez le menu contextuel d'un clic gauche de la souris et exécutez une des actions suivantes :
   - Pour activer l'utilisation de la règle, sélectionnez l'option **Actif**.
   - Pour désactiver l'utilisation de la règle, sélectionnez l'option **Désact**.
6. Dans la fenêtre **Anti-Bridging**, cliquez sur **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de la priorité d'une règle d'établissement de connexion

Pour modifier l'état de la règle d'établissement de la connexion Contrôle des applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Anti-Bridging**.

   La fenêtre **Anti-Bridging** s'ouvre.
4. Sélectionnez la règle dont vous souhaitez modifier la priorité.

5. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Monter** pour déplacer la règle vers le haut du tableau.
   - Cliquez sur le bouton **Descendre** pour déplacer la règle vers le bas du tableau.

   Plus la règle se trouve vers le haut du tableau des règles, plus elle bénéficie d'une priorité élevée. La fonction Anti-Bridging bloque toutes les connexions, à l'exception d'une connexion établie à l'aide du type d'appareils pour lequel la règle de priorité supérieure est utilisée.

6. Dans la fenêtre **Anti-Bridging**, cliquez sur **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Obtention de l'accès au périphérique bloqué

Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

La fonctionnalité de Kaspersky Endpoint Security qui garantit un accès temporaire à l'appareil est disponible uniquement dans le cas où l'appareil fonctionne sous une stratégie de Kaspersky Security Center et que cette fonctionnalité a été activée dans les paramètres de la stratégie (pour en savoir plus, consultez l'aide de Kaspersky Security Center).

Pour solliciter un accès à un périphérique bloqué, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle des appareils**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Demander l'accès**.

   La fenêtre **Demander l'accès à l'appareil** s'ouvre.

4. Sélectionnez dans la liste des périphériques connectés le périphérique que vous souhaitez accéder.

5. Cliquez sur le bouton **Créer un fichier de requête**.

   Bouton qui ouvre la fenêtre **Création du fichier de requête**.

6. Indiquez dans le champ **Durée de l'accès au périphérique** la durée pendant laquelle vous souhaitez avoir accès au périphérique.

7. Cliquez sur le bouton **Enregistrer**.

   La fenêtre standard de Microsoft Windows **Enregistrer le fichier d'accès à la demande** s'ouvre.

8. Dans la fenêtre **Enregistrer le fichier d'accès à la demande** de Microsoft Windows, sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier de demande d'accès pour le périphérique, puis cliquez sur le bouton **Enregistrer**.

9. Transmettez le fichier de requête d'accès au périphérique à l'administrateur du réseau local de l'organisation.

10. Il vous remettra le fichier contenant la clé d'accès au périphérique.

11. Dans la fenêtre **Demande d'accès au périphérique**, cliquez sur le bouton **Activer la clé d'accès**.

    La fenêtre standard de Microsoft Windows **Ouvrir la clé d'accès** s'ouvre.

12. Dans **Ouvrir la clé d'accès** fenêtre de Microsoft Windows, sélectionnez le fichier de clé d'accès au périphérique reçu de l'administrateur LAN et cliquez sur **Ouvrir**.

    La fenêtre **Activation de la clé d'accès pour l'appareil** s'ouvre et affiche des informations sur l'accès accordé.

13. Dans la fenêtre **Activation de la clé d'accès pour l'appareil**, cliquez sur **OK**.

Pour solliciter l'accès au périphérique bloqué via le lien dans le message de blocage de l'appareil, procédez comme suit :

1. Dans la fenêtre avec le message qui informe qu'un périphérique ou un bus de connexion est bloqué, cliquez sur le lien **Demander l'accès**.

   Bouton qui ouvre la fenêtre **Création du fichier de requête**.

2. Indiquez dans le champ **Durée de l'accès au périphérique** la durée pendant laquelle vous souhaitez avoir accès au périphérique.

3. Cliquez sur le bouton **Enregistrer**.

   La fenêtre standard de Microsoft Windows **Enregistrer le fichier d'accès à la demande** s'ouvre.

4. Dans la fenêtre **Enregistrer le fichier d'accès à la demande** de Microsoft Windows, sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier de demande d'accès pour le périphérique, puis cliquez sur le bouton **Enregistrer**.

5. Transmettez le fichier de requête d'accès au périphérique à l'administrateur du réseau local de l'organisation.

6. Il vous remettra le fichier contenant la clé d'accès au périphérique.

7. Dans la fenêtre **Demande d'accès au périphérique**, cliquez sur le bouton **Activer la clé d'accès**.

   La fenêtre standard de Microsoft Windows **Ouvrir la clé d'accès** s'ouvre.

8. Dans **Ouvrir la clé d'accès** fenêtre de Microsoft Windows, sélectionnez le fichier de clé d'accès au périphérique reçu de l'administrateur LAN et cliquez sur **Ouvrir**.

   La fenêtre **Activation de la clé d'accès pour l'appareil** s'ouvre et affiche des informations sur l'accès accordé.

9. Dans la fenêtre **Activation de la clé d'accès pour l'appareil**; cliquez sur **OK**.

La durée d'accès au périphérique octroyée peut varier de celle que vous avez demandée. L'accès au périphérique est octroyé pour une durée que l'administrateur du réseau local indique lors de la création de la clé d'accès au périphérique.

Création d'une clé d'accès à l'appareil bloqué à l'aide de Kaspersky Security Center

L'accès temporaire d'un utilisateur à un périphérique bloqué requiert un code d'accès à ce périphérique. Vous pouvez créer une clé d'accès à l'aide de Kaspersky Security Center.

Pour créer la clé d'accès au périphérique bloqué, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques.**
4. Dans la liste des postes clients, sélectionnez l'ordinateur à l'utilisateur duquel vous souhaitez octroyer un accès temporaire au périphérique bloqué.
5. Dans le menu contextuel de l'ordinateur, choisissez l'option **Autoriser l'accès en mode hors ligne**.

   La fenêtre **Autoriser l'accès en mode hors ligne** s'ouvre.
6. Sélectionnez l'onglet **Contrôle des périphériques**.
7. Sous l'onglet **Contrôle des périphériques**, cliquez sur **Parcourir**.

   La fenêtre standard de Microsoft Windows **Sélectionnez le fichier d'accès à la demande** s'ouvre.
8. Dans la fenêtre **Sélectionner le fichier d'accès aux demandes**, sélectionnez le fichier d'accès aux demandes que vous avez reçu de l'utilisateur et cliquez sur le bouton **Ouvrir**.

   Le **Contrôle des périphériques** affiche les détails de l'appareil verrouillé auquel l'utilisateur a demandé l'accès.
9. Définissez la valeur du paramètre **Durée d'accès**.

   Ce paramètre détermine la durée pendant laquelle vous permettez à l'utilisateur d'accéder au périphérique bloqué. La valeur proposée par défaut est celle indiquée par l'utilisateur lors de la création du fichier de requête.
10. Définissez la valeur du paramètre **Période d'activation**.

    Le paramètre définit la période au cours de laquelle l'utilisateur peut activer l'accès au périphérique bloqué à l'aide de la clé d'accès fournie.
11. Cliquez sur le bouton **Enregistrer**.

    Bouton qui ouvre une fenêtre Microsoft Windows **Enregistrement de la clé d'accès** standard.
12. Sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès au périphérique bloqué.
13. Cliquez sur le bouton **Enregistrer**.

Contrôle Internet

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Windows pour serveurs de fichiers.

Cette section contient des informations sur le Contrôle Internet et des instructions sur la configuration du module.

A propos du Contrôle Internet

Le module Contrôle Internet permet de contrôler l'activité utilisateur du réseau local d'entreprise : limiter ou autoriser l'accès aux sites Internet.

Une ressource Internet désigne aussi bien une page Internet individuelle ou plusieurs pages ainsi qu'un site Internet ou plusieurs sites regroupés selon des traits communs.

Le Contrôle Internet offre les possibilités suivantes :

- Économie du trafic.

  Pour contrôler le trafic le module offre la possibilité de limiter ou interdire le téléchargement des fichiers multimédia et de limiter ou interdire l'accès aux sites Internet sans rapport avec l'activité professionnelle.

- Délimitation de l'accès selon les catégories de contenu des sites Internet.

  Pour minimiser le trafic et les pertes éventuelles dues à l'abus d'accès, vous pouvez limiter ou interdire l'accès aux sites Internet de catégories spécifiques (par exemple, interdire l'accès aux sites Internet appartenant à la catégorie "Communication sur Internet").

- Une gestion centralisée d'accès aux sites Internet.

  Dans le cadre de l'utilisation de Kaspersky Security Center, il est possible de configurer l'accès aux ressources Internet tant pour des individus que pour des groupes.

Toutes les restrictions et tous les blocs appliqués pour accéder aux ressources Internet sont implémentés en tant que règles d'accès aux ressources Internet.

Activation et désactivation du Contrôle Internet

Le Contrôle Internet est activé par défaut. Vous pouvez désactiver le Contrôle Internet le cas échéant.

Pour activer ou désactiver le Contrôle Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Contrôle Internet** pour activer le Contrôle Internet.
   - Décochez la case **Contrôle Internet** pour désactiver le Contrôle Internet.

   Si le Contrôle Internet est désactivé, Kaspersky Endpoint Security ne contrôle pas l'accès aux sites Internet.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Catégories de contenu de ressources Internet

Les catégories de contenu de ressources Internet (ci-après, "catégories") reprises ci-dessous sont organisées de manière à décrire le plus complètement possible les informations publiées sur les ressources Internet en tenant compte de leurs caractéristiques thématiques et fonctionnelles. L'ordre des catégories dans la liste n'a aucun rapport avec l'importance relative de ces catégories, ni avec leur représentation sur Internet. Les noms des catégories sont conventionnels et ils sont uniquement utilisés dans le cadre des applications et des sites Internet de Kaspersky. Ils ne correspondent pas nécessairement à la définition qu'ils possèdent dans les législations applicables. Une même ressource Internet peut appartenir à plusieurs catégories simultanément.

Contenu pour adultes

Cette catégorie reprend les types de ressources Internet :

- Contenant des photos ou des vidéos illustrant les organes génitaux de personnes ou d'humanoïdes, des actes sexuels ou des scènes de masturbation impliquant des personnes ou des humanoïdes.
- Contenant du texte, y compris des textes littéraires et artistiques, décrivant les organes génitaux de personnes ou d'humanoïdes ou des actes sexuels ou des scènes de masturbation impliquant des personnes ou des humanoïdes.
- Traitant de la dimension sexuelle des relations humaines.
- Contenant du matériel érotique, des œuvres traitant de manière réaliste de la vie sexuelle de l'homme ou des œuvres d'art visant à stimuler l'excitation sexuelle.
- Sites de médias officiels ou de communautés en ligne avec un public cible proposant une rubrique spéciale et/ou des articles consacrés à la sexualité.
- Consacrées aux sévices sexuels.
- Consacrées à la publicité et à la vente d'objets prévus pour le sexe et la stimulation sexuelle, les services sexuels, les services de rencontre intime, y compris les services en ligne avec chat vidéo érotique, au "sexe par téléphone" ou au "sexe par correspondance" ("sexe virtuel").
- Les ressources Internet présentant le contenu suivant :
  - Articles et blogs consacrés à l'éducation sexuelle, de caractère scientifique ou de vulgarisation.
  - Encyclopédies médicales et leurs articles consacrés à la reproduction sexuelle.
  - Ressources d'institutions médicales et leurs sections consacrées au traitement des organes génitaux.

Logiciel, audio, vidéo

La catégorie inclut les sous-catégories suivantes que vous pouvez choisir séparément :

- **Audio et vidéo**.

  La sous-catégorie reprend les ressources Internet qui diffusent des clips audio ou vidéo : films, enregistrements d'événements sportifs, enregistrements de concerts, chansons, clips vidéo, enregistrements audio et vidéo scientifique, etc.

- **Torrents**.

  La sous-catégorie reprend les sites Internet de trackers torrent prévus pour l'échange de fichiers sans taille limite.

- **Partage de fichiers**.

  Cette sous-catégorie reprend les torrents et sites Internet de stockage de fichiers, quel que soit l'emplacement physique des fichiers propagés.

Alcool, tabac, narcotiques

La catégorie reprend les ressources Internet en rapport direct ou indirect avec la production d'alcool, le tabac et les drogues et autres substances psychotropes :

- Sites consacrés à la publicité et à la vente des substances ainsi qu'aux articles nécessaires à leur consommation.
- Contenant des instructions sur la consommation et la préparation des drogues et autres substances psychotropes.

Les ressources Internet traitant de sujets scientifiques ou médicaux appartiennent à cette catégorie.

Violence

La catégorie regroupe les ressources Internet contenant toute photo, vidéo ou texte qui décrivent des actes de violence physique ou psychologique contre des personnes ou de cruauté contre des animaux :

- Illustration ou description d'exécutions et de séances de torture, ainsi que des instruments intervenant dans de telles actions.

  Chevauchement avec la catégorie Armes, explosifs, pyrotechniques.

- Illustration/description de scènes de meurtre, de bagarres, de passage à tabac, de viol, de scènes de moqueries contre des personnes, des animaux ou des créatures imaginaires.
- Informations incitant à la réalisation d'action présentant une menace pour la vie et/ou la santé, y compris des actions pouvant entraîner le lecteur à s'infliger des blessures ou à se suicider.
- Informations justifiant l'utilisation de la violence et/ou de la cruauté ou incitant à la violence contre des personnes ou des animaux.
- Description/illustration réaliste des victimes ou des horreurs de la guerre, des conflits armés, des accidents, des catastrophes naturelles, des cataclysmes technologiques ou sociaux, de la souffrance des gens.
- Jeux contenant des scènes de violence et de cruauté, y compris les jeux contenant des mots tels que "shooter", "fighting", "slasher", etc.

  Chevauchement avec la catégorie "Jeux".

Armes, explosifs, pyrotechniques

Cette catégorie reprend les ressources Internet contenant des informations sur les armes, les substances explosives et les articles pyrotechniques :

- Sites des fabricants d'armes et de magasins d'armes, de substances explosives et de feux d'artifice.
- Sites consacrés à la préparation et à l'utilisation d'armes, de substances explosives et de feux d'artifice.
- Sites contenant des informations analytiques, historiques, pratiques et encyclopédiques sur les armes, les substances explosives et les feux d'artifice.

Par "arme", il faut entendre tout dispositif ou objet prévu pour nuire à la vie ou à la santé d'une personne ou d'un animal et/ou pour mettre hors service des équipements.

Vulgarité

Cette catégorie reprend les ressources Internet qui contiennent du langage vulgaire.

Chevauchement avec la catégorie "Contenu pour adultes".

Cette catégorie reprend également les ressources Internet proposant des documents linguistiques et philologiques qui étudient le langage vulgaire.

Communication sur le réseau

Cette catégorie reprend les ressources Internet qui, d'une manière ou d'une autre, permettent aux utilisateurs, enregistrés ou non, d'envoyer des messages personnels à d'autres utilisateurs des ressources correspondantes ou d'autres services Internet et/ou de participer, sous certaines conditions, à l'enrichissement de contenu public ou privé sur les sites correspondants. Vous pouvez choisir les sous-catégories suivantes séparément :

- **Tchats et forums**.

  La sous-catégorie reprend les ressources Internet prévues pour la discussion publique de divers sujets à l'aide d'applications Internet spéciales, ainsi que les ressources Internet destinées à la diffusion et au support des clients de messagerie instantanée qui permettent de communiquer en temps réel.

- **Blogs**.

  La sous-catégorie intègre les plateformes de blog, à savoir les sites Internet qui offrent des services gratuits ou payant de création et de maintien de blogs.

- **Réseaux sociaux**.

  Cette sous-catégorie reprend les sites prévus pour favoriser et organiser les contacts entre des personnes, organisations ou des gouvernements et dont l'utilisation requiert la création d'un compte utilisateur.

- **Sites de rencontres**.

  La sous-catégorie reprend les ressources Internet qui représentent une variété de réseaux sociaux et qui proposent des services gratuits ou payants.

Chevauchement avec les catégories "Contenu pour adultes".

- **Emails en ligne**.

  Cette sous-catégorie reprend les pages d'ouverture de session dans un service de messagerie et pages de boîte aux lettres contenant des messages électroniques et les données associées (par exemple, les contacts personnels). Les autres pages du fournisseur d'accès Internet qui propose le service de messagerie ne figurent pas dans cette catégorie.

Jeux de hasard, loterie, tirages au sort

Cette catégorie reprend les ressources Internet qui proposent aux visiteurs de jouer pour de l'argent, même si cela n'est pas une condition obligatoire de l'utilisation de la ressource Internet. La catégorie reprend les ressources Internet suivantes :

Jeux de hasard impliquant une mise financière.

Chevauchement avec la catégorie "Jeux".

- Tirages au sort impliquant une participation financière
- Loteries qui impliquent l'achat de billets de loterie ou des numéros.
- Informations pouvant donner l'envie de jouer à des jeux de hasard, de participer à des tirages au sort ou des loteries.

La catégorie reprend également les jeux proposant une participation gratuite en mode particulier, ainsi que les ressources Internet qui invitent activement les visiteurs à se rendre sur des sites appartenant aux types décrits dans cette catégorie.

Boutiques en ligne, banques en ligne, systèmes de paiement

Cette catégorie reprend les ressources Internet prévues pour la réalisation de n'importe quelle opération par paiement électronique en ligne à l'aide d'applications spéciales. Vous pouvez choisir les sous-catégories suivantes séparément :

- **Boutiques en ligne**.

  Cette sous-catégorie reprend les boutiques en ligne et les sites de vente aux enchères pour la vente de n'importe quel article, travail ou service à des personnes physiques ou morales, y compris les sites de magasins qui travaillent exclusivement sur Internet, ainsi que les représentations sur Internet de magasins traditionnels qui se caractérisent par la possibilité de réaliser des paiements en ligne.

- **Banques**.

  Cette sous-catégorie reprend les pages Internet spéciales de banques proposant des services de transactions bancaires par Internet, dont des virements électroniques entre comptes bancaires, l'ouverture de comptes, la conversion d'instruments financiers, le paiement des services d'organisations tierces, etc.

- **Systèmes de paiement**.

  Cette sous-catégorie reprend les pages Internet des systèmes de paiement électronique qui donnent accès compte utilisateur personnel de l'utilisateur.

- **Cryptodevises et mining**.

  La sous-catégorie reprend les sites Internet qui proposent des services d'achat et de vente de cryptodevises et les services d'informations relatives aux cryptodevises et au mining.

D'un point de vue technique, le paiement peut être réalisé à l'aide de cartes bancaires de n'importe quel type (physique ou virtuelle, de débit ou de crédit, locales ou internationales) ou d'argent électronique. L'identification de cette catégorie de ressource Internet peut s'opérer à l'aide d'aspects techniques tels que le transfert de données via le protocole SSL, l'utilisation d'outils de vérification de l'identité comme "3D Secure", etc.

Recrutement

Cette catégorie reprend les ressources Internet qui permettent d'établir un contact entre un employeur et un chercheur d'emploi :

- Sites de chasseurs de têtes (agences de recrutement et/ou de sélection du personnel).
- Pages Internet d'employeurs qui contiennent les descriptions des postes vacants et leurs avantages.
- Portails indépendants contenant des offres d'emploi publiées par des employeurs et des chasseurs de tête.
- Réseaux sociaux à caractère professionnel qui permettent, notamment, de diffuser ou de rechercher des données sur des experts qui ne recherchent pas un travail activement.

Outils d'anonymisation

Cette catégorie reprend les ressources Internet qui jouent le rôle d'intermédiaire dans le téléchargement de contenu d'autres sites à l'aide d'application Web spéciales dans les buts suivants :

- Contournement des restrictions imposées par l'administrateur du réseau local sur l'accès aux adresses Internet ou IP.
- Accès anonyme à des ressources Internet, dont des ressources qui n'acceptent pas les requêtes HTTP en provenance de certaines adresses IP ou de certaines plages d'adresses (par exemple, en fonction du pays).

Cette catégorie reprend aussi bien les ressources Internet prévues exclusivement pour les objectifs décrits ci-dessus (anonymat) que les ressources Internet qui possèdent des fonctions similaires sur le plan technique.

Jeux

Cette catégorie reprend les ressources Internet consacrées aux jeux des genres es plus divers :

- Sites Internet de développeurs de jeux.
- Sites Internet de discussion sur les jeux.
- Ressources Internet permettant de jouer en ligne, avec d'autres joueurs ou seul, avec une application locale ou non (navigateur).
- Ressources Internet consacrées à la publicité, à la diffusion et au support d'un jeu en particulier.

Religions, associations religieuses

Cette catégorie reprend les ressources Internet dont le contenu traite des mouvements publics, des communautés et des organisations suivant une idéologie religieuse et/ou un culte quelconque :

- Sites Internet d'organisations religieuses officielles de différents niveaux, depuis les religions mondiales jusqu'aux communautés religieuses locales.
- Sites Internet d'organisations religieuses non enregistrées, nées d'une séparation du courant ou de la communauté religieuse dominants.
- Sites Internet de mouvements ou de communautés religieuses qui sont apparus indépendamment des courants/mouvement religieux traditionnels, notamment à l'initiative d'une personnalité concrète.
- Sites Internet d'organisations pluriconfessionnelles au service des relations entre les représentants des religions traditionnelles.
- Sites Internet au contenu scientifique, historique ou encyclopédique sur la religion.
- Ressources Internet contenant des illustrations/des descriptions détaillées de cultes religieux, dont les prières et les rituels liés à l'adoration d'un dieu, ainsi que des substances et/ou objets dotés de propriétés surnaturelles.

Médias d'actualités

Cette catégorie reprend les ressources Internet qui contiennent des informations publiques générées par les médias ou des éditeurs Internet qui visent à offrir des informations aux utilisateurs :

- Sites Internet officiels de médias.
- Sites Internet proposant des services d'informations tirés de sources officielles.
- Sites Internet d'agrégation de contenu, à savoir de rassemblement d'informations tirées de diverses sources officielles ou non.
- Sites Internet d'informations générées par les utilisateurs ("sites d'informations sociaux").

Bandeaux publicitaires

Cette catégorie reprend les ressources Internet avec des bannières. Les publicités peuvent vous distraire les utilisateurs et le chargement des bannières augmente le volume du trafic.

Restrictions régionales légales

Cette catégorie contient les sous-catégories suivantes :

- **Bloqué conformément aux dispositions de la législation de la Fédération de Russie**.

  Cette sous-catégorie reprend les ressources Internet interdites conformément à la législation de la Fédération de Russie.

- **Bloqué conformément aux dispositions de la législation belge**.

  Cette sous-catégorie reprend les ressources Internet interdites conformément à la législation belge.

- **Bloqué conformément aux dispositions de la législation japonaise**.

  Cette sous-catégorie reprend les ressources Internet interdites conformément à la législation japonaise.

A propos des règles d'accès aux sites Internet

Il est déconseillé de créer plus de 1 000 règles d'accès aux ressources Web car cela peut provoquer l'instabilité du système.

La règle d'accès aux ressources Internet est un ensemble de filtres et d'actions que Kaspersky Endpoint Security exécute lorsque les utilisateurs consultent les ressources Internet définies dans la règle à l'heure planifiée indiquée du fonctionnement de la règle. Les filtres permettent de préciser les sites Internet dont l'accès est contrôlé par le Contrôle Internet.

Les filtres suivants sont accessibles :

- **Filtrage selon le contenu**. Le Contrôle Internet organise les ressources Internet par catégories de contenu et par catégories de type de données. Vous pouvez contrôler l'accès des utilisateurs aux données hébergées sur les ressources Web qui sont liées aux données déterminées par ces catégories. Lorsque les utilisateurs consultent les sites Internet qui appartiennent à la catégorie de contenu sélectionnée et/ou à la catégorie de type de données sélectionnée, Kaspersky Endpoint Security exécute l'action indiquée dans la règle.

- **Filtrage selon les URL des ressources Internet**. Vous pouvez contrôler l'accès des utilisateurs à toutes les adresses des sites Internet ou à certaines adresses des sites Internet/ou à certains groupes d'adresses des sites Internet.

  Si le filtrage selon le contenu et le filtrage selon les URL des ressources Internet sont activés et les adresses des sites Internet définies et/ou les groupes d'adresses des sites Internet définis appartiennent aux catégories de contenu ou aux catégories de types de données sélectionnées, Kaspersky Endpoint Security ne contrôle pas l'accès à tous les sites Internet des catégories de contenu sélectionnées et/ou des catégories de types de données sélectionnées. Au lieu de cela, l'application contrôle uniquement l'accès aux adresses de ressources Internet et/ou à des groupes d'adresses de ressources Internet définis.

- **Filtrer par nom d'utilisateur et de groupe d'utilisateurs**. Vous pouvez définir les utilisateurs et/ou les groupes d'utilisateurs pour lesquels l'accès aux sites Internet est contrôlé conformément à la règle.

- **Planification de l'application de la règle**. Vous pouvez planifier l'application de la règle. La planification de l'application de la règle définit le moment où Kaspersky Endpoint Security contrôle l'accès aux ressources Internet indiquées dans la règle.

Après l'installation de l'application Kaspersky Endpoint Security la liste des règles du module Contrôle Internet n'est pas vide. Deux règles sont prédéfinies :

- La règle "Scripts et tables de styles" qui autorise tous les utilisateurs à accéder à tout moment à tous les sites dont l'URL contient des fichiers portant l'extension css, js, vbs. Par exemple, http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- "Règle par défaut". Cette règle, en fonction de l'action choisie, autorise ou interdit l'accès pour tous les utilisateurs à toutes les ressources Internet qui ne sont pas soumises à l'action d'autres règles.

Actions avec les règles d'accès aux sites Internet

Vous pouvez exécuter avec les règles d'accès aux sites Internet les actions suivantes :

- Ajouter une nouvelle règle.
- Modifier la règle.
- Définir la priorité de la règle.

  La priorité d'une règle dépend de la position de la ligne avec une brève description de la règle dans le tableau des règles d'accès de la fenêtre de configuration du module Contrôle Internet. En d'autres termes, la règle qui se trouve au-dessus des autres règles dans le tableau des règles d'accès a une priorité supérieure.

  Si le site Internet que l'utilisateur essaie d'accéder correspond aux paramètres de plusieurs règles, l'action de Kaspersky Endpoint Security sera définie par la règle avec une priorité plus élevée.
- Vérifier le fonctionnement de la règle.

  Vous pouvez vérifier la cohérence du fonctionnement des règles à l'aide du service "Diagnostic des règles".
- activer et désactiver la règle ;

  Une règle d'accès aux ressources Internet peut être activée (état de fonctionnement : *Activé*) ou désactivée (état de fonctionnement : *Désactivé*). Par défaut, après la création d'une règle, elle est activée (état de l'opération : *Activé*). Vous pouvez désactiver la règle.
- Supprimer la règle.

Ajout et modification de la règle d'accès aux sites Internet

Pour ajouter ou modifier la règle d'accès aux sites Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Pour modifier une règle, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
4. Définissez ou modifiez les paramètres de la règle. Pour ce faire, procédez comme suit :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom**.

   b. Sélectionnez l'option requise dans la liste déroulante **Filtrer le contenu** :

   - **Tout contenu**.
   - **Par catégories**.
   - **Par types de données**.

- **Par catégories et types de données**.

c. Si un élément autre que **Tout contenu** est sélectionné, les groupes de sélection des catégories de contenu et/ou des catégories de type de données s'ouvrent. Cochez les cases en regard des catégories de contenu et/ou des catégories de type de données souhaitées.

Si la case en regard du nom de la catégorie de contenu et/ou de la catégorie de type de données est cochée, Kaspersky Endpoint Security, conformément à la règle, contrôle l'accès aux sites Internet qui appartiennent aux catégories de contenu et/ou aux catégories de type de données sélectionnées.

d. Choisissez l'option requise dans la liste déroulante **Appliquer aux adresses** :

- **A toutes les adresses**.
- **A certaines adresses**.

e. Si l'élément **A certaines adresses** est sélectionné, le groupe pour créer la liste des adresses des sites Internet s'ouvre. Vous pouvez ajouter ou modifier des adresses et/ou des groupes d'adresses de sites Internet à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**.

Si l'Analyse des connexions chiffrées est désactivée, seul le filtrage selon le nom du serveur est accessible pour le protocole https.

f. Choisissez l'option requise dans la liste déroulante **Appliquer aux adresses** :

- **A tous les utilisateurs**.
- **A certains utilisateurs ou groupes**.

g. Si vous avez choisi l'option **A certains utilisateurs ou groupes**, la section dans laquelle vous pouvez créer la liste des utilisateurs et/ou groupes d'utilisateurs dont l'accès aux ressources Internet est décrit dans la règle est régi par cette règle. Vous pouvez ajouter ou supprimer des utilisateurs et/ou des groupes d'utilisateurs à l'aide des boutons **Ajouter**, **Supprimer**.

Le bouton **Ajouter** ouvre la fenêtre standard de Microsoft Windows **Sélection de l'utilisateur ou du groupe**.

h. Choisissez l'option requise dans la liste déroulante **Action** :

- **Autoriser** Si cette valeur est sélectionnée, Kaspersky Endpoint Security autorise l'accès aux ressources Internet conformes aux paramètres de la règle.
- **Interdire** Si cette valeur est sélectionnée, Kaspersky Endpoint Security interdit l'accès aux ressources Internet conformes aux paramètres de la règle.
- **Avertir**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security affiche un message d'avertissement qui indique que la visite de la ressource Internet est déconseillée lorsque l'utilisateur tente d'accéder à une ressource qui satisfait à la règle. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

i. Dans la liste déroulante **Planification de l'application de la règle**, sélectionnez le nom de la planification requise ou composez une nouvelle planification sur la base de la planification sélectionnée de fonctionnement de la règle. Pour ce faire, procédez comme suit :

1. Cliquez sur le bouton **Configuration** en regard de la liste déroulante **Planification de l'application de la règle**.

   La fenêtre **Planification de l'application de la règle** s'ouvre.

2. Pour ajouter à la planification de l'application de la règle un intervalle au cours duquel la règle n'est pas appliquée, sélectionnez d'un clic gauche les cellules du tableau qui correspondent aux heures et aux jours voulus de la semaine pour la planification de l'application de la règle.

   La couleur des cellules deviendra grise.

3. Pour modifier, dans la planification de l'application de la règle, l'intervalle au cours duquel la règle est appliquée en intervalle au cours duquel la règle n'est pas appliquée, sélectionnez d'un clic gauche les cellules grises du tableau correspondant aux heures et aux jours voulus de la semaine.

   La couleur des cellules deviendra verte.

4. Cliquez sur le bouton **Enregistrer sous**.

   La fenêtre **Nom de la planification de l'application de la règle** s'ouvre.

5. Saisissez le nom de la planification de l'application de la règle ou gardez le nom proposé par défaut.

6. Cliquez sur le bouton **OK**.

5. Dans la fenêtre **Règle d'accès aux sites Internet**, cliquez **OK**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Définition de la priorité des règles d'accès aux sites Internet

Vous pouvez définir la priorité de chaque règle dans la liste des règles en les structurant dans l'ordre spécifique.

Pour définir la priorité des règles d'accès aux sites Internet, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez la règle dont vous souhaitez modifier la priorité.

4. Déplacez la règle en position souhaitée dans la liste des règles à l'aide des boutons **Monter** et **Descendre**.

5. Répétez les paragraphes 3 et 4 de l'instruction pour les règles dont la priorité vous souhaitez modifier.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Vérification du fonctionnement des règles d'accès aux sites Internet

Pour évaluer la coordination des règles du Contrôle Internet, vous pouvez vérifier leur fonctionnement. Pour ce faire, le module Contrôle Internet prévoit la fonction "Diagnostic des règles".

Pour vérifier le fonctionnement des règles d'accès aux sites Internet, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Diagnostic**.

   La fenêtre **Diagnostic des règles** s'ouvre.

4. Remplissez les champs dans le groupe **Conditions** :

   a. Cochez la case **Indiquer l'adresse** pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à un site Internet spécifique. Saisissez l'adresse de la ressource Internet dans le champ ci-dessous.

   b. Définissez la liste des utilisateurs et / ou des groupes d'utilisateurs si vous voulez vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet pour des utilisateurs et / ou des groupes d'utilisateurs spécifiques.

   c. Sélectionnez dans la liste déroulante **Filtrer le contenu** l'élément requis (**Par catégories**, **Par types de données** ou **Par catégories et types de données**) pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet avec des catégories de contenu et/ou des catégories de type de données.

   d. Cochez la case **Tenir compte de l'heure de la tentative d'accès** si vous voulez vérifier le fonctionnement des règles en tenant compte du jour de la semaine et de l'heure des tentatives d'accès aux sites Internet indiqués dans les conditions du diagnostic des règles. Indiquez ensuite le jour de la semaine et l'heure.

5. Cliquez sur le bouton **Tester**.

A l'issue de l'analyse, un message sur l'action de Kaspersky Endpoint Security conformément à la première règle appliquée au moment de l'accès au site Internet défini (autorisation, interdiction, avertissement) sera affiché. La première règle appliquée est celle qui se trouve dans la liste des règles de Contrôle Internet au-dessus des autres règles conformes aux conditions du diagnostic. Le message est affiché à droite du bouton **Tester**. Le tableau en dessous affiche la liste des autres règles qui se sont déclenchées et le nom de l'action exécutée par Kaspersky Endpoint Security. Les règles sont classées par ordre de priorité décroissante.

Activation et désactivation de la règle d'accès aux sites Internet

Pour activer ou désactiver la règle d'accès aux sites Internet, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez la règle que vous souhaitez activer ou désactiver.

4. Dans la colonne **État**, procédez comme suit :

   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Actif*.

   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Désact*.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Migration des règles d'accès aux ressources Internet depuis des versions antérieures de l'application

Lors de la mise à niveau de la version Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou antérieure jusqu'à la version Kaspersky Endpoint Security 11.1.1 for Windows, les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu migrent selon les règles suivantes :

- Les règles d'accès aux ressources Internet qui reposent sur une ou plusieurs catégories de contenu de la liste "Chats et forums", "Emails en ligne", "Réseaux sociaux" reposent sur les catégories de contenu de "Communication sur Internet".
- Les règles d'accès aux ressources Internet qui reposent sur une ou plusieurs catégories de contenu de la liste "Boutiques en ligne" et "Systèmes de paiement" reposent sur les catégories de contenu "Magasins en ligne, banques, systèmes de paiement".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de ressources Interne "Jeux de hasard" reposent sur les catégories de contenu des ressources "Jeux de hasard, loterie, tirages au sort".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu "Jeux en ligne" reposent sur les catégories de contenu des ressources "Jeux".
- Les règles d'accès aux ressources Internet qui reposent sur les catégories de contenu qui ne figurent pas dans les catégories ci-dessus migrent sans aucune modification.

Exportation et importation de la liste des adresses de sites Internet

Si vous avez créé dans la règle d'accès aux sites Internet une liste des adresses des sites Internet, vous pouvez l'exporter dans un fichier au format TXT. Vous pouvez ensuite importer la liste depuis ce fichier pour ne pas créer manuellement la liste des adresses des sites Internet lors de la configuration de la règle. La fonction de l'exportation et de l'importation de la liste des adresses des sites Internet peut vous être utile si vous créez par exemple les règles aux paramètres similaires.

Pour exporter la liste des adresses des sites Internet dans un fichier, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez la règle dont la liste des adresses des sites Internet vous souhaitez exporter dans un fichier.
4. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
5. Pour exporter uniquement une partie de la liste des adresses des sites Internet, sélectionnez les adresses requises des sites Internet.
6. Cliquez sur le bouton  à droite du champ avec la liste des adresses des sites Internet.

   La fenêtre de confirmation de l'action s'ouvre.

7. Exécutez une des actions suivantes :

   - Pour exporter uniquement les éléments sélectionnés dans liste des adresses des sites Internet, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Oui**.

   - Pour exporter tous les éléments sélectionnés dans liste des adresses des sites Internet, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Non**.

     La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvre.

8. Dans la fenêtre de Microsoft Windows **Enregistrer sous**, sélectionnez le fichier où vous souhaitez exporter la liste des adresses des sites Internet. Cliquez sur le bouton **Enregistrer**.

Pour importer dans la règle la liste des adresses des sites Internet depuis un fichier, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** pour créer une nouvelle règle d'accès aux sites Internet.

   - Sélectionnez la règle d'accès aux sites Internet que vous souhaitez modifier. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.

4. Exécutez une des actions suivantes :

   - Pour créer une nouvelle règle d'accès aux sites Internet, sélectionnez dans la liste déroulante **Appliquer aux adresses** l'élément **A certaines adresses**.

   - Si vous modifiez la règle d'accès aux sites Internet, passez au paragraphe 5 de l'instruction.

5. Cliquez sur le bouton à droite du champ avec la liste des adresses des sites Internet.

   Si vous créez une nouvelle règle la fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

   Si vous modifiez la règle, la fenêtre de confirmation de l'action s'ouvre.

6. Exécutez une des actions suivantes :

   - Si vous créez une nouvelle règle d'accès aux sites Internet, passez au paragraphe 7 de l'instruction.

   - Si vous modifiez la règle d'accès aux sites Internet, dans la fenêtre de confirmation de l'action exécutez une des actions suivantes :

     - Pour ajouter aux éléments existants les éléments importés de la liste des adresses des sites Internet, cliquez sur le bouton **Oui**.

     - Pour supprimer les éléments existants de la liste des adresses des sites Internet et ajouter les éléments importés, cliquez sur le bouton **Non**.

   La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

7. Sélectionnez dans la fenêtre de Microsoft Windows **Ouvrir le fichier** le fichier avec la liste des adresses des sites Internet à importer.

8. Cliquez sur le bouton **Ouvrir**.

9. Dans la fenêtre **Règle d'accès aux sites Internet**, cliquez **OK**.

Règles de création de masques d'adresses de sites Internet

Le *masque d'adresse du site Internet* (ci-après également "masque d'adresse") peut vous être utile lorsque vous devez saisir une multitude d'adresses de sites Internet similaires lorsque vous créez une règle d'accès aux sites Internet. Un seul masque correct peut se substituer à une multitude d'adresses des sites Internet.

Pour créer un masque d'adresses, il faut respecter les règles suivantes :

1. Le caractère `*` remplace n'importe quelle séquence de caractères dont le nombre de caractères est zéro ou plus.

   Par exemple, lors de la saisie du masque d'adresse *abc* la règle d'accès aux sites Internet s'applique à toutes les adresses qui contiennent la séquence abc. Exemple : http://www.example.com/page_0-9abcdef.html.

   Pour ajouter le caractère `*` au masque d'une adresse, il convient de saisir `*` à deux reprises.

2. La suite de caractère `www.` au début du masque d'adresse est remplacée par `*.`

   Exemple : le masque d'adresse www.example.com est équivalent à *.example.com.

3. Si le masque d'adresse commence par un caractère autre que `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `*.`

4. La séquence des caractères `*.` au début du masque d'adresse est traitée comme `*.` ou comme la ligne vide.

   Exemple : le masque d'adresse http://www.*.example.com couvre l'adresse http://www2.example.com.

5. Si le masque d'adresses se termine par le caractère différent de `/` ou `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `/*`.

   Exemple : le masque d'adresse http://www.example.com couvre les adresses du type http://www.example.com/abc, où a, b, c représentent n'importe quels caractères.

6. Si le masque d'adresse se termine par le caractère `/`, le contenu du masque d'adresse est équivalent au même contenu avec le suffixe `*.`

7. La séquence des caractères `/*` à la fin du masque d'adresse est traitée comme `/*` ou comme la ligne vide.

8. La vérification des adresses des sites Internet par masque d'adresse est effectuée compte tenu du schéma (http ou https) :

   - S'il n'y a pas de protocole réseau dans le masque d'adresse, ce masque d'adresse couvre l'adresse avec n'importe quel protocole réseau.

     Exemple : le masque d'adresse example.com couvre les adresses http://example.com et https://example.com.

   - S'il y a un protocole réseau dans le masque d'adresse, ce masque d'adresse couvre uniquement les adresses avec le protocole réseau identique à celui du masque d'adresse.

     Exemple : le masque d'adresse http://*.example.com couvre l'adresse http://www.example.com et ne couvre pas l'adresse https://www.example.com.

9. Le masque d'adresse dans les guillemets doubles est interprété sans aucune permutation supplémentaire, sauf le caractère * s'il faisait partie du masque d'adresse d'origine. Les règles 5 et 7 ne s'appliquent pas aux masques d'adresses repris entre double guillemets (cf. exemples 14 à 18 dans le tableau ci-dessous).

10. Lors de la comparaison au masque d'adresse du site Internet ne sont pas pris en compte le nom d'utilisateur et le mot de passe, le port de connexion et le registre de caractères.

Exemples d'application des règles de création de masques d'adresses

N°	Masque d'adresse	Adresse du site Internet analysée	Est-ce que l'adresse analysée satisfait au masque d'adresse	Commentaires
1	*.example.com	http://www.123example.com	Non	Cf. règle 1.
2	*.example.com	http://www.123.example.com	Oui	Cf. règle 1.
3	*example.com	http://www.123example.com	Oui	Cf. règle 1.
4	*example.com	http://www.123.example.com	Oui	Cf. règle 1.
5	http://www.*.example.com	http://www.123example.com	Non	Cf. règle 1.
6	www.example.com	http://www.example.com	Oui	Cf. règles 2, 1.
7	www.example.com	https://www.example.com	Oui	Cf. règles 2, 1.
8	http://www.*.example.com	http://123.example.com	Oui	Cf. règles 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Oui	Cf. règles 2, 5, 1.
10	example.com	http://www.example.com	Oui	Cf. règles 3, 1.
11	http://example.com/	http://example.com/abc	Oui	Cf. règles 6.
12	http://example.com/*	http://example.com	Oui	Cf. règle 7.
13	http://example.com	https://example.com	Non	Cf. règle 8.
14	"example.com"	http://www.example.com	Non	Cf. règle 9.
15	"http://www.example.com"	http://www.example.com/abc	Non	Cf. règle 9.
16	"*.example.com"	http://www.example.com	Oui	Cf. règles 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Oui	Cf. règles 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Oui	Cf. règles 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Non	Le masque d'adresse contient plus d'informations que l'adresse du site Internet

Modification des modèles de messages du Contrôle Internet

En fonction de l'action définie dans les propriétés des règles du Contrôle Internet, lorsque les utilisateurs essaient d'accéder aux sites Internet, Kaspersky Endpoint Security affiche un message (en remplaçant la réponse du serveur HTTP par une page HTML avec le message) de l'un des types suivants :

- Message d'avertissement. Ce message avertit l'utilisateur que la visite de la ressource Internet est déconseillée et/ou ne correspond pas à la stratégie de sécurité de l'entreprise. Kaspersky Endpoint Security affiche le message d'avertissement si dans les paramètres de la règle qui décrit ce site Internet, l'option **Avertir** a été sélectionnée dans la liste déroulante **Action**.

  Si l'utilisateur pense recevoir ce message d'avertissement par erreur, il peut cliquer sur le lien dans le corps du message d'avertissement pour envoyer un message prérédigé destiné à l'administrateur du réseau local d'entreprise.

- Message de blocage du site Internet. Kaspersky Endpoint Security affiche le message de blocage du site Internet si l'option **Interdire** a été sélectionnée dans la liste déroulante **Action** des propriétés de la règle qui décrit ce site Internet.

  Si l'utilisateur considère que l'accès à la ressource Internet a été bloqué par erreur, il peut cliquer sur le lien dans le corps du message de blocage du site Internet pour envoyer un message prérédigé destiné à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message d'avertissement, de message sur le blocage de l'accès à un site Internet et de message destiné à l'administrateur du réseau local d'entreprise. Vous pouvez modifier leur contenu.

Pour modifier le modèle de message du Contrôle Internet, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.
4. Exécutez une des actions suivantes :

   - Si vous voulez modifier le modèle du message envoyé à l'utilisateur pour lui signaler que la visite de la ressource Internet est déconseillée, choisissez l'onglet **Avertissement**.
   - Si vous souhaitez modifier le modèle du message de blocage d'accès au site Internet, sélectionnez l'onglet **Blocage**.
   - Si vous souhaitez modifier le modèle du message pour l'administrateur, sélectionnez l'onglet **Message pour l'administrateur**.
5. Modifier le modèle de message. De plus vous pouvez utiliser la liste déroulante **Variable**, ainsi que les boutons **Par défaut** et **Lien** (le bouton n'est pas disponible sous l'onglet **Message pour l'administrateur**).
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle évolutif des anomalies

Cette section présente le Contrôle évolutif des anomalies et explique comment en configurer les paramètres.

A propos du Contrôle évolutif des anomalies

Le composant Contrôle évolutif des anomalies est disponible uniquement pour les produits Kaspersky Endpoint Security for Business Extended et Kaspersky Total Security for Business (pour en savoir plus sur les produits Kaspersky Endpoint Security for Business, consultez le site de Kaspersky).

Le module Contrôle évolutif des anomalies surveille et bloque les actions suspectes atypiques pour les ordinateurs du réseau de l'organisation. Le Contrôle évolutif des anomalies utilise un ensemble de règles (par exemple, la règle *Lancement de Windows PowerShell depuis une application de bureautique*) pour suivre les actions atypiques. Ces règles sont créées par les experts de Kaspersky sur la base des scénarios typiques d'action malveillantes. Vous pouvez choisir le comportement du Contrôle évolutif des anomalies pour chacune des règles et, par exemple, autoriser le lancement de scripts PowerShell pour automatiser l'exécution des tâches d'entreprise. Kaspersky Endpoint Security met à jour l'ensemble de règles à l'aide les bases de données de l'application. La mise à jour de l'ensemble de règles doit être confirmer manuellement.

Configuration du Contrôle évolutif des anomalies

La configuration du Contrôle évolutif des anomalies comprend les étapes suivantes :

1. Apprentissage du Contrôle évolutif des anomalies

   Une fois que le Contrôle évolutif des anomalies a été activé, les règles fonctionnent en *mode d'apprentissage*. Au cours de l'apprentissage, le Contrôle évolutif des anomalies surveille le déclenchement des règles et envoie les événements déclencheurs à Kaspersky Security Center. La durée du mode d'apprentissage est propre à chaque règle. Celle-ci est définie par les experts de Kaspersky. En règle générale, le mode d'apprentissage dure 2 semaines.

   Si une règle n'a jamais été déclenchée lors de l'apprentissage, le Contrôle évolutif des anomalies considère les actions associées à cette règle comme suspectes. Kaspersky Endpoint Security bloquera toutes les actions associées à cette règle.

   Si la règle c'est déclenchée lors de l'apprentissage, Kaspersky Endpoint Security enregistre les événements dans rapport sur les déclenchements des règles et dans le stockage **Fonctionnement des règles en mode d'apprentissage**.

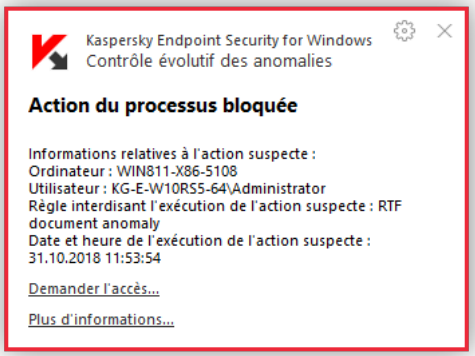
2. Analyse du rapport sur les déclenchements des règles

   L'administrateur analyse le rapport sur les déclenchements des règles ou le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Ensuite, l'administrateur peut sélectionner le comportement du Contrôle évolutif des anomalies lors du déclenchement d'une règle : bloquer ou autoriser. En outre, l'administrateur peut continuer à surveiller le déclenchement de la règle et prolonger le fonctionnement d'application en mode d'apprentissage. Si l'administrateur ne prend aucune mesure, l'application continuera également à fonctionner en mode d'apprentissage. Le décompte de la durée du mode d'apprentissage est remis à zéro.

La configuration du Contrôle évolutif des anomalies se déroule en temps réel. La configuration du Contrôle évolutif des anomalies se déroule de la manière suivante :

- Le Contrôle évolutif des anomalies commence automatiquement à bloquer les actions associées aux règles qui ne se sont pas déclenchées lors de l'apprentissage.
- Kaspersky Endpoint Security ajoute de nouvelles règles ou supprime les règles qui ne sont plus pertinentes.
- L'administrateur configure le fonctionnement du Contrôle évolutif des anomalies après avoir analysé le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Il est recommandé de vérifier le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**.

Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



Notification du Contrôle évolutif des anomalies

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Kaspersky Endpoint Security autorise ou non l'exécution d'une action associée à une règle selon l'algorithme suivant (cf. ill. ci-dessous).

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Activation et désactivation du Contrôle évolutif des anomalies

Le Contrôle évolutif des anomalies est activé par défaut. Le cas échéant, vous pouvez désactiver le Contrôle évolutif des anomalies.

Pour activer ou désactiver le Contrôle évolutif des anomalies, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Contrôle évolutif des anomalies** si vous voulez activer le Contrôle évolutif des anomalies.
   - Décochez la case **Contrôle évolutif des anomalies** si vous voulez désactiver le Contrôle évolutif des anomalies.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Action avec les règles du Contrôle évolutif des anomalies

Vous pouvez réaliser les opérations suivantes avec les règles du Contrôle évolutif des anomalies :

- modifier les paramètres d'une règle ;
- activer et désactiver la règle ;
- créer une exclusion pour une règle ;
- Importer et exporter les paramètres des règles ;
- appliquer des mises à jour pour une liste de règles.

Activation et désactivation d'une règle du Contrôle évolutif des anomalies

Pour activer ou désactiver une règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Dans le tableau de la partie droite de la fenêtre, sélectionnez une règle, puis réalisez une des opérations suivantes :
   - Dans la colonne **État**, cliquez-droit pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :
     - **Activé**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle évolutif des anomalies.
     - **Désactivée**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle évolutif des anomalies.
   - Cliquez sur le bouton **Modifier**.

     Dans la fenêtre **Règle du Contrôle évolutif des anomalies** :

     1. Dans le groupe **État de fonctionnement de la règle**, sélectionnez une des options suivantes :
        - **Activé**. Si vous avez choisi cette option, cette règle est utilisée pendant le fonctionnement du module Contrôle évolutif des anomalies.
        - **Désactivée**. Si vous avez choisi cette option, cette règle n'est pas utilisée pendant le fonctionnement du module Contrôle évolutif des anomalies.
     2. Dans la fenêtre **Règle du Contrôle évolutif des anomalies**, cliquez sur **OK**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action en cas de déclenchement d'une règle du Contrôle évolutif des anomalies

Pour modifier l'action en cas de déclenchement d'une règle du Contrôle évolutif des anomalies, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Dans le tableau de la partie droite de la fenêtre, sélectionnez une règle, puis réalisez une des opérations suivantes :

   - Dans la colonne **Action**, cliquez-droit pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :

     - **Intelligente**. Si vous choisissez cette option, la règle du Contrôle évolutif des anomalies fonctionne en mode d'apprentissage tout au long de la période définie par les experts de Kaspersky. Dans ce mode de fonctionnement de la règle du Contrôle évolutif des anomalies, Kaspersky Endpoint Security autorise toute activité qui tombe sous le coup de cette règle et crée un enregistrement dans le stockage **Fonctionnement des règles en mode d'apprentissage** du Serveur d'administration de Kaspersky Security Center. A l'issue de la période d'apprentissage, Kaspersky Endpoint Security bloque toute activité régie par une règle du Contrôle évolutif des anomalies et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

     - **Interdire**. Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security bloque l'activité qui tombe sous le coup de la règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

     - **Notifier**. Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security autorise l'activité qui tombe sous le coup de cette règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

   - Cliquez sur le bouton **Modifier**.

     Dans la fenêtre **Règle du Contrôle évolutif des anomalies** :

     1. Dans le groupe **Action lorsque la règle est déclenchée**, choisissez une des options suivantes :

        - **Intelligente**. Si vous choisissez cette option, la règle du Contrôle évolutif des anomalies fonctionne en mode d'apprentissage tout au long de la période définie par les experts de Kaspersky. Dans ce mode de fonctionnement de la règle du Contrôle évolutif des anomalies, Kaspersky Endpoint Security autorise toute activité qui tombe sous le coup de cette règle et crée un enregistrement dans le stockage **Fonctionnement des règles en mode d'apprentissage** du Serveur d'administration de Kaspersky Security Center. A l'issue de la période d'apprentissage, Kaspersky Endpoint Security bloque toute activité régie par une règle du Contrôle évolutif des anomalies et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

        - **Interdire**. Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security bloque l'activité qui tombe sous le coup de la règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

- **Notifier**. Si vous avez choisi cette option, quand une règle du Contrôle évolutif des anomalies se déclenche, Kaspersky Endpoint Security autorise l'activité qui tombe sous le coup de cette règle et crée dans le journal un enregistrement qui contient les informations relatives à cette activité.

2. Dans la fenêtre **Règle du Contrôle évolutif des anomalies**, cliquez sur **OK**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Création et modification d'une exclusion pour une règle du Contrôle évolutif des anomalies

Pour les règles du Contrôle évolutif des anomalies, il est impossible de créer plus de 1 000 exclusions. Il est déconseillé de créer plus de 200 exclusions. Pour diminuer la quantité d'exclusions utilisées, il est conseillé d'utiliser des masques dans les paramètres des exclusions.

L'exclusion pour la règle du Contrôle évolutif des anomalies contient une description des objets source et cible. *L'objet source* est l'objet qui exécute l'action. *L'objet cible* est l'objet qui subit l'action. Par exemple, vous avez ouvert le fichier `file.xlsx`. Par conséquent, un fichier de bibliothèque avec l'extension DLL est chargé dans la mémoire de l'ordinateur. Cette bibliothèque est utilisée par un navigateur (fichier exécutable intitulé `browser.exe`). Dans l'exemple donné, `file.xlsx` est l'objet source. Excel est le processus source, `browser.exe` est l'objet cible et Browser, le processus cible.

Pour créer ou modifier une exclusion pour une règle du Contrôle évolutif des anomalies, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.

3. Sélectionnez une règle dans le tableau de la partie droite de la fenêtre.

4. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle du Contrôle évolutif des anomalies** s'ouvre.

5. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une exclusion, cliquez sur le bouton **Ajouter**.

   - Pour modifier une exclusion existante, sélectionnez une ligne dans le tableau **Exclusions**, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Exclusion de la règle** s'ouvre.

6. Dans le champ **Description**, saisissez une description de l'exclusion.

7. Cliquez sur le bouton **Parcourir** à côté du champ **Utilisateur** pour indiquer les utilisateurs qui sont concernés par l'exclusion.

   La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

8. Définissez les paramètres de l'objet source ou du processus source lancés par l'objet :

- **Processus source**. Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, `C:\Dir\File.exe` ou `Dir\*.exe`).
- **Hash du processus source**. Hash du fichier.
- **Objet source**. Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, `C:\Dir\File.exe` ou `Dir\*.exe`). Par exemple, le chemin d'accès au fichier `document.docm` qui lance les processus cibles à l'aide d'un script ou d'une macro.

  Vous pouvez renseigner également d'autres objets pour l'exclusion, par exemple une adresse Internet, des macros, une commande de la ligne de commande, le chemin d'accès au registre, etc. Désignez l'objet selon le modèle suivant : `object://<objet>`, où `<objet>` désigne le nom de l'objet, par exemple, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Vous pouvez également utiliser des masques, par exemple, `object://*C:\Windows\temp\*`.
- **Hash de l'objet source**. Hash du fichier.

La règle du Contrôle évolutif des anomalies ne s'applique pas aux actions exécutées par l'objet, ni aux processus lancés par l'objet.

9. Définissez les paramètres de l'objet cible ou des processus cibles exécutés sur l'objet.
   - **Processus cible**. Le chemin ou le masque du chemin d'accès au fichier ou au dossier contenant les fichiers (par exemple, `C:\Dir\File.exe` ou `Dir\*.exe`).
   - **Hash du processus cible**. Hash du fichier.
   - **Objet cible**. Commande pour lancer le processus cible. Saisissez la commande selon le modèle suivant `object://<commande>`, par exemple, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Vous pouvez également utiliser des masques comme `object://*C:\windows\temp\*`.
   - **Hash de l'objet cible**. Hash du fichier.

   La règle du Contrôle évolutif des anomalies ne s'applique pas aux actions exécutées sur l'objet, ni sur processus exécutés sur l'objet.
10. Dans la fenêtre **Exclusion de la règle**, cliquez sur **OK**.
11. Dans la fenêtre **Règle du Contrôle évolutif des anomalies**, cliquez sur **OK**.
12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression d'une exclusion pour une règle du Contrôle évolutif des anomalies

Pour supprimer une exclusion pour une règle du Contrôle évolutif des anomalies, procédez comme suit, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.

3. Sélectionnez une règle dans le tableau de la partie droite de la fenêtre.
4. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle du Contrôle évolutif des anomalies** s'ouvre.
5. Dans le tableau **Exclusions de la règle**, choisissez la ligne nécessaire.
6. Cliquez sur le bouton **Supprimer**.
7. Dans la fenêtre **Règle du Contrôle évolutif des anomalies**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Importation des exclusions pour les règles du Contrôle évolutif des anomalies

Pour importer des exclusions pour les règles du Contrôle évolutif des anomalies, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Importer**.

   La fenêtre **Sélection du fichier de configuration** s'ouvre.
4. Dans la fenêtre **Sélection du fichier de configuration**, indiquez le nom du fichier au format XML depuis lequel vous souhaitez importer la liste des exclusions.
5. Cliquez sur le bouton **Ouvrir**.
6. Confirmez l'importation des exclusions en cliquant sur le bouton **Oui**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Exportation des exclusions pour les règles du Contrôle évolutif des anomalies

Pour exporter les exclusions pour les règles sélectionnées, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Dans le tableau dans la partie droite de la fenêtre, choisissez une ou plusieurs règles dont vous souhaitez exporter les exclusions.

4. Cliquez sur le bouton **Exporter**.

   La fenêtre **Sélection du fichier de configuration** s'ouvre.

5. Dans la fenêtre **Sélection du fichier de configuration**, procédez comme suit :

   a. Indiquez le nom du fichier, au format XML, dans lequel vous souhaitez exporter les exclusions.

   b. Choisissez le dossier dans lequel vous voulez enregistrer ce fichier.

   c. Cliquez sur le bouton **Enregistrer**.

6. Dans la boîte de dialogue qui s'ouvre, exécutez une des actions suivantes :

   - Cliquez sur le bouton **Oui** si vous voulez exporter les exclusions uniquement pour les règles sélectionnées.
   - Cliquez sur le bouton **Non** si vous voulez exporter les exclusions pour toutes les règles.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Application des mises à jour pour les règles du Contrôle évolutif des anomalies

De nouvelles règles du Contrôle évolutif des anomalies peuvent être ajoutées au tableau de règles et des règles existantes peuvent être supprimées du tableau suite à la mise à jour des bases antivirus. Kaspersky Endpoint Security met en évidence les règles du Contrôle évolutif des anomalies à supprimer ou à ajouter dans le tableau si la mise à jour n'a pas été appliquée à ces règles.

Tant que la mise à jour n'est pas appliquée, Kaspersky Endpoint Security affiche les règles du Contrôle évolutif des anomalies supprimées suite à la mise à jour dans le tableau des règles et leur attribue l'état *Désactivé*. Il est impossible de modifier les paramètres de ces règles. Kaspersky Endpoint Security affiche les règles ajoutées à la suite de la mise à jour du Contrôle évolutif des anomalies après que l'application de la mise à jour.

Pour appliquer les mises à jour aux règle du Contrôle évolutif des anomalies, procédez comme suit :

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

2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Confirmer les mises à jour**.

   Le bouton **Confirmer les mises à jour** est accessible si la mise à jour pour les règles du Contrôle évolutif des anomalies est disponible.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification des modèles de messages du Contrôle évolutif des anomalies

Quand l'utilisateur tente d'exécuter une action interdite par les règles de Contrôle évolutif des anomalies, Kaspersky Endpoint Security affiche un message sur le blocage des actions potentiellement dangereuses. Si l'utilisateur estime que le blocage n'a pas lieu d'être, il peut cliquer sur un lien dans la notification afin d'envoyer un message à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage des actions potentiellement dangereuses et pour les messages destinés à l'administrateur. Vous pouvez modifier les modèles de messages.

Pour modifier le modèle de message, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Contrôles de sécurité** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.
3. Cochez la case **Contrôle évolutif des anomalies** afin de pouvoir modifier les paramètres du module.
4. Cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles de messages** s'ouvre.
5. Exécutez une des actions suivantes :

   - Si vous souhaitez modifier le modèle de la notification relative au blocage des actions potentiellement dangereuses, choisissez l'onglet **Blocage**.
   - Pour modifier le modèle de message pour l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Message pour l'administrateur**.
6. Modifiez le modèle de message de blocage ou destiné à l'administrateur.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Consultation des rapports du Contrôle évolutif des anomalies

Pour consulter le rapport sur le fonctionnement du Contrôle évolutif des anomalies, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Contrôles de sécurité** ,choisissez la sous-section **Contrôle évolutif des anomalies**.

   Les paramètres du module Contrôle évolutif des anomalies apparaissent dans la partie droite de la fenêtre.

7. Exécutez une des actions suivantes :

   - Si vous voulez consulter le rapport sur les paramètres des règles du Contrôle évolutif des anomalies, cliquez sur le bouton **Rapport sur l'état des règles**.

   - Si vous voulez consulter le rapport sur les déclenchement des règles du Contrôle évolutif des anomalies, cliquez sur le bouton **Rapport sur les déclenchements des règles**.

8. Le processus de création du rapport est lancé.

   Le rapport s'ouvre dans une nouvelle fenêtre.

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

Cette section contient des informations sur la mise à jour des bases et des modules de l'application (ci-après mises à jour) et les instructions sur la configuration de la mise à jour.

A propos de la mise à jour des bases de données et des modules de l'application

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

Pour une mise à jour régulière, il faut une licence valide de l'application. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Les serveurs de mise à jour de Kaspersky sont la principale source de mise à jour pour Kaspersky Endpoint Security.

Pour réussir le téléchargement du paquet de mise à jour depuis les serveurs de mise à jour de Kaspersky, l'ordinateur doit être connecté à l'Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, il faudra configurer les paramètres du serveur proxy.

Le téléchargement des mises à jour s'opère selon le protocole HTTPS. Le téléchargement selon le protocole HTTP est possible quand le téléchargement des mises à jour selon le protocole HTTPS est impossible.

Lors de la mise à jour, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Les bases de Kaspersky Endpoint Security. La protection de l'ordinateur est garantie par l'utilisation de bases de données qui contiennent les signatures des virus et autres programmes présentant une menace ainsi que les informations sur les moyens de lutter contre elles. Ces informations sont utilisées par les modules de protection pour rechercher sur votre ordinateur les objets dangereux et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des menaces qui apparaissent et les moyens de lutter contre celles-ci. Pour cette raison, il est recommandé d'actualiser régulièrement les bases.

  En plus des bases de Kaspersky Endpoint Security, la mise à jour concerne également les pilotes réseau qui assurent l'interception du trafic réseau par les modules de protection.

- Modules de l'application. Outre les bases de Kaspersky Endpoint Security, il est possible d'actualiser les modules de l'application. Les mises à jour des modules de l'application permettent de supprimer les vulnérabilités de Kaspersky Endpoint Security, ajoutent de nouvelles fonctionnalités ou améliorent les fonctionnalités existantes.

Pendant la mise à jour, les bases et les modules de l'application installés sur votre ordinateur sont comparés à la dernière version stockée à la source des mises à jour. Si les bases et les modules de l'application actuels diffèrent de la dernière version, la partie manquante sera installée sur l'ordinateur.

La mise à jour des modules de l'application peut s'accompagner de la mise à jour de l'aide contextuelle de l'application.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Les informations sur l'état actuel des bases de Kaspersky Endpoint Security s'affichent dans le groupe **Mise à jour** de la fenêtre **Tâches**.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le rapport de Kaspersky Endpoint Security.

A propos des sources de mises à jour

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules de l'application de Kaspersky Endpoint Security.

La source des mises à jour peut être un serveur FTP, HTTP (par exemple, Kaspersky Security Center, les serveurs de mises à jour de Kaspersky), un dossier local ou de réseau.

Kaspersky Endpoint Security ne prend pas en charge le téléchargement de mises à jour à partir de serveurs HTTPS.

Configuration de la mise à jour

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres de la mise à jour :

- Ajouter de nouvelles sources des mises à jour.

  La liste des sources des mises à jour contient par défaut le serveur Kaspersky Security Center et les serveurs de mises à jour de Kaspersky. Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés.

  Si plusieurs ressources ont été sélectionnées en tant que sources des mises à jour, Kaspersky Endpoint Security les consultera pendant la mise à jour dans l'ordre de la liste et exécute la tâche de mise à jour en utilisant le paquet de mise à jour de la première source de mise à jour disponible.

  Si vous avez sélectionné en tant que source des mises à jour une ressource située hors de l'intranet, vous devrez être connecté à Internet pour effectuer la mise à jour.

- Sélectionnez la région du serveur de mises à jour de Kaspersky.

  Si vous utilisez les serveurs de Kaspersky en tant que source des mises à jour, vous pouvez sélectionner le serveur de mises à jour de Kaspersky pour télécharger le paquet de mise à jour en fonction de sa situation géographique. Serveurs de mise à jour de Kaspersky sont répartis dans plusieurs pays. En utilisant le serveur de mises à jour de Kaspersky le plus proche, vous pouvez réduire la durée nécessaire à la récupération des mises à jour.

  Par défaut, les paramètres de la mise à jour utilisent les informations géographiques reprises dans le registre du système d'exploitation.

- Configurer la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé.

  Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour de Kaspersky Endpoint Security sur les ordinateurs du réseau local d'entreprise depuis un dossier partagé. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère le dernier paquet de mise à jour depuis le serveur de Kaspersky Security Center ou les serveurs de mises à jour de Kaspersky et copie le paquet de mise à jour dans le dossier partagé. Après, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

- Sélectionner le mode d'exécution de la tâche de mise à jour.

  Si l'exécution de la tâche est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

  Vous pouvez reporter le lancement de la tâche de mise à jour par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche de mise à jour **Selon la planification** et l'heure de lancement de Kaspersky Endpoint Security est le même que l'heure programmée pour le lancement de la tâche de mise à jour. La tâche de mise à jour ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

- Configurer le lancement de la tâche de mise à jour avec les privilèges d'un autre utilisateur.

Ajout d'une source des mises à jour

Pour ajouter une source des mises à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Mode d'exécution et source des mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Source**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la source des mises à jour** s'ouvre.
5. Dans la fenêtre **Sélection de la source des mises à jour**, sélectionnez un dossier contenant le paquet de mise à jour ou saisissez le chemin complet du dossier dans le champ **Source**.
6. Cliquez sur le bouton **OK**.
7. Dans la fenêtre **Mise à jour**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection de la région du serveur de mises à jour

Pour choisir la région du serveur de mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Mode d'exécution et source des mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Source** dans le groupe **Paramètres régionaux**, sélectionnez **Sélectionner dans la liste**.
5. Sélectionnez dans la liste déroulante le pays le plus proche de vous.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la mise à jour depuis un dossier partagé

La configuration de la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé comprend les étapes suivantes :

1. Activation du mode de copie du paquet des mises à jour vers un dossier partagé sur un des ordinateurs du réseau local d'entreprise.
2. Configuration de la mise à jour de Kaspersky Endpoint Security de puis le dossier partagé indiqué sur les autres ordinateurs du réseau local d'entreprise.

Pour activer le mode de copie du paquet des mises à jour vers un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Avancé**, cochez la case **Copier les mises à jour dans le dossier**.
4. Saisissez le chemin d'accès au dossier partagé où sera stocké le paquet des mises à jour récupéré. Vous pouvez le faire d'une des manières suivantes :

   - Saisissez le chemin d'accès au dossier partagé dans le champ situé sous la case **Copier les mises à jour dans le dossier**.

- Cliquez sur le bouton **Parcourir**. Ensuite, sous la fenêtre **Sélection du dossier** qui s'ouvre, sélectionnez le dossier nécessaire et cliquez sur **OK**.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Pour configurer la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Mode d'exécution et source des mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Source**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la source des mises à jour** s'ouvre.
5. Dans la fenêtre **Sélection de la source des mises à jour**, sélectionnez le dossier partagé qui contient le paquet de mise à jour ou saisissez le chemin d'accès complet du dossier partagé dans le champ **Source**.
6. Cliquez sur le bouton **OK**.
7. Sous l'onglet **Source**, décochez les cases à côté des noms des sources de mise à jour que vous n'avez pas précisées comme étant le dossier partagé.
8. Cliquez sur le bouton **OK**.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection du mode de lancement de la tâche de mise à jour

Pour sélectionner le mode d'exécution de la tâche de mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Mise à jour** s'ouvre.
4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche de mise à jour :

   - Sélectionnez l'option **Automatique**, si vous souhaitez que Kaspersky Endpoint Security lance la tâche de mise à jour en fonction de la présence du paquet des mises à jour dans la source de mise à jour. L'intervalle de vérification de la présence du paquet des mises à jour par Kaspersky Endpoint Security est augmenté en cas d'épidémie et réduit en situation normale.

- Sélectionnez l'option **Manuelle** pour lancer la tâche de mise à jour manuellement.
- Sélectionnez l'option **Selon la planification** pour programmer l'exécution de la tâche de mise à jour.

5. Exécutez une des actions suivantes :
   - Si vous avez sélectionné l'option **Automatique** ou **Manuelle**, passez au paragraphe 6 de l'instruction.
   - Si vous avez sélectionné l'option **Selon la planification**, définissez les paramètres de planification du lancement de la tâche de mise à jour. Pour ce faire, procédez comme suit :
     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche de mise à jour. Sélectionnez une des options suivantes : **Minutes**, **Heures**, **Jours**, **Chaque semaine**, **A l'heure indiquée**, **Tous les mois**, **Après le lancement de l'application**.
     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche de mise à jour.
     c. Indiquez dans le champ **Reporter le lancement après le démarrage de l'application de** le temps qui doit s'écouler avant l'exécution de la tâche de mise à jour après le lancement de Kaspersky Endpoint Security.

        Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application**, le champ **Reporter le lancement après le démarrage de l'application de** est inaccessible.

     d. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches de mise à jour non exécutées en temps opportun.

        Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Heures**, **Minutes** ou **Après le lancement de l'application**, la case **Lancer les tâches non exécutées** est inaccessible.

6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement de la tâche de mise à jour avec les privilèges d'un autre utilisateur

Par défaut, la tâche de mise à jour de Kaspersky Endpoint Security est lancée au nom de l'utilisateur que vous avez utilisé pour ouvrir votre session dans le système d'exploitation. Cependant, la mise à jour de Kaspersky Endpoint Security peut se dérouler depuis une source à laquelle l'utilisateur n'a pas accès (par exemple, depuis un dossier partagé contenant le paquet des mises à jour) ou pour laquelle l'utilisation de l'authentification sur le serveur proxy n'a pas été configurée. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de Kaspersky Endpoint Security et lancer la tâche de mise à jour de Kaspersky Endpoint Security au nom de cet utilisateur.

Pour lancer une tâche de mise à jour sous les privilèges d'un autre utilisateur, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Mode d'exécution et source des mises à jour**, cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Mise à jour** s'ouvre.

4. Sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**.

5. Saisissez dans le champ **Nom** le compte utilisateur sous les privilèges duquel il faut accéder à la source des mises à jour.

6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur sous les privilèges duquel il faut accéder à la source des mises à jour.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la mise à jour des modules de l'application

Pour configurer la mise à jour des modules de l'application, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Avancé**, exécutez une des actions suivantes :

   - Cochez la case **Télécharger les mises à jour des modules de l'application** si vous souhaitez que l'application inclue la mise à jour des modules de l'application dans le paquet de mise à jour.

   - Dans le cas contraire, décochez la case **Télécharger les mises à jour des modules de l'application**.

4. Si vous avez coché la case **Télécharger les mises à jour des modules de l'application** à l'étape précédente, définissez les conditions dans lesquelles l'application installera les mises à jour des modules de l'application.

   - Choisissez l'option **Installer les mises à jour critiques et approuvées** si vous souhaitez que l'application installe les mises à jour critiques de l'application automatiquement, tandis que les autres mises à jour seront installées après confirmation de leur installation localement via l'interface de l'application ou via Kaspersky Security Center.

   - Choisissez l'option **Installer uniquement les mises à jour approuvées** si vous souhaitez que l'application installe les mises à jour des modules de l'application uniquement après approbation, localement via l'interface de l'application ou via Kaspersky Security Center.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement et arrêt des tâches

Quel que soit le mode d'exécution de la tâche de mise à jour sélectionné, vous pouvez lancer ou arrêter la tâche de mise à jour de Kaspersky Endpoint Security à tout moment.

Le téléchargement du paquet des mises à jour depuis les serveurs de mise à jour de Kaspersky requiert une connexion Internet.

Pour lancer ou arrêter la tâche de recherche de mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches** situé dans la partie inférieure de la fenêtre.

   La fenêtre **Tâches** s'ouvre.

2. Cliquez gauche pour sélectionner le groupe portant le nom de la tâche de mise à jour.

   Le groupe sélectionné se développe.

3. Exécutez une des actions suivantes :

   - Sélectionnez l'option **Démarrer** dans le menu pour lancer la tâche de mise à jour.

     L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche de mise à jour devient *En cours*.

   - Sélectionnez l'option **Arrêter** dans le menu pour arrêter la tâche de mise à jour.

     L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche de mise à jour devient *Arrêtée*.

Pour lancer ou arrêter la tâche de mise à jour lors de l'affichage de l'interface simplifiée de l'application, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :

   - Choisissez une tâche de mise à jour non-lancée pour la lancer.

   - Choisissez une tâche de mise à jour lancée pour l'arrêter.

   - Choisissez une tâche de mise à jour arrêtée pour la reprendre ou la relancer.

Annulation de la dernière mise à jour

Après la première mise à jour des bases et des modules de l'application, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour des bases et des modules de l'application.

Chaque fois que l'utilisateur lance la mise à jour, Kaspersky Endpoint Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Ceci permet de revenir, le cas échéant, à l'utilisation des bases et des modules de l'application antérieurs. La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sans danger.

Pour restaurer la dernière mise à jour, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches** situé dans la partie inférieure de la fenêtre.

   La fenêtre **Tâches** s'ouvre.

2. Cliquez gauche pour sélectionner le groupe portant le nom de la tâche de retour à l'état antérieur à la mise à jour.

   Le groupe sélectionné se développe.

3. Cliquez sur le bouton **Démarrer**.

   La tâche de retour à l'état antérieur à la mise à jour est lancée.

   L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche d'annulation de la mise à jour devient *En cours*.

Pour lancer ou arrêter la tâche d'annulation de la mise à jour en cas d'affichage de l'interface simplifiée de l'application, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :

   - Choisissez une tâche d'annulation de la mise à jour non-lancée pour la lancer.
   - Choisissez une tâche d'annulation de la mise à jour lancée pour l'arrêter.
   - Choisissez une tâche d'annulation de la mise à jour arrêtée pour la reprendre ou la relancer.

Configuration de l'utilisation du serveur proxy

Pour configurer les paramètres du serveur proxy, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Configuration**.

   La fenêtre **Paramètres du serveur proxy** s'ouvre.

   Vous pouvez également ouvrir la fenêtre **Paramètres du serveur proxy** dans la sous-section **Paramètres de l'application** de la section **Paramètres généraux** dans la fenêtre des paramètres de l'application.

4. Dans la fenêtre **Paramètres du serveur proxy**, cochez la case **Utiliser un serveur proxy**.

5. Choisissez une des options suivantes pour déterminer l'adresse du serveur proxy :

   - **Définir automatiquement les paramètres du serveur proxy**.

     Cette option est sélectionnée par défaut.

   - **Utiliser l'adresse et le port du serveur proxy indiqués**.

6. Si vous avez choisi l'option **Utiliser l'adresse et le port du serveur proxy indiqués**, définissez les valeurs dans les champs **Adresse** et **Port**.

7. Si vous voulez activer l'utilisation de l'authentification sur le serveur proxy, cochez la case **Définir le nom d'utilisateur et le mot de passe d'authentification** et indiquez les valeurs dans les champs suivants :

   - **Nom d'utilisateur**.

     Le champ de saisie du nom d'utilisateur qui est utilisé pour l'authentification sur le serveur proxy.

   - **Mot de passe**.

     Champ de saisie du mot de passe de l'utilisateur utilisé pour l'authentification sur le serveur proxy.

8. Si vous voulez désactiver l'utilisation du serveur proxy lors de la mise à jour de Kaspersky Endpoint Security à partir du dossier partagé, cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.

9. Cliquez sur le bouton **OK**.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse de l'ordinateur

La recherche de virus est un élément important dans la protection de l'ordinateur. Elle doit être réalisée régulièrement pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de protection en raison, par exemple, d'un niveau de sécurité faible ou pour toute autre raison.

Cette section présente les particularités et la configuration des tâches d'analyse, des niveaux de protection et des technologies d'analyse. Elle explique également comment manipuler les fichiers non traités par Kaspersky Endpoint Security lors de l'analyse.

A propos des tâches d'analyse

Lors de l'exécution des tâches d'analyse personnalisée ou complète, d'analyse des zones critiques, d'analyse depuis le menu contextuel ou d'analyse en arrière-plan, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive et ajoute au journal un enregistrement relatif à la non-analyse de ces fichiers.

Kaspersky Endpoint Security propose les tâches suivantes pour la recherche de virus et d'autres applications présentant une menace et pour la vérification de l'intégrité de ses modules :

Analyse complète

Analyse minutieuse de tout le système. Kaspersky Internet Endpoint analyse par défaut les objets suivants :

- mémoire du noyau ;
- Objets chargés au lancement du système d'exploitation
- secteurs d'amorçage ;
- Sauvegarde du système d'exploitation
- tous les disques durs et amovibles.

Pour économiser les ressources de l'ordinateur, il est conseillé de lancer la tâche d'analyse en arrière-plan au lieu de la tâche d'analyse complète. Le niveau de sécurité ne change pas.

Analyse des zones critiques

Par défaut, Kaspersky Endpoint Security analyse la mémoire du noyau, les processus lancés et les secteurs d'amorçage.

La tâche d'analyse complète et la tâche d'analyse rapide sont des tâches spécifiques. Pour ces tâches, il est déconseillé de modifier la zone d'analyse.

Analyse personnalisée

Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :

- Mémoire du noyau
- Objets chargés au lancement du système d'exploitation
- Sauvegarde du système d'exploitation
- Boîte aux lettres Outlook
- tous les disques durs, disques réseau et disques amovibles ;
- n'importe quel fichier sélectionné.

Analyse en arrière-plan

Kaspersky Endpoint Security analyse les objets de démarrage automatique, la mémoire du noyau et la partition du système. L'analyse en arrière-plan économise les ressources de l'ordinateur. Kaspersky Endpoint Security n'affiche aucune notification au lancement de l'Analyse en arrière-plan.

Vérification de l'intégrité

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

Une fois que les tâches d'analyse ont démarré, la progression des tâches s'affiche sous le nom de la tâche d'analyse en cours dans la fenêtre **Tâches**. Les informations relatives aux résultats de l'analyse et à tous les événements survenus pendant l'exécution des tâches d'analyse sont consignées dans le rapport de Kaspersky Endpoint Security.

Lancement et arrêt de la tâche d'analyse

Quel que soit le mode d'exécution de la tâche d'analyse sélectionné, vous pouvez lancer ou arrêter la tâche à tout moment.

Pour lancer ou arrêter la tâche d'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Tâches** situé dans la partie inférieure de la fenêtre.

   La fenêtre **Tâches** s'ouvre.

2. Cliquez gauche pour sélectionner le groupe portant le nom de la tâche d'analyse.

   Le groupe sélectionné se développe.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Démarrer** si vous voulez lancer la tâche d'analyse.

     L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche d'analyse devient *En cours*.

   - Sélectionnez l'option **Arrêter** dans le menu contextuel pour arrêter la tâche d'analyse.

     L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche d'analyse devient *Arrêtée*.

Pour lancer ou arrêter la tâche d'analyse lors de l'affichage de l'interface simplifiée de l'application, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.

2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :

   - Choisissez une tâche d'analyse non-lancée pour la lancer.

   - Choisissez une tâche d'analyse lancée pour l'arrêter.

   - Choisissez une tâche d'analyse arrêtée pour la reprendre ou la relancer.

Configuration des paramètres des tâches d'analyse

Pour configurer les paramètres des tâches d'analyse, vous pouvez exécuter les opérations suivantes :

- Modifier le niveau de sécurité.

  Vous pouvez sélectionner un des niveaux de sécurité prédéfinis ou personnaliser les paramètres du niveau de sécurité. Après avoir modifié les paramètres du niveau de sécurité, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de sécurité.

- Modifier l'action que Kaspersky Endpoint Security exécute en cas de détection d'un fichier infecté.

- Créer la zone d'analyse.

  Vous pouvez élargir ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets d'analyse ou en modifiant le type de fichiers à analyser.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. Vous pouvez également réduire la période d'analyse d'un fichier. A l'issue du temps défini, Kaspersky Endpoint Security exclut le fichier de l'analyse en cours (sauf les archives et les objets qui incluent plusieurs fichiers).

  Vous pouvez aussi activer les technologies iChecker et iSwift. Les technologies iChecker et iSwift permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

- Configurer l'analyse des fichiers composés.

- Configurer les méthodes d'analyse.

  Pendant qu'elle fonctionne, l'application Kaspersky Endpoint Security utilise la méthode d'analyse Machine learning et l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Endpoint Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky, Machine learning et l'analyse sur la base de signatures sont toujours activés.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des objets dans le système d'exploitation. L'analyse heuristique permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases Kaspersky Endpoint Security.

- Sélectionner le mode d'exécution des tâches d'analyse.

  Si l'exécution de la tâche d'analyse est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche d'analyse ignorée dès que cela est possible.

  Vous pouvez reporter le lancement de la tâche d'analyse par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche d'analyse **Selon la planification** et l'heure de lancement de Kaspersky Endpoint Security est le même que l'heure programmée pour le lancement de la tâche d'analyse. La tâche d'analyse ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

- Configurer le lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur.

- Configurer les paramètres d'analyse des disques amovibles à la connexion.

Modification du niveau de sécurité

Kaspersky Endpoint Security utilise différents ensembles de paramètres pour exécuter les tâches d'analyse. Les ensembles de paramètres enregistrés dans l'application sont dénommés *niveaux de sécurité*. Il existe trois niveaux prédéfinis de sécurité : **Élevé**, **Recommandé**, **Faible**. Les paramètres du niveau de sécurité **Recommandé** sont les paramètres optimaux. Ils sont recommandés par les spécialistes de Kaspersky.

Afin de modifier le niveau de sécurité, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise (**Analyse complète**, **Analyse des zones critiques** ou **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de sécurité**, exécutez une des actions suivantes :

   - Pour appliquer un des niveaux prédéfinis de sécurité (**Élevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de sécurité, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre portant le nom de la tâche d'analyse qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de sécurité, le nom du niveau de sécurité des fichiers dans le groupe **Niveau de sécurité** devient **Autre**.
   - Pour sélectionner le niveau de sécurité **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'action sur les fichiers infectés

Par défaut, en cas de détection de fichiers infectés, Kaspersky Endpoint Security tente de les désinfecter ou les supprime, si la désinfection est impossible.

Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Action en cas de détection d'une menace**, choisissez une des options suivantes :

   - Cochez la case **Désinfecter ; supprimer si la désinfection est impossible** si vous voulez que Kaspersky Endpoint Security tente de désinfecter les fichiers infectés détectés et les supprime si la désinfection est impossible.
   - Cochez la case **Désinfecter ; informer si la désinfection est impossible** si vous voulez que Kaspersky Endpoint Security tente de désinfecter les fichiers infectés détectés et vous informe si la désinfection est impossible.

- Cochez la case **Notifier** si vous voulez que Kaspersky Endpoint Security vous signale la détection de fichiers infectés.

En cas de détection de fichiers infectés qui appartiennent à une application de Windows Store, Kaspersky Endpoint Security exécute l'action **Supprimer**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition de la liste des objets à analyser

Pour composer une liste des objets à analyser, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Zone d'analyse**.

   La fenêtre **Zone d'analyse** s'ouvre.
4. Si vous voulez ajouter un nouvel objet à la zone d'analyse, procédez comme suit :

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

      La fenêtre **Sélection de la zone d'analyse** s'ouvre.

   b. Choisissez l'objet et cliquez sur le bouton **Ajouter**.

      Tous les objets sélectionnés dans la fenêtre **Sélection de la zone d'analyse** seront affichés dans la liste **Zone d'analyse**.

   c. Cliquez sur le bouton **OK**.
5. Si vous voulez modifier le chemin d'accès à l'objet de la zone d'analyse, procédez comme suit :

   a. Choisissez l'objet dans la zone d'analyse.

   b. Cliquez sur le bouton **Modifier**.

      La fenêtre **Sélection de la zone d'analyse** s'ouvre.

   c. Introduisez le nouveau chemin d'accès à l'objet de la zone d'analyse.

   d. Cliquez sur le bouton **OK**.
6. Si vous voulez supprimer un objet de la zone d'analyse, procédez comme suit :

   a. Choisissez l'objet que vous voulez supprimer de la zone d'analyse.

      Pour sélectionner plusieurs objets, choisissez-les en maintenant la touche **CTRL** enfoncée.

b. Cliquez sur le bouton **Supprimer**.

La fenêtre de confirmation de suppression s'ouvre.

c. Cliquez sur le bouton **Oui** dans la fenêtre de confirmation de la suppression.

Vous ne pouvez pas supprimer ou modifier les objets repris par défaut dans la zone d'analyse.

7. Pour exclure un objet de la zone d'analyse, décochez la case en regard de l'objet dans la fenêtre **Zone d'analyse**.

Cet objet ne sera pas analysé pendant l'exécution de la tâche d'analyse tout en restant dans la liste des objets de la zone d'analyse.

8. Cliquez sur le bouton **OK**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection du type de fichiers à analyser

Pour sélectionner les types d'objets à analyser, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre avec le nom de la tâche d'analyse sélectionnée, sélectionnez l'onglet **Zone d'action**.

5. Sélectionnez dans le groupe **Types de fichiers** le type de fichiers que vous souhaitez analyser pendant l'exécution de la tâche d'analyse :

- Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
- Sélectionnez **Fichiers analysés par format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
- Sélectionnez **Fichiers analysés par extension** si vous souhaitez analyser les fichiers dont les extensions sont caractéristiques des fichiers les plus exposés à l'infection.

Au moment de choisir le type d'objet à analyser, il convient de tenir compte des éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est faible. Mais il existe également des formats de fichiers qui contiennent un code exécutable (par exemple, les formats EXE, DLL) ou qui pourraient en contenir (par exemple, le format DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.
- Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné

l'analyse des fichiers selon l'extension, l'application ignorera ce fichier lors de l'analyse. Si l'analyse des fichiers selon le format a été sélectionnée, le module Protection contre les fichiers malicieux analyse les en-têtes de fichier quelle que soit l'extension. S'il s'avère que le fichier possède un format de fichier exécutable (par exemple, EXE), l'application l'analyse.

6. Dans la fenêtre avec le nom de la tâche d'analyse, cliquez sur **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Optimisation de l'analyse des fichiers

Pour optimiser l'analyse des fichiers, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Zone d'action**.

5. Dans le groupe **Optimisation de l'analyse**, procédez comme suit :

   - Cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

   - Cochez la case **Ignorer les fichiers si l'analyse dure plus de** et définissez la durée d'analyse d'un fichier (en secondes).

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des fichiers composés

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour identifier les virus et autres programmes présentant une menace dissimulés de cette façon, il faut décompresser le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limiter les types de fichiers composés à analyser pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise (**Analyse complète**, **Analyse des zones critiques** ou **Analyse personnalisée**).

Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Zone d'action**.

5. Sélectionnez dans le groupe **Analyse des fichiers composés** les fichiers composés à analyser : archives, paquets d'installation, fichiers aux formats Office, fichiers au format de messagerie ou fichiers protégés par un mot de passe.

6. Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée dans le groupe **Optimisation de l'analyse**, cliquez sur le lien **tous/ nouveaux** situé à côté du nom du type de fichier composé pour décider s'il faut analyser ou non tous les fichiers de ce type ou uniquement les nouveaux fichiers.

   La valeur du lien change quand vous cliquez dessus.

   Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée, l'application analyse uniquement les nouveaux fichiers.

7. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

8. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Si vous ne souhaitez pas décompresser les fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

   - Si vous souhaitez décompresser les fichiers composés quelle que soit leur taille, décochez la case **Ne pas décompresser les fichiers composés de grande taille**.

   Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

9. Cliquez sur le bouton **OK**.

10. Dans la fenêtre contenant le nom de la tâche d'analyse, cliquez sur **OK**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des méthodes d'analyse

Pour utiliser les méthodes d'analyse, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

5. Dans le groupe **Méthodes d'analyse**, cochez la case Analyse heuristique, si vous souhaitez que l'application utilise l'analyse heuristique pendant l'exécution de la tâche d'analyse. Ensuite, définissez le niveau de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des technologies d'analyse

Pour utiliser des technologies d'analyse, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse des zones critiques**, **Analyse personnalisée**, **Analyse depuis le menu contextuel**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

5. Dans le groupe **Technologies d'analyse**, cochez les cases à côté des noms des technologies que vous souhaitez utiliser pendant l'analyse.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Sélection du mode de lancement de la tâche d'analyse

Pour sélectionner le mode d'exécution de la tâche d'analyse, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse correspondante : **Analyse complète**, **Analyse des zones critiques** ou **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Mode d'exécution**.

   La fenêtre des propriétés de la tâche sélectionnée s'ouvre à l'onglet **Mode d'exécution**.

4. Dans le groupe **Mode d'exécution**, sélectionnez le mode d'exécution de la tâche : **Manuelle** ou **Selon la planification**.

5. Si vous avez sélectionné l'option **Selon la planification**, définissez les paramètres de planification. Pour ce faire, procédez comme suit :

   a. Dans la liste déroulante **Fréquence**, sélectionnez la fréquence de lancement de la tâche (**Minutes**, **Heures**, **Jours**, **Chaque semaine**, **A l'heure indiquée**, **Tous les mois**, **Après le lancement de l'application**, **Après chaque mise à jour**).

   b. En fonction de la fréquence sélectionnée, configurez les paramètres complémentaires afin d'affiner la planification du lancement de la tâche.

   c. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches d'analyse non exécutées en temps opportun.

   > Si dans la liste déroulante **Fréquence** l'élément **Minutes**, **Heures**, **Après le lancement de l'application** ou **Après chaque mise à jour** est sélectionné, la case **Lancer les tâches non exécutées** est inaccessible.

   a. Cochez la case **Exécuter lorsque l'ordinateur celui-ci est inactif** si vous voulez que Kaspersky Endpoint Security suspende la tâche quand les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security démarre la tâche d'analyse si l'ordinateur est verrouillé.

   Cette option de planification permet d'économiser la puissance de calcul de l'ordinateur pendant l'utilisation de celui-ci.

6. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration du lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur

Par défaut, la tâche d'analyse est lancée avec les privilèges du compte utilisateur employé pour ouvrir la session dans le système d'exploitation. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche d'analyse sous les privilèges d'un autre utilisateur. Vous pouvez indiquer l'utilisateur bénéficiant de ces privilèges, dans les paramètres de la tâche d'analyse et lancer la tâche d'analyse au nom de cet utilisateur.

Pour configurer le lancement de la tâche d'analyse avec les privilèges d'un autre utilisateur, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section qui porte le nom de la tâche d'analyse correspondante : **Analyse complète**, **Analyse des zones critiques** ou **Analyse personnalisée**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Mode d'exécution**.

   La fenêtre des propriétés de la tâche sélectionnée s'ouvre à l'onglet **Mode d'exécution**.

4. Sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**.

5. Saisissez dans le champ **Nom** le nom d'utilisateur dont vous souhaitez utiliser les privilèges pour lancer la tâche d'analyse.

6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur dont vous souhaitez utiliser les privilèges pour lancer la tâche d'analyse.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse des disques amovibles lors de leur connexion à l'ordinateur

Certains programmes malveillants exploitent des vulnérabilités du système d'exploitation pour se propager via les réseaux locaux et les disques amovibles. Kaspersky Endpoint Security prend en charge la recherche de virus et d'autres programmes présentant une menace sur les disques amovibles lors de leur connexion à l'ordinateur.

Pour configurer l'analyse des disques amovibles lors de leur connexion à l'ordinateur, procédez comme suit :

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

2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Analyse des disques amovibles**.

   Les paramètres d'analyse des disques amovibles s'affichent dans la partie droite de la fenêtre.

3. Dans la liste déroulante **Action à exécuter lors de la connexion d'un disque amovible** choisissez l'action nécessaire :

   - **Ne pas analyser**

   - **Analyse approfondie**

     Dans ce mode, Kaspersky Endpoint Security analyse tous les fichiers situés sur le disque amovible, y compris les fichiers joints à l'intérieur des objets composés.

   - **Analyse rapide**

     Dans ce mode Kaspersky Endpoint Security analyse uniquement les fichiers infectables et il ne décompacte pas les objets composés.

4. Exécutez une des actions suivantes :

   - Si vous souhaitez que Kaspersky Endpoint Security analyse uniquement les disques amovibles dont la taille ne dépasse pas la valeur indiquée, cochez la case **Taille maximale du disque amovible**, puis définissez la valeur en mégaoctets dans le champ à côté.

   - Si vous souhaitez que Kaspersky Endpoint Security analyse tous les disques amovibles, décochez la case **Taille maximale du disque amovible**.

5. Exécutez une des actions suivantes :

   - Si vous souhaitez que l'application Kaspersky Endpoint Security affiche l'état d'avancement de l'analyse des disques amovibles dans une nouvelle fenêtre, cochez la case **Afficher la progression de l'analyse**.

Exécutez une des actions suivantes :

- Si vous souhaitez que Kaspersky Endpoint Security interdise l'arrêt d'une tâche d'analyse des disques amovibles, cochez la case **Interdire l'arrêt de la tâche d'analyse**.
- Si vous souhaitez que la tâche d'analyse des disques amovibles puisse être arrêtée, décochez la case **Interdire l'arrêt de la tâche d'analyse**.

- Si vous souhaitez que l'application Kaspersky Endpoint Security lance l'analyse des disques amovibles en arrière-plan, décochez la case **Afficher la progression de l'analyse**.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage automatique, la mémoire du noyau et la partition du système. L'Analyse en arrière-plan est lancée dans les cas suivants :

- après la mise à jour des bases antivirus ;
- trente minutes après le lancement de Kaspersky Endpoint Security ;
- toutes les six heures ;
- quand un ordinateur est inactif pendant cinq minutes ou plus.

L'analyse en arrière-plan réalisée quand l'ordinateur est en veille est interrompue lorsque l'une des conditions suivantes est remplie :

- L'ordinateur est réactivé.

  Si l'analyse en arrière-plan n'a pas été réalisée depuis plus de dix jours, l'analyse n'est pas interrompue.

- L'ordinateur (ordinateur portable) est passé en mode batterie.

Lors de l'analyse en arrière-plan, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.

Pour désactiver l'analyse en arrière-plan de l'ordinateur, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la sous-section **Analyse en arrière-plan**.

   Les paramètres de l'analyse en arrière-plan s'afficheront dans la partie droite de la fenêtre.
3. Cochez la case **Activer l'analyse de l'ordinateur lorsque celui-ci est inactif**.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Manipulation des menaces actives

Cette section explique comment manipuler les fichiers infectés que Kaspersky Endpoint Security n'a pas traité lors de la recherche d'éventuels de virus et autres programmes dangereux sur l'ordinateur.

A propos des menaces actives

L'application Kaspersky Endpoint Security consigne les informations relatives aux fichiers qu'elle n'a pas traités pour une raison quelconque. Ces informations se présentent sous la forme d'événements dans la liste des menaces actives.

Un fichier infecté est considéré comme *traité* si Kaspersky Endpoint Security, lors de la recherche de la présence éventuelle de virus et autres programmes dangereux, a réalisé une des opérations suivantes sur ce fichier conformément aux paramètres définis de l'application :

- Réparer.
- Supprimer.
- Supprimer si la désinfection est impossible.

Kaspersky Endpoint Security place le fichier dans la liste des menaces actives si, pour une raison quelconque, il n'a pas terminé l'action sur ce fichier conformément à la configuration de l'application lors de la recherche de virus et programmes dangereux sur l'ordinateur.

Cette situation peut se présenter dans les cas suivants :

- Le fichier à analyser n'est pas accessible (par exemple, il se trouve sur un disque réseau ou sur un support externe sans droit en écriture).
- Dans le groupe **Action en cas de détection d'une menace** des paramètres de l'application pour les tâches, l'action **Notifier** a été sélectionnée et lorsque le message relatif au message infecté s'est affiché, l'utilisateur a choisi l'option **Ignorer**.

Vous pouvez exécuter une des actions suivantes :

- Lancer manuellement la tâche d'analyse personnalisée de fichiers depuis la liste des menaces actives après la mise à jour des bases et des modules de l'application. L'état des fichiers peut changer après l'analyse.
- Supprimer des enregistrements de la liste des menaces actives.

Utilisation de la liste des menaces actives

La liste des menaces actives est présentée sous la forme d'un tableau des événements liés aux fichiers infectés qui n'ont pas été traités pour une raison quelconque.

Vous pouvez exécuter les actions suivantes sur les fichiers de la liste des menaces actives :

- consulter la liste des menaces actives ;
- analyser au départ de la liste des menaces actives à l'aide de la version actuelle des bases et des modules de Kaspersky Endpoint Security ;
- restaurer des fichiers de la liste des menaces actives vers leurs dossiers d'origine ou vers n'importe quel autre dossier (si le dossier d'origine du fichier n'est pas accessible en écriture) ;
- supprimer des fichiers de la liste des menaces actives ;
- ouvrir le dossier où se trouvait au départ le fichier de la liste des menaces actives.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer les menaces actives selon les valeurs des colonnes ou à l'aide de filtres complexes ;
- utiliser la fonction de recherche de menaces actives ;
- trier les menaces actives ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des menaces actives ;
- regrouper les menaces actives.

Le cas échéant, vous pouvez copier les informations relatives aux menaces actives sélectionnées dans le Presse-papiers.

Lancement de la tâche d'analyse personnalisée des fichiers de la liste des menaces actives

Vous pouvez lancer manuellement la tâche d'analyse personnalisée des fichiers infectés qui n'ont pas été traités pour une raison quelconque. Vous pouvez lancer l'analyse si, par exemple, la dernière analyse avait été interrompue pour une raison quelconque ou si vous souhaitez analyser à nouveau les fichiers de la liste des menaces actives après la dernière mise à jour régulière des bases de données et des modules de l'application.

Pour lancer une tâche d'analyse personnalisée des fichiers de la liste des menaces actives, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le groupe **<...> menaces actives**.

   La fenêtre **Menaces actives** s'ouvre.

2. Dans le tableau de la fenêtre **Menaces actives**, sélectionnez un ou plusieurs enregistrements relatifs aux fichiers que vous souhaitez analyser.

   Pour sélectionner plusieurs enregistrements, choisissez-les en maintenant la touche **CTRL** enfoncée.

3. Lancez la tâche d'analyse personnalisée des fichiers d'une des manières suivantes :

   - Cliquez sur le bouton **Nouvelle analyse**.
   - Ouvrez le menu contextuel d'un clic droit de la souris et sélectionnez l'option **Nouvelle analyse**.

Suppression des enregistrements dans la liste des menaces actives

Pour supprimer un enregistrement de la liste des menaces actives, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le groupe **<...> menaces actives**.

   La fenêtre **Menaces actives** s'ouvre.

2. Dans le tableau dans la fenêtre **Menaces actives**, sélectionnez un ou plusieurs enregistrements que vous voulez supprimer de la liste des menaces actives.

   Pour sélectionner plusieurs enregistrements, choisissez-les en maintenant la touche **CTRL** enfoncée.

3. Supprimez les enregistrements à l'aide d'un des moyens suivants :

   - Cliquez sur le bouton **Supprimer**.
   - Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer**.

Vérification de l'intégrité des modules de l'application.

Cette section contient des informations sur les particularités et la configuration de la tâche de vérification de l'intégrité.

A propos de la tâche de vérification de l'intégrité

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

Après le lancement de la tâche de vérification de l'intégrité, l'état d'avancement de celle-ci s'affiche sur la ligne qui apparaît sous le nom de la tâche dans la fenêtre **Tâches**.

Les informations relatives à l'exécution de la tâche de vérification de l'intégrité sont consignées dans les rapports.

Lancement et arrêt de la tâche de vérification de l'intégrité

Quel que soit le mode d'exécution sélectionné, vous pouvez lancer ou arrêter la tâche de vérification de l'intégrité à tout moment.

Pour lancer ou arrêter la tâche de vérification de l'intégrité, procédez comme suit :

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

   La fenêtre **Tâches** s'ouvre.

2. Cliquez gauche pour sélectionner le groupe portant le nom de la tâche de vérification de l'intégrité.

   Le groupe sélectionné se développe.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Démarrer** si vous voulez lancer la tâche de vérification de l'intégrité.

L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche de vérification de l'intégrité devient *En cours*.

- Sélectionnez l'option **Arrêter** dans le menu contextuel pour arrêter la tâche de vérification de l'intégrité.

  L'état de l'exécution de la tâche qui apparaît sous le nom de la tâche de vérification de l'intégrité devient *Arrêtée*.

Pour lancer ou arrêter la tâche de vérification de l'intégrité lors de l'affichage de l'interface simplifiée de l'application, procédez comme suit :

1. Cliquez-droit pour ouvrir le menu contextuel de l'icône de l'application située dans la zone de notification de la barre des tâches.
2. Dans la liste déroulante **Tâches** du menu contextuel, exécutez une des actions suivantes :
   - Choisissez une tâche de vérification de l'intégrité non-lancée pour la lancer.
   - Choisissez une tâche de vérification de l'intégrité lancée pour l'arrêter.
   - Choisissez une tâche de vérification de l'intégrité arrêtée pour la reprendre ou la relancer.

Sélection du mode de lancement de la tâche de vérification de l'intégrité

Pour sélectionner le mode d'exécution de la tâche de vérification de l'intégrité, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Tâches** qui se trouve dans la partie gauche de la fenêtre, sélectionnez **Vérification de l'intégrité**.

   Les paramètres de la tâche de vérification de l'intégrité s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Mode d'exécution**, choisissez une des options suivantes :
   - Sélectionnez l'option **Manuelle** pour lancer la tâche de vérification de l'intégrité manuellement.
   - Sélectionnez l'option **Selon la planification**, pour programmer l'exécution de la tâche de vérification de l'intégrité.
4. Si vous avez sélectionné l'option **Selon la planification** à l'étape précédente, définissez les paramètres de planification du lancement de la tâche de vérification. Pour ce faire, procédez comme suit :
   a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche de vérification de l'intégrité. Sélectionnez une des options suivantes : **Minutes**, **Heures**, **Jours**, **Chaque semaine**, **A l'heure indiquée**, **Tous les mois**, **Après le lancement de l'application**.
   b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche de vérification de l'intégrité.
   c. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches de vérification de l'intégrité non exécutées en temps opportun.

Si dans la liste déroulante **Fréquence** l'option **Après le lancement de l'application**, **Minutes** ou **Heures** a été sélectionnée, la case **Lancer les tâches non exécutées** est inaccessible.

d. Cochez la case **Exécuter lorsque l'ordinateur celui-ci est inactif** si vous voulez que Kaspersky Endpoint Security suspende la tâche quand les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security démarre la tâche d'analyse si l'ordinateur est verrouillé.

Cette option de planification permet d'économiser la puissance de calcul de l'ordinateur pendant l'utilisation de celui-ci.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation des rapports

Cette section explique comment utiliser les rapports et en configurer les paramètres.

A propos des rapports

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'exécution de chaque tâche d'analyse, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans des rapports.

Les rapports se trouvent dans le dossier ProgramData\Kaspersky Lab\KES\Report.

Les rapports peuvent contenir les données suivantes de l'utilisateur :

- chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;
- chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
- nom d'utilisateur Microsoft Windows ;
- adresses des pages Web ouvertes par l'utilisateur.

Les données du rapport se présentent sous la forme d'un tableau qui reprend la liste des événements. Chaque ligne du tableau contient des informations sur un événement distinct. Les attributs des événements sont situés dans les colonnes du tableau. Certaines colonnes sont complexes et contiennent des sous-colonnes avec des attributs complémentaires. Pour consulter les attributs supplémentaires, vous devez appuyer sur le bouton ⊞ situé à côté du nom du graphique. Les événements enregistrés durant le fonctionnement des différents modules ou pendant l'exécution des différentes tâches ont différentes sélections d'attributs.

Les rapports suivants sont disponibles :

- Rapport **Audit système**. Ce rapport contient les informations relatives aux événements survenus pendant l'interaction de l'utilisateur avec l'application, ainsi que pendant le fonctionnement de l'application dans son ensemble mais sans rapport avec un module ou une tâche particuliers de Kaspersky Endpoint Security.
- Rapport sur le fonctionnement d'un module ou l'exécution d'une tâche de Kaspersky Endpoint Security.
- Rapport de **chiffrement**. Contient les informations relatives aux événements survenus pendant le chiffrement et le déchiffrement des données.

Les niveaux d'importance suivants sont utilisés dans les rapports :

- **Messages d'information**. Icône . Événements à caractère informatif qui en général ne contiennent aucune information importante.
- **Avertissements**. Icône . Événements qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement de l'application.
- **Événements critiques**. Icône . Événements critiques entraînant des problèmes dans le fonctionnement de Kaspersky Endpoint Security ou des vulnérabilités dans la protection de l'ordinateur.

Pour faciliter l'utilisation des rapports, vous pouvez modifier la représentation des données à l'écran d'une des manières suivantes :

- filtrer la liste des événements selon divers critères ;
- utiliser la fonction de recherche d'un événement en particulier ;
- consulter l'événement sélectionné dans un groupe distinct ;
- trier la liste des événements selon chaque colonne du rapport ;
- afficher et masquer les événements regroupés à l'aide d'un filtre ;
- modifier l'ordre et la sélection des colonnes affichées dans le rapport.

Le cas échéant vous pouvez exporter le rapport obtenu dans un fichier texte.

Vous pouvez également supprimer des informations des rapports selon les modules ou les tâches de Kaspersky Endpoint Security regroupés dans le rapport. Kaspersky Endpoint Security supprime toutes les entrées des rapports sélectionnés depuis la plus ancienne jusqu'à l'heure actuelle.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les informations relatives aux événements peuvent être transmises au Serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur l'utilisation des rapports dans Kaspersky Security Center, consultez l'Aide de Kaspersky Security Center.

Configuration des paramètres des rapports

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres des rapports :

- Configurer la durée maximale de conservation des rapports.

  Par défaut, la durée maximale de conservation des rapports sur les événements détectés par Kaspersky Endpoint Security est de 30 jours. A l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

- Configurer la taille maximale du fichier de rapport.

  Vous pouvez définir la taille maximale du fichier contenant le rapport. Par défaut, la limite sur la taille du fichier du rapport est de 1 024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale. Vous pouvez lever la restriction sur la taille du fichier du rapport ou définir une autre valeur.

Configuration de la durée maximale de conservation des rapports

Pour configurer la durée maximale de conservation des rapports, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Rapports et stockage**.
3. Dans la partie droite de la fenêtre dans le groupe **Rapports**, exécutez une des actions suivantes :
   - Cochez la case **Supprimer les rapports après** si vous voulez établir des restrictions sur la conservation des rapports. Dans le champ à droite de la case **Supprimer les rapports après**, indiquez la durée maximale d'enregistrement des rapports.

     La durée maximale de conservation par défaut des rapports est de 30 jours.
   - Décochez la case **Supprimer les rapports après** si vous voulez annuler les restrictions sur l'enregistrement des rapports.

   Par défaut, la restriction de la durée d'enregistrement des rapports est activée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la taille maximale du fichier de rapport

Pour configurer la taille maximale du fichier de rapport, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Rapports et stockage**.
3. Dans la partie droite de la fenêtre dans le groupe **Rapports**, exécutez une des actions suivantes :
   - Cochez la case **Taille maximale du fichier** si vous souhaitez établir une limite sur la taille du fichier du rapport. Dans le champ situé à droite de la case **Taille maximale du fichier**, saisissez la taille maximale du fichier du rapport.

     Par défaut, la limite sur la taille du fichier du rapport est de 1 024 Mo.
   - Décochez la case **Taille maximale du fichier** si vous souhaitez lever la restriction sur la taille du fichier du rapport.

   Par défaut, la limite sur la taille du fichier du rapport est activée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Consultation des rapports

Si l'affichage des rapports est disponible pour l'utilisateur, celui-ci peut consulter tous les événements repris dans les rapports.

Pour consulter les rapports, procédez comme suit :

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

   La fenêtre **Rapports** s'ouvre.

2. Sélectionnez le module ou la tâche dans la liste proposée dans la partie gauche de la fenêtre **Rapports**.

   La partie droite de la fenêtre affiche le rapport qui contient la liste des événements survenus suite au fonctionnement du module sélectionné ou de la tâche de Kaspersky Endpoint Security.

Vous pouvez trier les événements dans le rapport selon les valeurs des cellules d'une des colonnes. Par défaut, les événements dans le rapport sont classés selon l'ordre croissant des valeurs des cellules la colonne **Date de l'événement**.

Consultation des informations relatives à l'événement dans le rapport

Vous pouvez consulter des informations détaillées pour chaque événement dans le rapport.

Pour consulter les informations détaillées sur un événement dans le rapport, procédez comme suit :

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

   La fenêtre **Rapports** s'ouvre.

2. Dans la partie gauche de la fenêtre, sélectionnez le rapport sur le fonctionnement d'un module ou d'une tâche qui vous intéresse.

   Les événements couverts par le rapport apparaissent dans la partie droite de la fenêtre. Pour rechercher des événements particuliers dans le rapport, utilisez les fonctions de filtre, de recherche et de tri.

3. Sélectionnez l'événement qui vous intéresse dans le rapport.

Une section reprenant des informations de synthèse sur l'événement apparaît dans la partie inférieure de la fenêtre.

Enregistrement du rapport dans un fichier

L'utilisateur est seul responsable de la sécurité des informations du rapport enregistré dans le fichier et, plus particulièrement, du contrôle et de la restriction de l'accès à ces informations.

Le rapport composé peut être enregistré dans le fichier texte au format TXT ou CSV.

Kaspersky Endpoint Security enregistre l'événement dans un rapport de la même manière qu'il est présenté à l'écran, c'est-à-dire avec la même composition et avec la même séquence d'attributs de l'événement.

Pour enregistrer le rapport dans un fichier, procédez comme suit :

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

   La fenêtre **Rapports** s'ouvre.

2. Sélectionnez le module ou la tâche dans la liste proposée dans la partie gauche de la fenêtre **Rapports**.

   La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche de Kaspersky Endpoint Security.

3. S'il faut, modifiez la présentation des données dans le rapport à l'aide des moyens suivants :

   - filtrage des événements ;
   - recherche d'événements ;
   - modification de l'emplacement des colonnes ;
   - classement des événements.

4. Cliquez sur le bouton **Enregistrer le rapport** situé dans la partie supérieure droite de la fenêtre.

   Un menu contextuel s'ouvre.

5. Dans le menu contextuel, sélectionnez l'encodage requis pour l'enregistrement du fichier : **Enregistrer au format ANSI** ou **Enregistrer au format Unicode**.

   La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvre.

6. Dans la fenêtre ouverte **Enregistrer sous**, saisissez le champ dans lequel vous voulez enregistrer le fichier de rapport.

7. Saisissez le nom du fichier du rapport dans le champ **Nom du fichier**.

8. Dans le champ **Type de fichier**, sélectionnez le format requis du fichier de rapport : TXT ou CSV.

9. Cliquez sur le bouton **Enregistrer**.

Suppression des informations des rapports

Pour supprimer les informations des rapports, procédez comme suit :

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

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Rapports et stockage**.

3. Dans la partie droite de la fenêtre, dans le groupe **Rapports**, cliquez sur le bouton **Supprimer les rapports**.

   La fenêtre **Suppression des rapports** s'ouvre.

4. Cochez les cases pour les rapports depuis lesquels vous voulez supprimer les informations :

   - **Tous les rapports**.
   - **Rapport des modules de protection**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Endpoint Security :
     - Détection comportementale.

- Protection contre les Exploits.
- Prévention des intrusions.
- Protection contre les fichiers malicieux.
- Protection contre les menaces Internet.
- Protection contre les menaces par emails.
- Protection contre les menaces réseau.
- Protection BadUSB.
- Fournisseur de protection AMSI.

- **Rapport des modules de contrôle**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Endpoint Security :
  - Contrôle des applications.
  - Contrôle des périphériques.
  - Contrôle Internet.
  - Contrôle évolutif des anomalies.
- **Rapport sur le chiffrement des données**. Contient les informations sur les tâches de chiffrement des données exécutées.
- **Rapport des tâches d'analyse**. Contient les informations sur les tâches d'analyse exécutées suivantes :
  - Analyse complète.
  - Analyse des zones critiques.
  - Analyse personnalisée.

  Les informations sur l'exécution de la tâche Vérification de l'intégrité sont supprimées uniquement si la case **Tous les rapports** est cochée.
- **Rapport des tâches de mise à jour**. Contient les informations sur les tâches de mise à jour exécutées :
- **Rapport du module Pare-feu**. Contient les informations sur le fonctionnement du Pare-feu.
- **Rapport du module Endpoint Sensor**. Contient les informations relatives au fonctionnement du module Endpoint Sensor.

5. Cliquez sur le bouton **OK**.

Service des notifications

Cette section reprend les informations sur le service des notifications qui signalent aux utilisateurs les événements survenus pendant le fonctionnement de Kaspersky Endpoint Security, ainsi que les instructions sur la configuration des paramètres de ces notifications.

A propos des notifications de Kaspersky Endpoint Security

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Endpoint Security. Les notifications relatives à ces événements peuvent avoir un caractère informatif ou importants. Par exemple, la notification peut signaler la réussite de la mise à jour des bases et des modules de l'application ou signaler une erreur dans le fonctionnement d'un module qu'il faudra rectifier au plus vite.

Kaspersky Endpoint Security permet de consigner les informations relatives aux événements survenus dans le fonctionnement de l'application dans le journal des événements Microsoft Windows et/ou dans le journal de Kaspersky Endpoint Security.

Kaspersky Endpoint Security peut remettre les notifications de la manière suivante :

- Via des pop-ups de notification dans la zone de notification de la barre des tâches de Microsoft Windows.
- Par email.

Vous pouvez configurer les modes de remise des notifications. Le mode de remise des notifications est défini pour chaque type d'événement.

Configuration des paramètres du service des notifications

Vous pouvez exécuter les opérations suivantes pour configurer le service des notifications :

- Configurer les paramètres des journaux des événements dans lesquels Kaspersky Endpoint Security enregistre les événements.
- Configurer l'affichage des notifications à l'écran.
- Configurer la remise des notifications par courrier électronique.

Grâce au tableau des événements pour la configuration du service des notifications, vous pouvez réaliser les opérations suivantes :

- filtrer les événements du service des notifications en fonction de la valeur des colonnes ou selon un filtre complexe ;
- utiliser la fonction de recherche des événements du service des notifications ;
- trier les événements du service des notifications ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des événements du service des notifications.

Configuration des paramètres des journaux des événements

Pour configurer les paramètres des journaux des événements, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Interface**.

   Les paramètres de l'interface de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Notifications**.

   La fenêtre **Notifications** s'ouvre.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

   Les événements peuvent contenir les données suivantes de l'utilisateur :

   - chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;
   - chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
   - nom d'utilisateur Microsoft Windows ;
   - adresses des pages Web ouvertes par l'utilisateur.
4. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer les paramètres des journaux des événements.
5. Cochez les cases en regard des événements requis dans les colonnes **Enregistrer dans le journal local** et **Enregistrer dans le journal d'événements Windows**.

   Les événements dont la case a été cochée dans la colonne **Enregistrer dans le journal local** s'affichent dans les **Journaux des applications et des services** de la section **Journal des événements Kaspersky**. Les événements dont la case a été cochée dans la colonne **Enregistrer dans le journal d'événements Windows** s'affichent dans les **Journaux Windows** de la section **Application**. Pour ouvrir les journaux des événements, sélectionnez **Démarrer → Panneau de configuration → Administration → Consultation des événements**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'affichage et la remise des notifications

Pour configurer les paramètres d'affichage et de remise des notifications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Interface**.

   Les paramètres de l'interface de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Notifications**.

   La fenêtre **Notifications** s'ouvre.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.

   Les événements peuvent contenir les données suivantes de l'utilisateur :

   - chemins d'accès aux fichiers analysés à l'aide de Kaspersky Endpoint Security ;

- chemins d'accès aux clés du registre modifiées pendant le fonctionnement de Kaspersky Endpoint Security ;
- nom d'utilisateur Microsoft Windows ;
- adresses des pages Web ouvertes par l'utilisateur.

4. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer la remise des notifications.
5. Dans la colonne **Notifier sur écran**, cochez les cases en regard des événements requis.

   Les informations relatives aux événements sélectionnés sont affichées dans des messages contextuels dans la zone de notification de la barre des tâches de Microsoft Windows.
6. Dans la colonne **Notifier par email**, cochez les cases en regard des événements requis.

   Les informations relatives aux événements sélectionnés sont remises par email si les paramètres de remise des notifications par courrier ont été définis.
7. Cliquez sur le bouton **Configuration des notifications par email**.

   La fenêtre **Configuration des notifications par email** s'ouvre.
8. Cochez la case **Envoyer les notifications sur les événements** si vous souhaitez activer la remise des informations sur les événements du fonctionnement de Kaspersky Endpoint Security, sélectionnés dans la colonne **Notifier par email**.
9. Définissez les paramètres de remise des messages électroniques.
10. Dans la fenêtre **Paramètres des notifications par email**, cliquez sur le bouton **OK**.
11. Dans la fenêtre **Notifications**, cliquez sur le bouton **OK**
12. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'affichage des avertissements sur l'état de l'application dans la zone de notification

Pour configurer l'affichage des avertissements sur l'état de l'application à la zone de notification, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Interface**.

   Les paramètres de l'interface de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Avertissements**, cochez les cases en regard des catégories d'événements pour lesquels vous souhaitez voir des notifications dans la zone de notification de Microsoft Windows.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Quand un événement de la catégorie choisie survient, l'icône de l'application dans la zone de notification se transformera en  ou  en fonction de l'importance de l'avertissement.

Utilisation de la sauvegarde

Cette section explique comment configurer les paramètres du dossier de sauvegarde et comment les utiliser.

À propos de la Sauvegarde

La *Sauvegarde* une liste de copies de sauvegarde des fichiers qui ont été supprimés ou modifiés pendant le processus de désinfection. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès à ce dossier sont accordées aux utilisateurs du groupe Administrators. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Kaspersky Endpoint Security n'offre pas la possibilité de configurer les autorisations d'accès des utilisateurs aux copies de sauvegarde des fichiers.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la désinfection. Si le fichier désinfecté contenait des informations critiques partiellement ou complètement perdues suite à la désinfection, vous pouvez tenter de restaurer le fichier depuis sa copie de sauvegarde dans son dossier d'origine.

Si Kaspersky Endpoint Security est administré par Kaspersky Security Center, les copies de sauvegarde des fichiers peuvent être transmises au serveur d'administration de Kaspersky Security Center. Pour en savoir plus sur l'utilisation des copies de sauvegarde des fichiers dans Kaspersky Security Center, consultez l'Aide de Kaspersky Security Center.

Configuration de la Sauvegarde

Vous pouvez réaliser les opérations suivantes au niveau de la configuration du dossier de sauvegarde :

- Configurer la durée maximale de conservation des copies de fichiers dans le dossier de sauvegarde.

  Par défaut, la durée maximale de conservation des copies dans le dossier de sauvegarde est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens de la sauvegarde. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

- Configurer la taille maximale du dossier de sauvegarde.

  Par défaut, la taille maximale du dossier de sauvegarde est de 100 Mo. Quand le stockage des données atteint la taille maximale configurée, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens du dossier de sauvegarde afin de ne plus dépasser la limite. Vous pouvez lever la restriction sur la taille maximale du dossier de sauvegarde ou modifier la taille maximale.

Configuration de la durée de conservation maximale des fichiers dans la sauvegarde

Pour configurer la durée de conservation maximale des fichiers dans le dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Rapports et stockage**.
3. Exécutez une des actions suivantes :
   - Dans la partie droite de la fenêtre, dans le groupe **Sauvegarde**, cochez la case **Supprimer les objets après** si vous souhaitez limiter la durée de conservation des copies dans la Sauvegarde. Dans le champ situé à droite de **Supprimer les objets après**, saisissez la durée de conservation maximale des copies de fichiers dans le dossier de sauvegarde. Par défaut, la durée maximale de conservation des copies dans le dossier de sauvegarde est de 30 jours.
   - Dans la partie droite de la fenêtre, dans le groupe **Sauvegarde**, décochez la case **Supprimer les objets après** si vous souhaitez annuler la limite de la durée de conservation des copies dans la Sauvegarde.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de la taille maximale de la Sauvegarde

Pour configurer la taille maximale du dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Rapports et stockage**.
3. Exécutez une des actions suivantes :
   - Si vous souhaitez limiter la taille totale de la Sauvegarde, cochez la case **Taille maximale du stockage** dans la partie droite de la fenêtre dans le groupe **Sauvegarde** et indiquez la taille maximale de la Sauvegarde dans le champ situé droite de la case **Taille maximale du stockage**.

     Par défaut la taille maximale du stockage de données, qui reprend la Sauvegarde des fichiers, est de 100 Mo.
   - Si vous voulez annuler la restriction sur la taille de la sauvegarde, décochez la case **Taille maximale du stockage** dans le groupe **Sauvegarde** de la partie droite de la fenêtre.

   Par défaut, la taille de la sauvegarde n'est pas limitée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Restauration et suppression des fichiers depuis la sauvegarde

Si Kaspersky Endpoint Security détecte un code malveillant dans un fichier, il bloque celui-ci, lui attribue l'état *Infecté* et place une copie dans le dossier de sauvegarde avant de tenter de le désinfecter. Si le fichier est réparé, l'état de la copie de sauvegarde devient *Réparé*. Le fichier est accessible dans le dossier d'origine. En cas d'échec de la désinfection, Kaspersky Endpoint Security le supprime du dossier d'origine. Vous pouvez restaurer le fichier à partir de sa copie de sauvegarde dans le dossier d'origine.

En cas de détection d'un code malveillant dans un fichier qui appartient à une app de Windows Store, Kaspersky Endpoint Security ne place pas la copie de fichier dans la sauvegarde, mais le supprime directement. Dans ce cas, pour restaurer l'intégrité de l'app de Windows Store, vous pouvez utiliser les outils du système d'exploitation Microsoft Windows 8 (pour en savoir plus sur la restauration d'une app de Windows Store, lisez *l'Aide de Microsoft Windows 8*).

Kaspersky Endpoint Security supprime les copies de sauvegarde des fichiers de n'importe quel état automatiquement à l'issue de la période définie dans les paramètres de l'application.

Vous pouvez aussi supprimer vous-même n'importe quelle copie de fichier dans la sauvegarde.

La liste des copies de sauvegarde des fichiers se présente sous la forme d'un tableau.

Vous pouvez réaliser les opérations suivantes sur les copies de sauvegarde des fichiers du dossier de sauvegarde :

- Consulter la liste des copies de sauvegarde des fichiers.

  Pour la copie de sauvegarde du fichier, le chemin d'accès au dossier d'emplacement d'origine de ce fichier apparaît. Ce chemin d'accès peut contenir des données personnelles.

- Restaurer les fichiers à partir des copies de sauvegarde dans leurs dossiers d'origine.
- Supprimer des copies de sauvegarde de fichiers du dossier de sauvegarde.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer les copies de sauvegarde selon les colonnes, y compris à l'aide de filtres complexes ;
- utiliser la fonction de recherche de copies de sauvegarde ;
- trier les copies de sauvegarde ;
- modifier l'ordre et la sélection des colonnes affichées dans le tableau des copies de sauvegarde.

Vous pouvez copier les informations relatives aux fichiers sélectionnés de la sauvegarde dans le Presse-papiers. Pour sélectionner plusieurs fichiers de la sauvegarde, ouvrez le menu contextuel de n'importe quel fichier d'un clic droit, puis choisissez l'option **Tout sélectionner**. Ensuite, sélectionnez les fichiers que vous souhaitez retirer de la sélection en maintenant la touche **CTRL** enfoncée.

Restauration des fichiers depuis la sauvegarde

Si la Sauvegarde contient plusieurs fichiers portant le même nom, mais de contenu différent placés dans le même dossier, seul le fichier placé en dernier dans la Sauvegarde peut être restauré.

Pour restaurer des fichiers depuis le dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale des applications, cliquez sur le bouton **Stockages**.

   La fenêtre **Sauvegarde** s'ouvre.

2. Si vous voulez restaurer tous les fichiers de la sauvegarde, choisissez l'option **Restaurer tout** dans le menu contextuel de n'importe quel fichier de la fenêtre **Sauvegarde**.

   Kaspersky Endpoint Security restaure tous les fichiers depuis le dossier de sauvegarde vers leurs dossiers d'origine.

3. Si vous souhaitez restaurer un ou plusieurs fichiers depuis le dossier de sauvegarde, procédez comme suit :

   a. Dans le tableau de la fenêtre **Sauvegarde**, sélectionnez un ou plusieurs fichiers du dossier de sauvegarde.

      Pour sélectionner plusieurs fichiers de la sauvegarde, ouvrez le menu contextuel de n'importe quel fichier d'un clic droit, puis choisissez l'option **Tout sélectionner**. Ensuite, sélectionnez les fichiers que vous souhaitez retirer de la sélection en maintenant la touche **CTRL** enfoncée.

   b. Choisissez une des méthodes suivantes pour restaurer les fichiers :

      - Cliquez sur le bouton **Restaurer**.
      - Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Restaurer**.

   Kaspersky Endpoint Security restaure tous les fichiers sélectionnés depuis le dossier de sauvegarde vers leurs dossiers d'origine.

Suppression des copies de sauvegarde des fichiers depuis le dossier de sauvegarde

Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :

1. Dans la fenêtre principale des applications, cliquez sur le bouton **Stockages**.
2. La fenêtre **Sauvegarde** s'ouvre.
3. Si vous voulez supprimer tous les fichiers de la Sauvegarde, exécutez une des actions suivantes :

   - Dans le menu contextuel de n'importe quel fichier, choisissez l'option **Tout supprimer**.
   - Cliquez sur le bouton **Purger le stockage**.

   Kaspersky Endpoint Security supprimera toutes les copies de sauvegarde des fichiers de la sauvegarde.

4. Si vous souhaitez supprimer un ou plusieurs fichiers depuis la sauvegarde, procédez comme suit :

   a. Dans le tableau de la fenêtre **Sauvegarde**, sélectionnez un ou plusieurs fichiers du dossier de sauvegarde.

      Pour sélectionner plusieurs fichiers de la sauvegarde, ouvrez le menu contextuel de n'importe quel fichier d'un clic droit, puis choisissez l'option **Tout sélectionner**. Ensuite, sélectionnez les fichiers que vous souhaitez retirer de la sélection en maintenant la touche **CTRL** enfoncée.

   b. Supprimez les fichiers à l'aide d'un des moyens suivants :

- Cliquez sur le bouton **Supprimer**.
- Cliquez-droit pour ouvrir le menu contextuel, puis sélectionnez l'option **Supprimer**.

Kaspersky Endpoint Security supprimera les copies de sauvegarde sélectionnées des fichiers de la sauvegarde.

Configuration avancée de l'application

Cette section contient les informations sur la configuration généraux de Kaspersky Endpoint Security.

Zone de confiance

Cette section présente des informations sur la zone de confiance et explique comment configurer les exclusions de l'analyse et composer une liste d'applications de confiance.

A propos de la zone de confiance

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Vous pouvez exclure de l'analyse les éléments suivants :

- fichiers d'un format déterminé ;
- fichiers selon un masque ;
- fichiers séparés ;
- dossiers ;
- processus des applications.

Exclusions de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Les exclusions de l'analyse permettent d'utiliser des applications légitimes qui pourraient être employées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques vers des sites Internet payants. Ce genre d'application n'est pas considéré comme un virus. Des détails sur les logiciels légaux qui peuvent être utilisés par des criminels pour endommager l'ordinateur ou les données personnelles sont disponibles sur l'encyclopédie Kaspersky Virus à l'adresse https://encyclopedia.kaspersky.com/knowledge/riskware/.

Kaspersky Endpoint Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des exclusions de l'analyse sur les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque du nom de la menace conformément au classement de l'Encyclopédie des virus de Kaspersky. Par exemple, vous utilisez souvent dans le cadre de votre travail l'application Radmin prévue pour l'administration à distance des ordinateurs. Kaspersky Endpoint Security classe cette activité parmi les activités suspectes et peut la bloquer. Pour exclure le blocage d'une application, il est nécessaire de créer une exclusion de l'analyse dans laquelle vous indiquerez le nom ou le masque du nom selon la classification de l'Encyclopédie des virus de Kaspersky.

Si votre ordinateur est doté d'une application qui récolte et envoie des informations à traiter, Kaspersky Endpoint Security peut la considérer comme une application malveillante. Pour éviter cela, vous pouvez exclure ce programme de l'analyse, en configurant Kaspersky Endpoint Security de manière décrite dans ce document.

Les exclusions de l'analyse peuvent être utilisées pendant le fonctionnement des modules et des tâches suivants de l'application définis par l'administrateur du système :

- Détection comportementale.
- Protection contre les Exploits.
- Prévention des intrusions.
- Protection contre les fichiers malicieux.
- Protection contre les menaces Internet.
- Protection contre les menaces par emails.
- Tâches d'analyse.

Liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et réseau (y compris l'activité malveillante), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Endpoint Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Kaspersky Endpoint Security exclut de l'analyse toute application ajoutée à la liste des applications de confiance.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance. L'analyse ignore ensuite les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Endpoint Security considère comme suspectes peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic réseau d'un ordinateur par Kaspersky Endpoint Security et un autre logiciel antivirus) et d'améliorer les performances de l'ordinateur, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre programmes présentant une menace. Pour exclure entièrement l'application de l'analyse Kaspersky Endpoint Security, il est nécessaire d'utiliser les exclusions de l'analyse.

Définition de l'exclusion de l'analyse

Kaspersky Endpoint Security n'analyse pas l'objet si au lancement d'une des tâches d'analyse le disque dur ou le dossier d'emplacement de cet objet figure dans la zone d'analyse. Cependant, lors du lancement de la tâche d'analyse personnalisée, l'exclusion de l'analyse n'est pas appliquée à cet objet.

Pour créer une exclusion de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions de l'analyse**.

4. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion de l'analyse** s'ouvre. Cette fenêtre permet de créer une exclusion de l'analyse à l'aide d'un ou de deux critères du groupe **Propriétés**.

5. Si vous souhaitez exclure un fichier ou un dossier de l'analyse, procédez comme suit :

   a. Dans le groupe **Propriétés**, cochez la case **Fichier ou dossier**.

   b. Le lien **sélectionnez le fichier ou le dossier** situé dans le groupe **Description de l'exclusion de l'analyse** permet d'ouvrir la fenêtre **Nom du fichier ou du dossier**.

   c. Saisissez le nom du fichier ou du dossier, le masque du nom du fichier ou du dossier ou choisissez le fichier ou le dossier dans l'arborescence des dossiers après avoir cliqué sur le bouton **Parcourir**.

      Utilisez des masques :

      - Le caractère `*` (astérisque) remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque

`C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` (point d'interrogation) remplace n'importe quel caractère unique dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

Dans le masque du nom du fichier ou du dossier, vous pouvez utiliser le caractère * qui remplace n'importe quelle suite de caractères dans le nom du fichier.

Par exemple, vous pouvez utiliser les masques pour ajouter les chemins suivants :

- Chemins d'accès à des fichiers situés dans n'importe quel dossier :
  - Le masque `*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe.
  - Le masque `example` reprend tous les chemins d'accès aux fichiers dont le nom est EXAMPLE.
- Chemins d'accès à des fichiers situés dans le dossier indiqué :
  - Le masque C:\dir*.* reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
  - Le masque C:\dir* reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
  - Le masque C:\dir\ reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
  - Le masque C:\dir*.exe reprend tous les chemins d'accès aux fichiers portant l'extension exe dans le dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
  - Le masque C:\dir\test reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
  - Le masque C:\dir*\test reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\ et dans les sous-dossiers du dossier C:\dir\.
- Chemin d'accès aux fichiers situés dans tous les dossiers portant le nom indiqué :
  - Le masque dir*.* reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
  - Le masque dir* reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
  - Le masque dir\ reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.

- Le masque dir*.exe reprend tous les chemins d'accès aux fichiers portant l'extension exe dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque dir\test reprend tous les chemins d'accès aux fichiers portant le nom test dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.

d. Cliquez sur le bouton **OK** dans la fenêtre **Nom du fichier ou du dossier**.

Le lien vers le fichier ou le dossier ajouté apparaît dans le groupe **Description de l'exclusion de l'analyse** de la fenêtre **Exclusion de l'analyse**.

6. Si vous voulez exclure de l'analyse des objets portant un nom précis, procédez comme suit :

a. Dans le groupe **Propriétés**, cochez la case **Nom de l'objet**.

b. Le lien **saisissez le nom de l'objet** situé dans le groupe **Description de l'exclusion de l'analyse** permet d'ouvrir la fenêtre **Nom de l'objet**.

c. Saisissez le nom ou le masque de l'objet conformément au classement de l'Encyclopédie de virus de Kaspersky.

d. Cliquez sur le bouton **OK** dans la fenêtre **Nom de l'objet**.

Le lien vers le nom de l'objet ajouté apparaît dans le groupe **Description de l'exclusion de l'analyse** de la fenêtre **Exclusion de l'analyse**.

7. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

8. Définissez les modules de Kaspersky Endpoint Security qui doivent appliquer l'exclusion de l'analyse :

a. Cliquez sur le lien **quelconque** situé dans le groupe **Description de l'exclusion de l'analyse** pour activer le lien **sélectionnez les modules**.

b. Cliquez sur le lien **sélectionnez les modules** pour ouvrir la fenêtre **Modules de protection**.

c. Cochez les cases en regard modules auxquels s'appliqueront les exclusions de l'analyse.

d. Cliquez sur le bouton **OK** dans la fenêtre **Modules de protection**.

Si les modules sont indiqués dans les paramètres de l'exclusion de l'analyse, l'exclusion n'est appliquée que lorsque l'analyse est effectuée par ces modules de Kaspersky Endpoint Security.

Si les modules ne sont pas indiqués dans les paramètres de l'exclusion de l'analyse, l'exclusion est appliquée lors de l'analyse effectuée par tous les modules de Kaspersky Endpoint Security.

9. Cliquez sur le bouton **OK** dans la fenêtre **Exclusion de l'analyse**.

L'exclusion de l'analyse ajoutée apparaît dans le tableau de l'onglet **Exclusions de l'analyse** de la fenêtre **Zone de confiance**. Le groupe **Description de l'exclusion de l'analyse** affiche les paramètres définis de cette exclusion de l'analyse.

10. Dans la fenêtre **Zone de confiance**, cliquez sur **OK**.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Modification de l'exclusion de l'analyse

Pour modifier une exclusion de l'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions de l'analyse**.
4. Sélectionnez l'exclusion de l'analyse souhaitée dans la liste.
5. Modifiez les paramètres de l'exclusion de l'analyse d'une des manières suivantes :

   - Cliquez sur le bouton **Modifier**.

     La fenêtre **Exclusions de l'analyse** s'ouvre.
   - Ouvrez la fenêtre où vous pourrez modifier le paramètre via le lien dans le champ **Description de l'exclusion de l'analyse**.
6. Si vous aviez cliqué sur le bouton **Modifier** à l'étape précédente, cliquez sur le bouton **OK** dans la fenêtre **Exclusion de l'analyse**.

   Le groupe **Description de l'exclusion de l'analyse** affiche les modifications apportées aux paramètres de cette exclusion de l'analyse.
7. Dans la fenêtre **Zone de confiance**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Suppression de l'exclusion de l'analyse

Pour supprimer une exclusion de l'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions de l'analyse**.
4. Sélectionnez l'exclusion souhaitée dans la liste des exclusions de l'analyse.
5. Cliquez sur le bouton **Supprimer**.

   L'exclusion de l'analyse supprimée disparaît de la liste.
6. Dans la fenêtre **Zone de confiance**, cliquez sur **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lancement et arrêt du fonctionnement de l'exclusion de l'analyse

Pour lancer ou arrêter une exclusion de l'analyse, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre sous l'onglet **Exclusions de l'analyse**.
4. Sélectionnez l'exclusion souhaitée dans la liste des exclusions.
5. Exécutez une des actions suivantes :

   - Cochez la case en regard du nom de l'exclusion de l'analyse si vous souhaitez activer cette exclusion.
   - Décochez la case en regard du nom de l'exclusion de l'analyse si vous souhaitez suspendre temporairement le fonctionnement de cette exclusion.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Composition de la liste des applications de confiance

Pour composer une liste des applications de confiance, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.
4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.
5. Si vous voulez ajouter une application à la liste des applications de confiance, procédez comme suit :

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

   b. Dans le menu déroulant ouvert, exécutez une des actions suivantes :

   - Sélectionnez l'option **Applications** si vous voulez trouver l'application dans la liste des applications installées sur l'ordinateur.

La fenêtre **Sélection de l'application** s'ouvre.

- Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin au fichier exécutable de l'application nécessaire.

  La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

c. Sélectionnez l'application à l'aide d'un des moyens suivants :

- Si vous aviez choisi, à l'étape précédente, l'option **Applications**, choisissez l'application dans la liste des applications installées sur l'ordinateur, puis cliquez sur le bouton **OK** dans la fenêtre **Sélection de l'application**.

- Si vous aviez choisi, à l'étape précédente, l'option **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application requise, puis cliquez sur le bouton **Ouvrir** dans la fenêtre standard Microsoft Windows **Ouvrir**.

Suite aux actions exécutées, la fenêtre **Exclusions de l'analyse pour l'application** s'ouvre.

a. Cochez les cases en regard des règles requises de la zone de confiance pour l'application choisie :

- **Ne pas analyser les fichiers ouverts**.
- **Ne pas surveiller l'activité de l'application**.
- **Ne pas hériter les restrictions du processus parent (application)**.
- **Ne pas surveiller l'activité des applications enfants**.
- **Ne pas bloquer l'interaction avec l'interface de l'application**.
- **Ne pas bloquer l'interaction avec le fournisseur de protection AMSI**.
- **Ne pas analyser le trafic réseau**.

b. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de l'analyse pour l'application**.

L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.

6. Si vous voulez modifier les paramètres de l'application de confiance, procédez comme suit :

a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

b. Cliquez sur le bouton **Modifier**.

c. La fenêtre **Exclusions de l'analyse pour l'application** s'ouvre.

d. Cochez ou décochez les cases en regard des règles requises de la zone de confiance pour l'application choisie.

> Si dans la fenêtre **Exclusions de l'analyse pour l'application** aucune des règles de la zone de confiance pour l'application n'a été choisie, l'application de confiance est incluse dans l'analyse. L'application de confiance n'est pas supprimée de la liste des applications de confiance, seule sa case est décochée.

e. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de l'analyse pour l'application**.

7. Si vous voulez supprimer l'application de confiance de la liste des applications de confiance, procédez comme suit :

   a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

   b. Cliquez sur le bouton **Supprimer**.

8. Dans la fenêtre **Zone de confiance**, cliquez sur **OK**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de l'effet des règles de la zone de confiance sur l'application de la liste des applications de confiance

Pour activer ou désactiver l'effet des règles de la zone de confiance sur une application de la liste des applications de confiance, procédez comme suit :

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

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Analyser les exclusions et la zone de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.

4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.

5. Sélectionnez l'application de confiance requise dans la liste des applications de confiance.

6. Exécutez une des actions suivantes :

   - Cochez la case en regard du nom de l'application de confiance si vous souhaitez l'exclure de l'analyse de Kaspersky Endpoint Security.

   - Décochez la case en regard du nom de l'application de confiance si vous souhaitez l'inclure dans l'analyse de Kaspersky Endpoint Security.

7. Cliquez sur le bouton **OK**.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Utilisation du stockage système sécurisé des certificats

L'utilisation du stockage système sécurisé des certificats permet d'exclure de l'analyse antivirus les applications signées par une signature numérique de confiance. Kaspersky Endpoint Security attribue automatiquement ces applications au groupe *De confiance*

Pour commencer à utiliser le stockage système sécurisé des certificats, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvre.
4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Stockage système sécurisé des certificats**.
5. Cochez la case **Utiliser le stockage système sécurisé des certificats**.
6. Dans la liste déroulante **Stockage système sécurisé des certificats**, choisissez le stockage système que Kaspersky Endpoint Security devra considéré comme sécurisé.
7. Dans la fenêtre **Zone de confiance**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Contrôle du trafic réseau

Cette section contient des informations sur le contrôle du trafic réseau et les instructions sur la configuration des paramètres des ports réseau contrôlés.

A propos du contrôle du trafic réseau

Lors du fonctionnement de Kaspersky Endpoint Security, les composants Contrôle Internet, Protection contre les menaces par emails et Protection contre les menaces Internet contrôlent les flux de données transmis via des protocoles déterminés sur les ports TCP et UDP définis et ouverts de l'ordinateur de l'utilisateur. Par exemple, le composant Protection contre les menaces par emails analyse les informations transmises via le protocole SMTP et le module Protection contre les menaces Internet, les informations transmises via les protocoles HTTP et FTP.

Kaspersky Endpoint Security répartit les ports TCP et UDP du système d'exploitation en plusieurs groupes en fonction de la probabilité d'une attaque réussie contre ceux-ci. Il est conseillé de soumettre les ports réseaux associés à des services vulnérables à un contrôle plus strict car ceux-ci courent un risque plus élevé d'être pris pour cible par une attaque réseau. Si vous utilisez des services non standards quelconques affectés à des ports réseau inhabituels, sachez que ces ports peuvent être eux-aussi soumis à une attaque. Vous pouvez préciser une liste de ports réseau et une liste d'applications qui demandent un accès au réseau. Lors de la surveillance du trafic réseau, ces ports et applications font ensuite l'objet d'une attention particulière de la part des composants Protection contre les menaces par emails et Protection contre les menaces Internet.

A propos de l'analyse des connexions sécurisées

Lors du premier lancement après l'installation, Kaspersky Endpoint Security ajouter le certificat de Kaspersky au stockage des certificats système.

La fonction d'analyse des connexions sécurisées est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous un système d'exploitation Microsoft Windows pour postes de travail. La fonction d'analyse des connexions sécurisées n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous un système d'exploitation Microsoft Windows pour serveurs de fichiers.

Pour analyser les connexions sécurisées dans Firefox et Thunderbird, Kaspersky Endpoint Security active, dans les paramètres de ces navigateurs, l'utilisation du stockage système des certificats de confiance.

Les modules Contrôle Internet, Protection contre les menaces par emails et Protection contre les menaces Internet sont en mesure de déchiffrer et d'analyser le trafic réseau transmis via des connexions chiffrées selon les protocoles suivants :

- SSL 3.0 ;
- TLS 1.0, TLS 1.1, TLS 1.2.

Configuration des paramètres de contrôle du trafic réseau

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres du contrôle du trafic réseau :

- Activer le contrôle de tous les ports réseau.
- Composer la liste des ports réseau contrôlés.
- Composer la liste des applications dont tous les ports réseau sont contrôlés.

Activation du contrôle de tous les ports réseau

Pour activer le contrôle de tous les ports réseau, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

   Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler tous les ports réseau**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation de l'analyse des ports pour les applications de la liste composée par les experts de Kaspersky

Pour créer la liste des ports réseau contrôlés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.

4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre.

5. Cochez la case **Contrôler tous les ports pour les applications de la liste recommandée par Kaspersky**.

   Si vous cochez cette case, Kaspersky Endpoint Security contrôle tous les ports pour les applications suivantes :

   - Adobe Reader.
   - AIM for Windows.
   - Apple Application Support.
   - Chrome.
   - Digsby.
   - Edge.
   - Firefox.
   - Google Talk.
   - ICQ.
   - Internet Explorer.
   - Java.
   - Mail.ru Agent.
   - Miranda IM.
   - mIRC.
   - Opera.
   - Pidgin.
   - QIP Infium.
   - QIP.
   - QNext.
   - QNextClient.
   - Rockmelt.
   - Safari.

- Simple Instant Messenger.
- Trillian.
- Windows Live Messenger.
- Windows Messenger.
- X-Chat.
- Yahoo! Messenger.
- Navigateur Yandex.

Constitution de la liste des ports réseau contrôlés

Pour créer la liste des ports réseau contrôlés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

   Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre. La fenêtre **Ports réseau** contient la liste des ports réseau utilisés habituellement pour le transfert du courrier électronique et du trafic réseau. Cette liste est livrée avec Kaspersky Endpoint Security.
5. Dans la liste des ports réseau, procédez comme suit :
   - Cochez les cases en regard des ports réseau que vous souhaitez ajouter à la liste des ports réseau contrôlés.

     Par défaut, les cases sont cochées pour tous les ports réseau présentés dans la fenêtre **Ports réseau**.
   - Décochez les cases en regard des ports réseau que vous souhaitez exclure de la liste des ports réseau contrôlés.
6. Si le port réseau contrôlé ne figure pas sur la liste des ports réseau, ajoutez-la de la manière suivante :
   a. Le lien **Ajouter** situé sous la liste des ports réseau permet d'ouvrir la fenêtre **Port réseau**.
   b. Saisissez le numéro du port réseau dans le champ **Port**.
   c. Dans le champ **Description**, saisissez le nom du port réseau.
   d. Cliquez sur le bouton **OK**.

      La fenêtre **Port réseau** se ferme. Le port réseau que vous ajoutez apparaît en fin de liste.
7. Cliquez sur le bouton **OK** dans la fenêtre **Ports réseau**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lors de l'utilisation du protocole FTP en mode passif, la connexion peut être établie via un port réseau aléatoire qui n'a pas été ajouté dans la liste des ports réseau contrôlés. Pour protéger ces connexions, il faut cocher la case **Contrôler tous les ports réseau** dans le groupe **Ports contrôlés** ou configurer le contrôle de tous les ports pour les applications à l'aide desquelles la connexion FTP est établie.

Constitution de la liste des applications dont tous les ports réseau sont contrôlés

Vous pouvez composer une liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security.

Il est conseillé d'ajouter à cette liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security les applications qui reçoivent ou envoient les données via le protocole FTP.

Pour composer la liste des applications dont tous les ports réseau seront contrôlés, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

   Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports réseau sélectionnés**.
4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre.
5. Cochez la case **Contrôler tous les ports pour les applications indiquées**.
6. Dans la liste des applications situé sous la case **Contrôler tous les ports pour les applications indiquées**, procédez comme suit :

   - Cochez les cases en regard des noms des applications dont tous les ports réseau vous souhaitez contrôler.

     Par défaut, les cases sont cochées pour toutes les applications présentées dans la fenêtre **Ports réseau**.
   - Décochez les cases en regard des noms des applications dont tous les ports réseau vous ne souhaitez pas contrôler.
7. Si l'application ne figure pas dans la liste des applications, ajoutez-la d'une des manières suivantes :

   a. A l'aide du lien **Ajouter** situé sous la liste des applications ouvrez le menu contextuel.

   b. Sélectionnez dans le menu contextuel le mode d'ajout d'une application à la liste des applications :

   - Sélectionnez l'option **Applications** pour sélectionner l'application de la liste des applications installées sur l'ordinateur. La fenêtre **Sélection de l'application** s'ouvre, à l'aide de laquelle vous pourrez indiquer le nom de l'application.
   - Sélectionnez l'option **Parcourir** pour désigner l'emplacement du fichier exécutable de l'application. La fenêtre standard Microsoft Windows **Ouvrir** s'ouvre, à l'aide de laquelle vous pourrez indiquer le nom du fichier exécutable de l'application.

   Après avoir sélectionné l'application, la fenêtre **Application** s'ouvre.

c. Saisissez dans le champ **Nom** le nom pour l'application sélectionnée.

d. Cliquez sur le bouton **OK**.

La fenêtre **Application** se ferme. L'application que vous avez ajoutée apparaît dans la liste des applications.

8. Cliquez sur le bouton **OK** dans la fenêtre **Ports réseau**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration de l'analyse des connexions chiffrées

Vous pouvez réaliser les opérations suivantes pour configurer l'analyse des connexions chiffrées :

- Activer l'analyse des connexions chiffrées.
- Configurer les paramètres d'analyse des connexions chiffrées.
- Créer une exclusion pour l'analyse des connexions chiffrées.

Activation et désactivation de l'analyse des connexions chiffrées

Pour activer ou désactiver l'analyse des connexions chiffrées, procédez comme suit :

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

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre dans le groupe **Analyse des connexions chiffrées** exécutez une des actions suivantes :

- Cochez la case **Analyser les connexions sécurisées** si vous voulez que Kaspersky Endpoint Security analyse le trafic réseau chiffré.
- Décochez la case **Analyser les connexions sécurisées** si vous ne voulez pas que Kaspersky Endpoint Security analyse le trafic réseau chiffré.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Configuration des paramètres d'analyse des connexions chiffrées

Pour configurer les paramètres d'analyse des connexions chiffrées, procédez comme suit :

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

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.

3. Dans le groupe **Analyse des connexions chiffrées** de la partie droite de la fenêtre, cliquez sur le bouton **Paramètres complémentaires**.

La fenêtre **Paramètres complémentaires** s'ouvre.

4. Dans la liste déroulante **Lors de l'accès à un domaine avec un certificat douteux**, choisissez une des options suivantes :

   - **Autoriser** Si vous choisissez cette option, Kaspersky Endpoint Security autorise l'établissement d'une connexions réseau lors de l'accès à un domaine avec un certificat douteux.

     Si vous accédez à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui reprend un avertissement et la raison pour laquelle il est déconseillé de visiter ce domaine. Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé. Après que vous avez cliqué sur le lien, Kaspersky Endpoint Security n'affiche plus d'avertissements sur le certificat douteux pendant une heure quand vous accédez à d'autres ressources dans le même domaine.

   - **Interdire**. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau établie avec ce domaine en cas d'accès à un domaine avec un certificat douteux.

     Lors de l'accès à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui indique la raison pour laquelle l'accès à ce domaine est bloqué.

5. Dans la liste déroulante **En cas d'erreur lors de l'analyse des connexions sécurisées**, choisissez une des options suivantes :

   - **Couper la connexion**. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée.

   - **Ajouter le domaine aux exclusions**. Si vous choisissez cette option, en cas d'erreur lors de l'analyse d'une connexion sécurisée, Kaspersky Endpoint Security ajoute le domaine dont l'accès est à l'origine de l'erreur à la liste des domaines avec erreurs d'analyse et il n'analyse pas le trafic réseau chiffré lors de l'accès à ce domaine.

     Le lien **Domaines avec erreurs d'analyse** permet d'ouvrir la fenêtre **Domaines avec erreurs d'analyse** qui reprend les domaines ajoutés aux exclusions suite à l'erreur d'analyse de la connexion sécurisée.

     Le lien **Domaines avec erreurs d'analyse** est accessible après la sélection de l'option **Ajouter le domaine aux exclusions**.

     Si vous choisissez l'option **Couper la connexion** dans la liste déroulante **En cas d'erreur lors de l'analyse des connexions sécurisées**, Kaspersky Endpoint Security supprime toutes les exclusions énumérées dans la fenêtre **Domaines avec erreurs d'analyse**.

6. Cochez la case **Bloquer les connexions selon le protocole SSL 2.0** si vous voulez que Kaspersky Endpoint Security bloque les connexions réseau établies selon le protocole SSL 2.0.

   Décochez la case **Bloquer les connexions selon le protocole SSL 2.0** si vous voulez que Kaspersky Endpoint Security ne bloque pas les connexions réseau établies selon le protocole SSL 2.0 et n'analyse pas le trafic réseau transmis via ces connexions.

   Il est déconseillé d'utiliser le protocole SSL 2.0 car il contient des défauts qui ont un impact sur la sécurité de la transmission des données.

7. Cochez la case **Déchiffrer les connexions sécurisées avec un certificat EV** si vous voulez que Kaspersky Endpoint Security déchiffre et surveille le trafic réseau transmis par des connexions chiffrées établies dans le navigateur à l'aide d'un certificat EV.

   Décochez la case **Déchiffrer les connexions sécurisées avec un certificat EV** si vous ne voulez pas que Kaspersky Endpoint Security déchiffre et surveille le trafic réseau transmis par des connexions chiffrées établies dans le navigateur à l'aide d'un certificat EV.

8. Cliquez sur le bouton **OK**.

9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Création d'une exclusion pour l'analyse des connexions chiffrées

Kaspersky Endpoint Security n'analyse pas les connexions sécurisées établies par des applications pour lesquelles la case **Ne pas analyser le trafic réseau** de la fenêtre **Exclusions de l'analyse pour l'application** a été cochée.

Pour exclure un domaine de l'analyse des connexions chiffrées, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

   Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Domaines de confiance** dans le groupe **Analyse des connexions chiffrées**.

   La fenêtre **Domaines de confiance** s'ouvre.
4. Exécutez une des actions suivantes :

   - Si vous voulez ajouter un nom de domaine ou un masque de nom de domaine à la liste des exclusions, cliquez sur le bouton **Ajouter**.
   - Si vous souhaitez modifier un nom de domaine ou un masque de nom de domaine, sélectionnez l'élément dans la liste des exclusions et cliquez sur le bouton **Modifier**.

   La fenêtre **Nom de domaine** s'ouvre.
5. Saisissez l'adresse Internet, le nom de domaine ou le masque de nom de domaine si vous ne souhaitez pas que Kaspersky Endpoint Security analyse les connexions sécurisées établies lors de l'accès à ce domaine.
6. Cliquez sur le bouton **OK** dans la fenêtre **Nom de domaine**.
7. Dans la fenêtre **Domaines de confiance**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Consultation des exclusions globales de l'analyse du trafic chiffré

Pour consulter les exclusions globales de l'analyse du trafic chiffré, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Paramètres du réseau**.

   Les paramètres du réseau apparaissent dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre **Analyse des connexions chiffrées**, cliquez sur le lien **sites** :

   La fenêtre **Exclusions globales de l'analyse du trafic chiffré** s'ouvre.

La fenêtre affiche le tableau créé par les experts de Kaspersky avec les informations relatives aux sites et aux applications pour lesquels Kaspersky Endpoint Security n'analyse pas les connexions chiffrées. Le tableau peut être actualisé suite à la mise à jour des bases et les modules de Kaspersky Endpoint Security.

4. Cliquez sur le bouton **Fermer** pour fermer la fenêtre

Autodéfense de Kaspersky Endpoint Security

Cette section contient les informations sur les mécanismes de l'autodéfense de Kaspersky Endpoint Security et contre l'administration externe de Kaspersky Endpoint Security, ainsi que les instructions sur la configuration de ces mécanismes.

A propos de l'autodéfense de Kaspersky Endpoint Security

Kaspersky Endpoint Security protège les ordinateurs contre les programmes malveillants, y compris ceux qui tentent de bloquer le fonctionnement de Kaspersky Endpoint Security ou de le supprimer de l'ordinateur.

La stabilité du système de protection de l'ordinateur de l'utilisateur est garantie par les mécanismes d'autodéfense et de protection contre l'administration externe intégrés à Kaspersky Endpoint Security.

Le mécanisme d'*autodéfense* empêche la modification ou la suppression des fichiers d'application sur le disque dur, les processus de mémoire et les entrées dans le registre système.

La *défense de gestion externe* bloque toutes les tentatives d'un ordinateur distant pour contrôler les services d'application.

Sous les systèmes d'exploitation 64 bits, seule l'administration du mécanisme d'autodéfense de Kaspersky Endpoint Security contre la modification et la suppression de fichiers de l'application sur le disque dur ou contre la modification ou la suppression de clés dans la base de registre système est accessible.

Activation et désactivation du mécanisme de l'autodéfense

Par défaut, le mécanisme de l'autodéfense de Kaspersky Endpoint Security est activé. S'il faut, vous pouvez désactiver le mécanisme de l'autodéfense.

Pour activer ou désactiver le mécanisme de l'autodéfense procédez comme suit :

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

2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.

   Les paramètres complémentaires de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer l'autodéfense** si vous voulez activer le mécanisme d'autodéfense de l'application.

- Décochez la case **Activer l'autodéfense** si vous voulez désactiver le mécanisme d'autodéfense de l'application.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation du mécanisme de l'autodéfense contre l'administration externe

Par défaut, le mécanisme de l'autodéfense contre l'administration externe est activé. Le cas échéant, vous pouvez désactiver le mécanisme de l'autodéfense contre l'administration externe.

Pour activer ou désactiver le mécanisme de l'autodéfense contre l'administration externe, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.

   Les paramètres complémentaires de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Désactiver la gestion externe des services systèmes** si vous voulez activer le mécanisme de protection contre l'administration externe.
   - Décochez la case **Désactiver la gestion externe des services systèmes** si vous voulez désactiver le mécanisme de protection contre l'administration externe.

     Pour quitter l'application via la ligne de commande, il faut décocher la case **Désactiver la gestion externe des services systèmes**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Assurance de fonctionnement des applications de l'administration à distance

Il arrive souvent que lors de l'utilisation de mécanismes de protection contre l'administration externe il soit nécessaire d'appliquer une application d'administration externe.

Pour garantir le fonctionnement des applications d'administration à distance, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvre.

4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.
5. Cliquez sur le bouton **Ajouter**.
6. Dans le menu déroulant ouvert, exécutez une des actions suivantes :

   - Sélectionnez l'option **Applications** si vous voulez trouver l'application d'administration à distance dans la liste des applications installées sur l'ordinateur.

     La fenêtre **Sélection de l'application** s'ouvre.

   - Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin d'accès au fichier exécutable de l'application d'administration à distance.

     La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

7. Sélectionnez l'application à l'aide d'un des moyens suivants :

   - Si vous aviez choisi, à l'étape précédente, l'option **Applications**, choisissez l'application dans la liste des applications installées sur l'ordinateur, puis cliquez sur le bouton **OK** dans la fenêtre **Sélection de l'application**.

   - Si vous aviez choisi, à l'étape précédente, l'option **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application requise, puis cliquez sur le bouton **Ouvrir** dans la fenêtre standard Microsoft Windows **Ouvrir**.

   Suite aux actions exécutées, la fenêtre **Exclusions de l'analyse pour l'application** s'ouvre.

8. Cochez la case **Ne pas surveiller l'activité de l'application**.
9. Cliquez sur le bouton **OK** dans la fenêtre **Exclusions de l'analyse pour l'application**.

   L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.

10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

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

Cette section contient les informations sur les performances de Kaspersky Endpoint Security et sur la compatibilité avec d'autres applications, ainsi que les instructions sur la sélection des types d'objets à détecter et le mode de fonctionnement de Kaspersky Endpoint Security.

A propos des performances de Kaspersky Endpoint Security et de la compatibilité avec d'autres applications

Performances de Kaspersky Endpoint Security

Les performances de Kaspersky Endpoint Security désignent le nombre de types d'objets nuisibles à l'ordinateur qui peuvent être détectés et la consommation en ressources et en énergie de l'ordinateur.

Sélection des types d'objets à détecter

Kaspersky Endpoint Security permet de configurer en souplesse la protection de l'ordinateur et de sélectionner les types d'objets que l'application va détecter durant son fonctionnement. Kaspersky Endpoint Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans le système d'exploitation. Vous ne pouvez pas désactiver l'analyse pour ces types d'objets. Ces programmes peuvent infliger des dégâts considérables à l'ordinateur de l'utilisateur. Pour élargir la protection offerte à l'ordinateur, vous pouvez enrichir la liste des types d'objets à détecter en activant le contrôle de l'activité des applications légitimes qui pourraient être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

Utilisation du mode d'économie d'énergie

Si vous utilisez un ordinateur portable, la consommation électrique qu'entraînent les applications revêt une certaine importance. Bien souvent, les tâches programmées de Kaspersky Endpoint Security sont très gourmandes en ressources. Quand l'ordinateur est alimenté par la batterie, pour économiser la charge vous pouvez utiliser le mode d'économie d'énergie.

Le mode d'économie d'énergie permet de reporter automatiquement l'exécution des tâches qui ont été programmées.

- tâche de mise à jour ;
- tâche d'analyse complète ;
- tâche d'analyse rapide ;
- tâche d'analyse personnalisée ;
- tâche d'analyse de l'intégrité.

Cliquez-droit pour ouvrir le menu contextuel de l'application Kaspersky Endpoint Security for Windows et choisissez l'option Propriétés ou cliquez sur le bouton Propriétés situé sous la liste des applications. La tâche de chiffrement reprend dès que l'ordinateur portable est rebranché sur le secteur.

Transfert des ressources de l'ordinateur à d'autres applications

L'utilisation des ressources de l'ordinateur par Kaspersky Endpoint Security peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés à l'utilisation conjointe d'applications en cas de surcharge du processeur et des sous-systèmes de disque, Kaspersky Endpoint Security peut suspendre l'exécution des tâches programmées et céder les ressources à d'autres applications.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas de l'exécution de ces applications, il ne faut pas leur céder les ressources du système d'exploitation.

Au besoin, vous pouvez lancer ces tâches manuellement.

Application de la technologie de désinfection avancée

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. Quand Kaspersky Endpoint Security a détecté une activité malveillante dans le système d'exploitation, il exécute une procédure de désinfection étendue en appliquant la technologie de désinfection avancée. La *technologie de désinfection avancée* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui empêchent Kaspersky Endpoint Security de les supprimer à l'aide d'autres méthodes. La menace est ainsi neutralisée. Pendant l'exécution de la désinfection de l'infection active, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registre du système d'exploitation. La technologie de désinfection avancée est gourmande en ressource et peut ralentir d'autres applications.

A l'issue de la désinfection de l'infection active sur un ordinateur tournant sous Microsoft Windows pour postes de travail, Kaspersky Endpoint Security demande à l'utilisateur de confirmer le redémarrage de l'ordinateur. Après le redémarrage de l'ordinateur, Kaspersky Endpoint Security supprime les fichiers de l'application malveillante et lance une analyse complète simplifiée de l'ordinateur.

Sous Microsoft Windows pour serveurs de fichiers, il est impossible de demander à l'utilisateur de confirmer le redémarrage en raison des particularités de la version de Kaspersky Endpoint Security pour serveurs de fichiers. Le redémarrage non prévu du serveur de fichiers peut entraîner des problèmes liés à l'accès temporairement refusé aux données du serveur de fichiers ou à la perte des données non enregistrées. Il est conseillé de redémarrer le serveur de fichiers strictement selon la planification prévue. Par défaut, la technologie de désinfection avancée pour les serveurs de fichiers est désactivée.

En cas de détection d'une infection active sur un serveur de fichiers, un événement relatif à la nécessité de désinfecter l'infection active est envoyé au Kaspersky Security Center. Pour désinfecter l'infection active sur le serveur de fichiers, il faut activer la technologie de désinfection avancée pour les serveurs de fichiers et lancer la tâche de groupe *Recherche de virus* à l'heure qui convient le mieux aux utilisateurs des serveurs de fichiers.

Sélection des types d'objets à détecter

Pour sélectionner les types d'objets à identifier, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez la sous-section **Exclusions**.

   Les paramètres des exclusions apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Objets à détecter**.

   La fenêtre **Objets à détecter** s'ouvre.
4. Cochez les cases pour les types d'objets que Kaspersky Endpoint Security doit détecter :

   - **Outils malveillants**
   - **Applications publicitaires**
   - **Numéroteurs automatiques**
   - **Autres**
   - **Fichiers compressés qui peuvent nuire**
   - **Fichiers compressés à plusieurs reprises**
5. Cliquez sur le bouton **OK**.

La fenêtre **Objets à détecter** se ferme. Le groupe **Objets à détecter** sous l'inscription **Activation de la détection des types d'objets suivants** affichera les types d'objets que vous avez sélectionnés.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Activation et désactivation de la technologie de désinfection avancée pour les postes de travail

Pour activer ou désactiver la technologie de désinfection avancée pour les postes de travail, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.

   Les paramètres complémentaires de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :
   - Cochez la case **Appliquer la technologie de désinfection de l'infection active** si vous souhaitez activer la technologie de désinfection avancée.
   - Décochez la case **Appliquer la technologie de désinfection de l'infection active** si vous souhaitez désactiver la technologie de désinfection avancée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Lors du lancement de la désinfection de l'infection active via Kaspersky Security Center, l'utilisateur n'aura pas accès à la majorité des fonctions du système d'exploitation. Le poste de travail redémarrera une fois la tâche terminée.

Activation et désactivation de la technologie de désinfection avancée pour les serveurs de fichiers

Pour activer la technologie de désinfection avancée pour les serveurs de fichiers, réalisez une des opérations suivantes :

- Activez la technologie de désinfection avancée dans les propriétés de la stratégie active de Kaspersky Security Center. Pour ce faire, procédez comme suit :
  a. Ouvrez la section **Paramètres de l'application** de la fenêtre des propriétés de la stratégie.
  b. Cochez la case **Appliquer la technologie de désinfection de l'infection active**.
  c. Cliquez sur le bouton **OK** dans la fenêtre des propriétés de la stratégie afin d'enregistrer les modifications introduites.

- Dans les propriétés de la tâche de groupe Recherche de virus du Kaspersky Security Center, cochez la case **Exécuter la désinfection de l'infection active immédiatement**.

Pour désactiver la technologie de désinfection avancée pour les serveurs de fichiers, réalisez une des opérations suivantes :

- Désactivez la technologie de désinfection avancée dans les propriétés de la stratégie active de Kaspersky Security Center. Pour ce faire, procédez comme suit :

  a. Ouvrez la section **Paramètres de l'application** de la fenêtre des propriétés de la stratégie.

  b. Décochez la case **Appliquer la technologie de désinfection de l'infection active**.

  c. Cliquez sur le bouton **OK** dans la fenêtre des propriétés de la stratégie afin d'enregistrer les modifications introduites.

- Dans les propriétés de la tâche de groupe Recherche de virus du Kaspersky Security Center, décochez la case **Exécuter la désinfection de l'infection active immédiatement**.

Activation et désactivation du mode d'économie d'énergie

Pour activer ou désactiver le mode d'économie d'énergie, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.

   Les paramètres complémentaires de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Performance**, procédez comme suit :

   - Cochez la case **Reporter les tâches planifiées en cas d'alimentation par batterie** si vous voulez activer le mode d'économie d'énergie.

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

     - tâche de mise à jour ;
     - tâche d'analyse complète ;
     - tâche d'analyse rapide ;
     - tâche d'analyse personnalisée ;
     - tâche d'analyse de l'intégrité.

   - Décochez la case **Reporter les tâches planifiées en cas d'alimentation par batterie** si vous voulez désactiver le mode d'économie d'énergie. Dans ce cas, Kaspersky Endpoint Security exécute les tâches dont le lancement est planifiée, quelle que soit la source d'alimentation de l'application.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

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

Pour activer ou désactiver le mode de transfert des ressources vers d'autres applications, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Paramètres de l'application**.

   Les paramètres complémentaires de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Dans le groupe **Performance**, procédez comme suit :

   - Cochez la case **Céder les ressources aux autres applications** si vous voulez activer le mode de transfert des ressources vers d'autres applications.

     Si ce mode est activé, Kaspersky Endpoint Security reporte l'exécution des tâches si le lancement planifié a été défini pour ces tâches et que leur exécution ralentit le fonctionnement d'autres applications :

     - tâche de mise à jour ;
     - tâche d'analyse complète ;
     - tâche d'analyse rapide ;
     - tâche d'analyse personnalisée ;
     - tâche d'analyse de l'intégrité.
   - Décochez la case **Céder les ressources aux autres applications** si vous voulez désactiver le mode de transfert des ressources vers d'autres applications. Dans ce cas, Kaspersky Endpoint Security exécute les tâches planifiées même si d'autres applications fonctionnent.

   Le mode de transfert des ressources vers d'autres applications est activé par défaut.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Protection par mot de passe

Cette section contient les informations sur les restrictions d'accès à Kaspersky Endpoint Security à l'aide du mot de passe.

A propos des restrictions d'accès à Kaspersky Endpoint Security

Pour les versions de Kaspersky Endpoint Security 11.1.0 et suivantes, le fonctionnement de la Protection par mot de passe a changé. Kaspersky Endpoint Security 11.1.0 permet de limiter l'accès à l'application pour certains utilisateurs sans utiliser un compte utilisateur unique. Lors de la mise à jour depuis les versions antérieures de l'application, si la Protection par mot de passe est activée, Kaspersky Endpoint Security conserve le mot de passe existant. Lors de la première modification des paramètres de la Protection par mot de passe, utilisez le nom d'utilisateur KLAdmin et le mot de passe existant.

L'ordinateur peut être utilisé par plusieurs personnes dont les connaissances informatiques varient. L'accès illimité des utilisateurs à Kaspersky Endpoint Security et à ses paramètres peut entraîner une réduction du niveau de sécurité de l'ordinateur dans son ensemble. La Protection par mot de passe permet de limiter l'accès des utilisateurs à Kaspersky Endpoint Security en fonction d'autorisations octroyées (par exemple, autorisation pour quitter l'application).

La Protection par mot de passe permet d'accéder à l'application via une des méthodes suivantes.

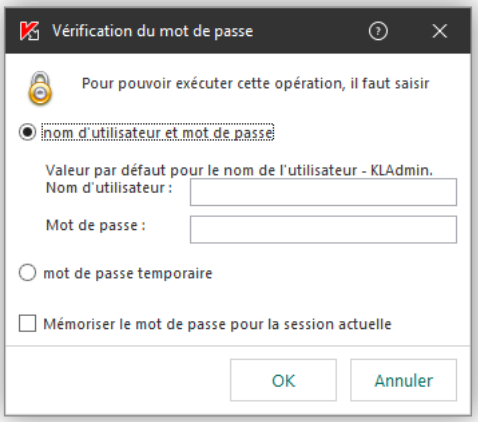
- Saisie du nom d'utilisateur et du mot de passe.

  Ce mode est pratique pour l'utilisation quotidienne. Pour exécuter une action protégée par un mot de passe, il faut saisir les données du compte utilisateur du domaine.

- Saisie d'un mot de passe temporaire.

  Cette méthode est pratique quand l'utilisateur se trouve en-dehors du réseau de l'entreprise et doit absolument obtenir un accès temporaire pour pouvoir réaliser une action interdite (par exemple, quitter l'application). A l'issue de la validité du mot de passe temporaire ou à la fin de la session, l'application rétablit les valeurs antérieures des paramètres de Kaspersky Endpoint Security.

Si l'utilisateur tente d'exécuter une action protégée par un mot de passe, Kaspersky Endpoint Security propose à l'utilisateur de saisir le nom d'utilisateur et le mot de passe ou le mot de passe temporaire (cf. ill. ci-après).



Sollicitation du mot de passe d'accès à Kaspersky Endpoint Security

Nom d'utilisateur et mot de passe

Pour pouvoir accéder à Kaspersky Endpoint Security, il faut absolument saisir les données du compte utilisateur du domaine. La Protection par mot de passe fonctionne avec les comptes utilisateur suivants :

- **KLAdmin**. Compte d'administrateur sans aucune restriction d'accès à Kaspersky Endpoint Security. Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe. Il est impossible de retirer l'autorisation pour le compte utilisateur KLAdmin. Kaspersky Endpoint Security exige la définition du mot de passe du compte utilisateur KLAdmin lors de l'activation de la Protection par mot de passe.

- **Groupe "Tous"**. Groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise. Les utilisateurs du groupe "Tous" peuvent accéder à l'application avec certaines restrictions.

- **Utilisateurs ou groupes distincts**. Comptes utilisateurs pour lesquels vous pouvez configurer des autorisations particulières. Par exemple, si une action est interdite pour le groupe "Tous", vous pouvez l'autoriser pour un utilisateur ou un groupe en particulier.

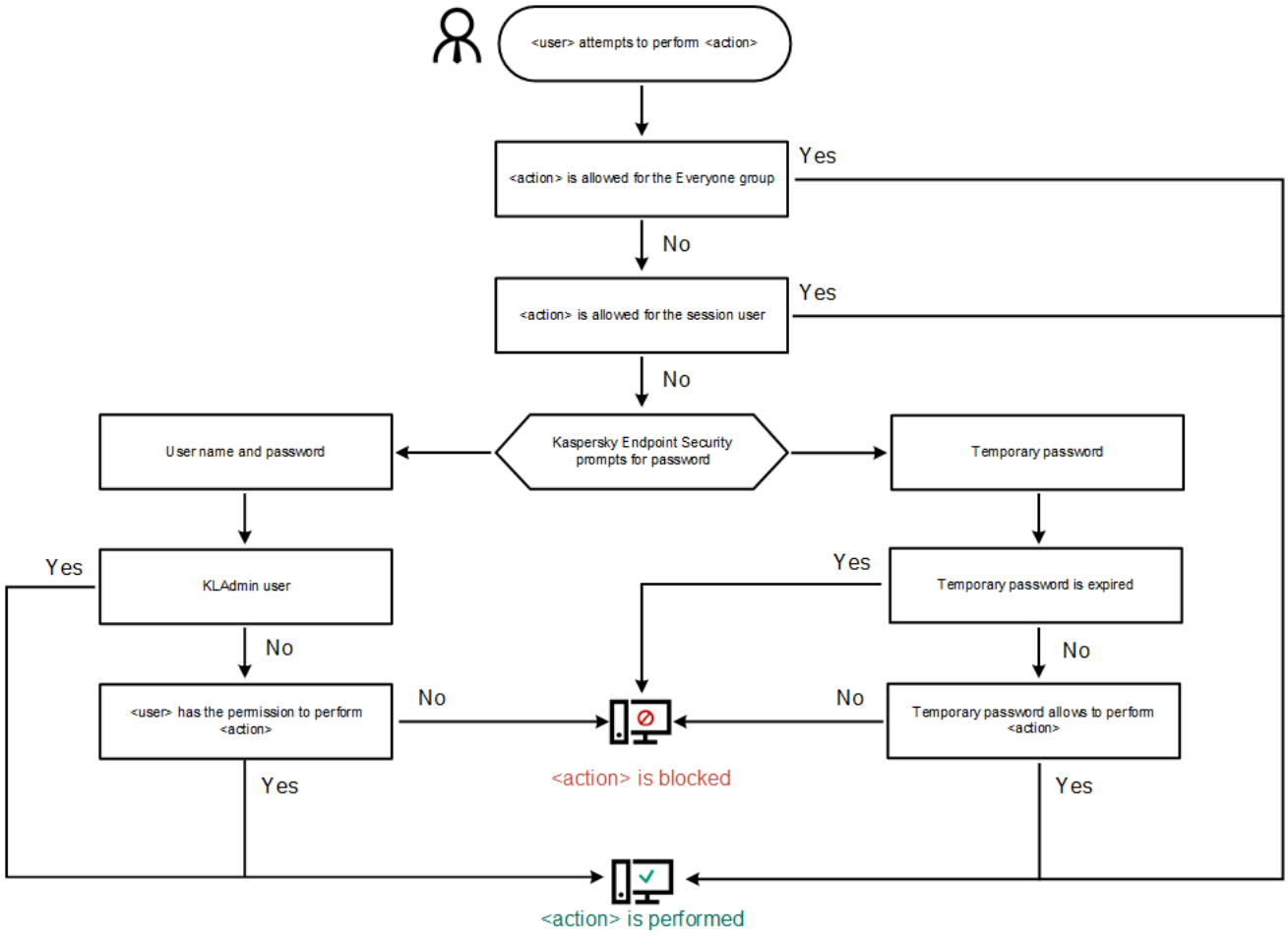
- **Utilisateur de session**. Compte de l'utilisateur qui a ouvert une session Windows. Vous pouvez changer d'utilisateur de session lors de la saisie du mot de passe (case **Mémoriser le mot de passe pour la session actuelle**). Dans ce cas, Kaspersky Endpoint Security désigne comme utilisateur de session. l'utilisateur dont vous avez saisi les identifiants au lieu de l'utilisateur qui a ouvert la session Windows.

Mot de passe temporaire

Le mot de passe temporaire permet d'octroyer un accès temporaire à Kaspersky Endpoint Security pour un ordinateur particulier hors du réseau de l'entreprise. L'administrateur crée un mot de passe temporaire pour un ordinateur distinct dans Kaspersky Security Center dans les propriétés de l'ordinateur de l'utilisateur. L'administrateur sélectionne les actions couvertes par le mot de passe temporaire, ainsi que la durée de validité de ce dernier.

Algorithme de fonctionnement de la Protection par mot de passe

Kaspersky Endpoint Security autorise ou non l'exécution d'une action protégée par mot de passe selon l'algorithme suivante (cf. ill. ci-dessous).



Algorithme de fonctionnement de la Protection par mot de passe

Activation de la Protection par mot de passe

La Protection par mot de passe permet de limiter l'accès des utilisateurs à Kaspersky Endpoint Security en fonction d'autorisations octroyées (par exemple, autorisation pour quitter l'application).

Pour activer la Protection par mot de passe, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la fenêtre des propriétés de l'application, sélectionnez la section **Paramètres généraux → Interface**.
3. Dans le groupe **Protection par mot de passe**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection par mot de passe** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cochez la case **Activer la Protection par mot de passe**.
5. Définissez le mot de passe pour le compte utilisateur KLAdmin :

   a. Dans le tableau **Autorisations**, ouvrez la liste des autorisations pour le compte utilisateur KLAdmin d'un double-clic de la souris.

   Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe.

   b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Mot de passe**.

   c. Définissez le mot de passe pour le compte utilisateur KLAdmin et confirmez-le.

   d. Cliquez sur le bouton **OK**.

   > Si l'ordinateur est administré par une stratégie, l'administrateur doit réinitialiser le mot de passe pour le compte utilisateur KLAdmin dans les propriétés de la stratégie. Si l'ordinateur n'est pas connecté à Kaspersky Security Center et si vous avez oublié le mot de passe du compte utilisateur KLAdmin, il est impossible de récupérer le mot de passe.
6. Définissez les autorisations pour tous les utilisateurs du réseau de l'entreprise.

   a. Dans le tableau **Autorisations**, ouvrez la liste des autorisations pour le groupe "Tous" d'un double-clic de la souris.

   Le *groupe "Tous"* est un groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise.

   b. Cochez la case en regard des actions que les utilisateurs pourront exécuter sans mot de passe.

   Si une case n'est pas cochée, les utilisateur ne peuvent pas réaliser cette action. Par exemple, si la case en regard de **Quitter l'application** est décochée, vous pouvez quitter l'application uniquement à l'aide du compte utilisateur KLAdmin, d'un compte utilisateur particulier possédant l'autorisation requise ou à l'aide d'un mot de passe temporaire.

   > Les autorisations de la Protection par mot de passe se caractérisent par une série de particularités. Assurez-vous que toutes les conditions sont remplies pour l'accès à Kaspersky Endpoint Security.

   c. Cliquez sur le bouton **OK**.

7. Cliquez sur le bouton **Enregistrer**.

Une fois que la Protection par mot de passe a été activée, l'application limite l'accès des utilisateurs à Kaspersky Endpoint Security conformément aux restrictions du groupe "Tous". Les actions interdites pour le groupe "Tous" peuvent être exécutées uniquement sous le compte utilisateur KLAdmin, sous un compte particulier doté des autorisations requises ou à l'aide d'un mot de passe temporaire.

Vous pouvez désactiver la protection par mot de passe uniquement avec le compte KLAdmin. Il n'est pas possible de désactiver la protection par mot de passe avec un autre compte ou avec un mot de passe temporaire.

Pendant la vérification du mot de passe, vous pouvez cocher la case **Mémoriser le mot de passe pour la session actuelle**. Dans ce cas, Kaspersky Endpoint Security n'exigera pas la saisie du mot de passe quand l'utilisateur tentera d'exécuter une autre action autorisée, protégée par un mot de passe, au cours de la session actuelle.

Octroi d'autorisations à des utilisateurs ou des groupes distincts

Vous pouvez octroyer l'accès à Kaspersky Endpoint Security à des utilisateurs ou groupes distincts. Par exemple si le groupe "Tous" ne peut pas quitter l'application, vous pouvez octroyer l'autorisation **Quitter l'application** à un utilisateur en particulier. Dès lors, il sera possible de quitter l'application uniquement sous ce compte utilisateur ou sous le compte utilisateur KLAdmin.

Vous pouvez utiliser les informations du compte utilisateur pour accéder à l'application uniquement si l'ordinateur se trouve dans le domaine. Si l'ordinateur n'est pas dans le domaine, vous pouvez utiliser un compte utilisateur KLAdmin ou un mot de passe temporaire.

Pour octroyer une autorisation à des utilisateurs ou groupes distincts, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la fenêtre des propriétés de l'application, sélectionnez la section **Paramètres généraux → Interface**.
3. Dans le groupe **Protection par mot de passe**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection par mot de passe** s'ouvre.
4. Cliquez sur le bouton **Ajouter** dans le tableau **Autorisations**.

   La fenêtre **Autorisations de l'utilisateur/du groupe** s'ouvre.
5. A droite du champ **Utilisateur/Groupe**, cliquez sur le bouton **Sélectionner**.

   La fenêtre standard de Windows pour la sélection d'utilisateurs ou de groupes s'ouvre.
6. Sélectionnez l'utilisateur ou le groupe Active Directory, puis confirmez votre choix.
7. Dans le tableau **Autorisations**, cochez la case en regard des actions que l'utilisateur ou le groupe ajouté pourra exécuter sans saisir le mot de passe.

   Si une case n'est pas cochée, les utilisateur ne peuvent pas réaliser cette action. Par exemple, si la case en regard de **Quitter l'application** est décochée, vous pouvez quitter l'application uniquement à l'aide du compte utilisateur KLAdmin, d'un compte utilisateur particulier possédant l'autorisation requise ou à l'aide d'un mot de passe temporaire.

Les autorisations de la Protection par mot de passe se caractérisent par une série de particularités. Assurez-vous que toutes les conditions sont remplies pour l'accès à Kaspersky Endpoint Security.

8. Dans la fenêtre **Autorisations de l'utilisateur/du groupe**, cliquez sur **OK**.
9. Dans la fenêtre **Protection par mot de passe**, cliquez sur **OK**.
10. Cliquez sur le bouton **Enregistrer**.

Par conséquent, si l'accès à l'application est restreint pour le groupe "Tous", les utilisateurs auront accès à Kaspersky Endpoint Security conformément aux autorisations définies pour eux.

Utilisation du mot de passe temporaire pour octroyer un accès

Le mot de passe temporaire permet d'octroyer un accès temporaire à Kaspersky Endpoint Security pour un ordinateur particulier hors du réseau de l'entreprise. Ceci s'impose pour autoriser l'exécution d'une action interdite sans transmettre à l'utilisateur les identifiants du compte KLAdmin. Pour pouvoir utiliser un mot de passe temporaire, l'ordinateur doit être ajouté à Kaspersky Security Center.

Pour permettre à un utilisateur d'exécuter une action interdite via la saisie d'un mot de passe temporaire, procédez comme suit :

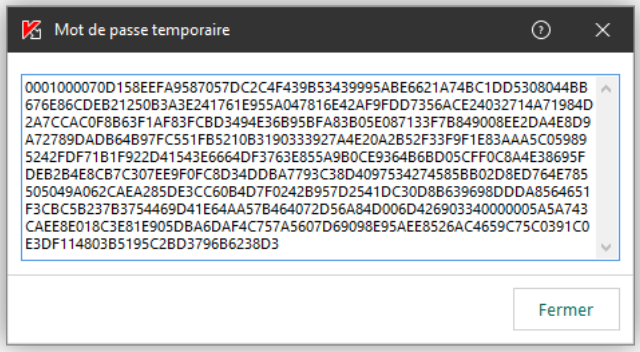
1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Ouvrez les propriétés de l'ordinateur d'un double clic.
5. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.
6. Dans la liste des applications de Kaspersky installées sur l'ordinateur, choisissez **Kaspersky Endpoint Security for Windows**, puis ouvrez les propriétés de l'application d'un double-clic.
7. Dans la fenêtre des propriétés de l'application, sélectionnez la section **Paramètres généraux → Interface**.
8. Dans le groupe **Protection par mot de passe**, cliquez sur le bouton **Configuration**.

   La fenêtre **Protection par mot de passe** s'ouvre.
9. Dans le groupe **Mot de passe temporaire**, cliquez sur le bouton **Configuration**.

   La fenêtre **Création d'un mot de passe temporaire** s'ouvre.
10. Dans le champ **Date d'expiration**, définissez la durée de validité du mot de passe temporaire.
11. Dans le tableau **Zone d'action du mot de passe temporaire**, cochez la case en regard des opérations que l'utilisateur pourra réalisé après avoir saisi le mot de passe temporaire.
12. Cliquez sur le bouton **Générer**.

    La fenêtre du mot de passe temporaire s'ouvre (cf. ill. ci-dessous).

13. Copiez et transmettez celui-ci à l'utilisateur.



Mot de passe temporaire

Particularités des autorisations de la Protection par mot de passe

Les autorisations de la Protection par mot de passe se caractérisent par une série de particularités et limites.

Configuration des paramètres de l'application

- Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs ouverts).
- Pour désactiver des modules de la protection et de contrôle dans les paramètres de l'application, l'utilisateur doit avoir les autorisations **Désactivation des modules de la protection** et **Désactivation des modules de contrôle**.
- Pour configurer les paramètres de l'application via la ligne de commande, désactivez l'autorisation **Configuration des paramètres de l'application** pour le groupe "Tous". Pour autoriser non seulement l'utilisateur KLAdmin, mais également un autre utilisateur à configurer les paramètres de l'application, ajoutez l'utilisateur ou le groupe avec l'autorisation **Configuration des paramètres de l'application** dans les paramètres de la Protection par mot de passe.

Quitter l'application

Pour arrêter l'application via le menu contextuel (option **Quitter**) ou via la ligne de commande, désactivez l'autorisation **Quitter l'application** pour le groupe "Tous". Pour autoriser non seulement l'utilisateur KLAdmin, mais également un autre utilisateur à quitter l'application, ajoutez l'utilisateur ou le groupe avec l'autorisation **Quitter l'application** dans les paramètres de la Protection par mot de passe.

Désactivation des modules de la protection

- Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs ouverts).
- Pour désactiver les modules de la protection dans les paramètres de l'application, l'utilisateur doit avoir l'autorisation **Configuration des paramètres de l'application**.

- Pour désactiver les modules de la protection via le menu contextuel (option **Suspension de la protection**), l'utilisateur doit avoir l'autorisation **Désactivation des modules de contrôle**.

- Pour désactiver les modules de la protection via la ligne de commande, désactivez les autorisations **Configuration des paramètres de l'application** et **Désactivation des modules de la protection** pour le groupe "Tous". Pour permettre aux utilisateurs autres que KLAdmin de configurer les paramètres de l'application, ajoutez un utilisateur ou un groupe disposant des autorisations **Configurer les paramètres de l'application** et **Désactiver les modules de la protection** dans les paramètres de protection par mot de passe.

Désactivation des modules de contrôle

- Si l'ordinateur de l'utilisateur est administré par une stratégie, assurez-vous que les paramètres requis dans la stratégie peuvent être modifiés (attributs ouverts).

- Pour désactiver les modules de contrôle dans les paramètres de l'application, l'utilisateur doit avoir l'autorisation **Configuration des paramètres de l'application**.

- Pour désactiver les modules de contrôle via le menu contextuel (option **Suspension de la protection**), l'utilisateur doit avoir l'autorisation **Désactivation des modules de la protection**.

- Pour désactiver les modules de contrôle via la ligne de commande, désactivez les autorisations **Configuration des paramètres de l'application** et **Désactivation des modules de contrôle** pour le groupe "Tous". Pour permettre aux utilisateurs autres que KLAdmin de configurer les paramètres d'application, ajoutez un utilisateur ou un groupe disposant des autorisations **Configurer les paramètres d'application** et **Désactiver les modules de contrôle** dans les paramètres de protection par mot de passe.

Désactivation de la stratégie de Kaspersky Security Center

Pour désactiver une stratégie de Kaspersky Security Center via le menu contextuel (option **Désactivation de la stratégie**) via la ligne de commande, désactivez l'autorisation **Désactivation de la stratégie de Kaspersky Security Center** pour le groupe "Tous". Pour autoriser la configuration des paramètres de l'application non seulement par l'utilisateur KLAdmin, mais également par un autre utilisateur, ajoutez l'utilisateur ou le groupe avec l'autorisation **Désactivation de la stratégie de Kaspersky Security Center** dans les paramètres de la Protection par mot de passe.

Suppression de la clé

Pour supprimer une clé de licence via la ligne de commande, désactivez l'autorisation **Suppression de la clé** pour le groupe "Tous". Pour permettre à des utilisateurs autres que KLAdmin de supprimer une clé de licence, ajoutez un utilisateur ou un groupe disposant de l'autorisation **Supprimer la clé** dans les paramètres de protection par mot de passe.

Suppression / modification / réparation de l'application

Le compte utilisateur KLAdmin est le seul autorisé à supprimer, modifier ou réparer l'application. Il est impossible de permettre à un autre utilisateur d'exécuter ces actions.

Restauration de l'accès aux données sur les appareils chiffrés

Le compte utilisateur KLAdmin est le seul qui peut restaurer l'accès aux données sur les appareils chiffrés. Il est impossible de permettre à un autre utilisateur d'exécuter cette action.

Consultation des rapports

Il n'y a aucune particularité ou restriction.

Restauration depuis la Sauvegarde

Pour restaurer un fichiers depuis la sauvegarde via la ligne de commande, désactivez l'autorisation **Restauration depuis la Sauvegarde** pour le groupe "Tous" Pour permettre aux utilisateurs autres que KLAdmin de restaurer à partir de la Sauvegarde, ajoutez un utilisateur ou un groupe disposant de l'autorisation **Restaurer à partir de la Sauvegarde** dans les paramètres de protection par mot de passe.

Création et utilisation d'un fichier de configuration

Le fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Endpoint Security permet de réaliser les tâches suivantes :

- Exécuter l'installation locale de Kaspersky Endpoint Security via la ligne de commande selon des paramètres définis à l'avance.

  Pour cela, il faut enregistrer le fichier de configuration dans le même dossier que celui où se trouve le paquet de distribution.

- Exécuter l'installation à distance de Kaspersky Endpoint Security via Kaspersky Security Center avec selon des paramètres définis à l'avance.

- Transférer les paramètres de fonctionnement de Kaspersky Endpoint Security d'un ordinateur à l'autre.

Pour créer un fichier de configuration, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Administration des paramètres**.

   Les fonctions d'administration des paramètres s'affichent dans la partie droite de la fenêtre.
3. Dans le groupe **Administration des paramètres**, cliquez sur le bouton **Enregistrer**.

   La fenêtre standard de Microsoft Windows **Sélection du fichier de configuration** s'ouvre.
4. Indiquez le chemin où vous voulez enregistrer le fichier de configuration et saisissez son nom.

   > Pour utiliser le fichier de configuration dans le cadre d'une installation locale ou à distance de Kaspersky Endpoint Security, il faut le nommer install.cfg.

5. Cliquez sur le bouton **Enregistrer**.

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

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans la section **Paramètres généraux** de la partie gauche de la fenêtre, sélectionnez **Administration des paramètres**.

Les fonctions d'administration des paramètres s'affichent dans la partie droite de la fenêtre.

3. Dans le groupe **Administration des paramètres**, cliquez sur le bouton **Télécharger**.

   La fenêtre standard de Microsoft Windows **Sélection du fichier de configuration** s'ouvre.

4. Indiquez le chemin d'accès au fichier de configuration.

5. Cliquez sur le bouton **Ouvrir**.

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

Administration de l'application via la Console d'administration Kaspersky Security Center

Cette section présente l'administration à distance de Kaspersky Endpoint Security via Kaspersky Security Center.

Présentation de l'administration de l'application via Kaspersky Security Center

Kaspersky Security Center permet d'installer, de supprimer, de lancer et d'arrêter Kaspersky Endpoint Security à distance, de configurer les paramètres de fonctionnement de l'application, de modifier la sélection des modules, d'ajouter des clés et de lancer et d'arrêter les tâches de mise à jour et d'analyse.

La section sur le Contrôle des applications présente les informations sur l'administration des règles de contrôle des applications à l'aide de Kaspersky Security Center.

Pour en savoir plus sur l'administration de l'application via Kaspersky Security Center, *consultez l'aide de Kaspersky Security Center*.

L'administration de l'application via Kaspersky Security Center s'opère à l'aide du plug-in d'administration Kaspersky Endpoint Security.

La version du plug-in d'administration peut différer de la version de Kaspersky Endpoint Security installée sur l'ordinateur client. Si la version installée du plug-in d'administration prévoit moins de fonctions que dans la version installée de Kaspersky Endpoint Security, les paramètres des fonctions manquantes ne sont pas régis par le plug-in d'administration. Ces paramètres peuvent être modifiés par l'utilisateur dans l'interface locale de Kaspersky Endpoint Security.

Lancement et arrêt de Kaspersky Endpoint Security sur un ordinateur client

Pour démarrer ou arrêter l'application sur l'ordinateur client, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sélectionnez l'ordinateur sur lequel vous souhaitez lancer ou arrêter l'application.
5. Cliquez-droit pour ouvrir le menu contextuel de l'ordinateur client, puis choisissez l'option **Propriétés**.

   La fenêtre des propriétés du poste client s'ouvre.
6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.

   Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky installées sur le poste client.

7. Choisissez l'application Kaspersky Endpoint Security.

8. Procédez comme suit :

   - Si vous souhaitez démarrer l'application, cliquez sur le bouton à droite de la liste des applications Kaspersky ou procédez comme suit :

     a. Choisissez l'option **Propriétés** dans le menu contextuel de l'application Kaspersky Endpoint Security ou cliquez sur le bouton **Propriétés** situé sous la liste des applications de Kaspersky.

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

     b. Dans la section **Général**, cliquez sur le bouton **Démarrer** dans la partie droite de la fenêtre.

   - Si vous souhaitez arrêter l'application, cliquez sur le bouton à droite de la liste des applications Kaspersky ou procédez comme suit :

     a. Choisissez l'option **Propriétés** dans le menu contextuel de l'application Kaspersky Endpoint Security ou cliquez sur le bouton **Propriétés** situé sous la liste des applications de Kaspersky.

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

     b. Dans la section **Général**, cliquez sur le bouton **Arrêter** dans la partie droite de la fenêtre.

Configuration des paramètres de Kaspersky Endpoint Security

Pour configurer les paramètres de Kaspersky Endpoint Security, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.

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

4. Choisissez l'ordinateur pour lequel vous souhaitez configurer les paramètres de Kaspersky Endpoint Security.

5. Dans le menu contextuel de l'ordinateur client, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du poste client s'ouvre.

6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.

   Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky installées sur le poste client.

7. Choisissez l'application Kaspersky Endpoint Security.

8. Exécutez une des actions suivantes :

   - Dans le menu contextuel de l'application Kaspersky Endpoint Security, choisissez l'option **Propriétés**.

   - Cliquez sur le bouton **Propriétés** sous la liste des applications de Kaspersky.

   La fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows** s'ouvre.

9. Dans la section **Paramètres généraux**, configurez les paramètres de fonctionnement de Kaspersky Endpoint Security, ainsi que les paramètres des rapports et des stockages.

   Les autres sections de la fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows** sont les mêmes que les sections standards de Kaspersky Security Center. Elles sont décrites en détail dans l'aide de Kaspersky Security Center.

   Si l'application est soumise à une stratégie qui interdit la modification de certains paramètres, ceux-ci ne seront pas accessibles lors de la configuration des paramètres de l'application dans la section **Paramètres généraux**.

10. Dans la fenêtre **Paramètres de l'application Kaspersky Endpoint Security for Windows**, cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Particularités de l'utilisation de plug-ins d'administration de différentes versions

Le plug-in d'administration permet de modifier les éléments suivants :

- les stratégies ;
- les profils de stratégie ;
- les tâches de groupe ;
- les tâches locales ;
- les paramètres locaux de l'application Kaspersky Endpoint Security.

Pour administrer l'application Kaspersky Endpoint Security via Kaspersky Security Center, il faut disposer d'un plug-in d'administration d'une version égale ou supérieure à celle indiquée dans les informations de compatibilité de Kaspersky Endpoint Security avec le plug-in d'administration. Vous pouvez regarder la version minimale requise du plug-in d'administration dans le fichier installer.ini qui fait partie de la distribution.

À l'ouverture de n'importe quel élément (par exemple, une stratégie ou une tâche), le plug-in d'administration vérifie les informations sur la compatibilité. Si la version du plug-in d'administration est égale ou supérieure à la version indiquée dans les informations sur la compatibilité, vous pouvez modifier les paramètres de cet élément. Dans le cas contraire, la modification des paramètres de l'élément sélectionné via le plug-in d'administration est inaccessible. Il est recommandé de mettre à jour le plug-in d'administration.

Mise à jour du plug-in d'administration de Kaspersky Endpoint Security 10 for Windows

Si le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows est installé dans la Console d'administration, l'installation du plug-in d'administration pour Kaspersky Endpoint Security 11 for Windows possède les particularités suivantes :

- Le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows n'est pas supprimé et peut toujours être utilisé.

- Le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows ne prend pas en charge l'administration de l'application Kaspersky Endpoint Security 10 for Windows sur les ordinateurs des utilisateurs.
- Le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows ne prend pas en charge les éléments (par exemple, une stratégie ou une tâche), créés à l'aide du plug-in d'administration Kaspersky Endpoint Security 10 for Windows.

  Si vous avez supprimé le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows et installé le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows, vous devez créer de nouvelles stratégies, tâches, etc. Vous pouvez également installer le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows avec le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows réaliser une migration. Après l'exécution de la migration, supprimez le plug-in d'administration de Kaspersky Endpoint Security 10 for Windows.

Mise à jour du plug-in d'administration de Kaspersky Endpoint Security 11 for Windows

Si le plug-in d'administration de Kaspersky Endpoint Security 11 for Windows est installé dans la Console d'administration, l'installation de la nouvelle version du plug-in d'administration pour Kaspersky Endpoint Security 11 for Windows possède les particularités suivantes :

- La version précédente du plug-in d'administration de Kaspersky Endpoint Security 11 for Windows est supprimée.
- Le plug-in d'administration de Kaspersky Endpoint Security 11 pour Windows d'une nouvelle version prend en charge l'administration de l'application Kaspersky Endpoint Security 11 for Windows de la version antérieure sur les ordinateurs des utilisateurs.
- Grâce au plug-in d'administration de la nouvelle version, vous pouvez modifier les paramètres dans les stratégies, les tâches etc., créée par le plug-in d'administration de la version antérieure.
- Pour les nouveaux paramètres, le plug-in d'administration de la nouvelle version définit les valeurs par défaut lors du premier enregistrement d'une stratégie, d'un profil de stratégie ou d'une tâche.

  Après la mise à jour du plug-in d'administration, il est conseillé de vérifier et d'enregistrer les valeurs des nouveaux paramètres dans les stratégies et les profils de stratégie. Dans le cas contraire, les nouveaux groupes de paramètres de Kaspersky Endpoint Security sur l'ordinateur de l'utilisateur prendront les valeurs par défaut et pourront être modifiés (attribut). Il est conseillé de débuter le contrôle par les stratégies et les profils de stratégie du niveau supérieur de la hiérarchie. Il est également recommandé d'utiliser le compte utilisateur autorisé à accéder à toutes les zones fonctionnelles Kaspersky Security Center.

  Pour en savoir plus sur les nouvelles fonctions de l'application, consultez les Notes de version ou l'aide de l'application.

- Si un nouveau paramètre a été ajouté à un groupe de paramètres dans la nouvelle version du plug-in d'administration, l'attribut / affecté antérieurement à ce groupe ne change pas.

Gestion de la tâche

Cette section fournit des informations sur la gestion des tâches pour Kaspersky Endpoint Security. Pour en savoir plus sur le concept de gestion des tâches via Kaspersky Security Center, *consultez l'aide de Kaspersky Security Center*.

A propos des tâches pour Kaspersky Endpoint Security

Kaspersky Security Center utilise des tâches pour gérer le fonctionnement des applications de Kaspersky installées sur les postes client. Les tâches prennent en charge les principales fonctions de gestion telles que l'ajout d'une clé, l'analyse de l'ordinateur ou la mise à jour des bases de données et des modules de l'application.

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration ;
- des tâches pour des sélections d'ordinateurs qui n'appartiennent pas à des groupes d'administration.

  Les tâches pour les sélections d'ordinateurs qui n'appartiennent pas à des groupes d'administration sont exécutées uniquement pour les postes clients définis dans les paramètres de la tâche. Si de nouveaux postes clients sont ajoutés à une sélection d'ordinateurs pour laquelle une tâche a été créée, cette tâche ne s'applique pas à ces nouveaux postes. Dans ce cas, il faut créer une tâche ou modifier les paramètres de la tâche existante.

Dans le cadre de l'administration à distance de Kaspersky Endpoint Security, vous pouvez utiliser les tâches suivantes de n'importe quel type :

- **Ajout d'une clé**. Kaspersky Endpoint ajoute une clé, dont une clé complémentaire, pour activer l'application.
- **Modification de la sélection des modules de l'application**. Kaspersky Endpoint Security installe ou supprime les modules sur les ordinateurs client selon la liste des modules indiquée dans les paramètres de la tâche.
- **Inventaire**. Kaspersky Endpoint Security récupère des informations sur tous les fichiers exécutables des applications de l'ordinateur.

  Vous pouvez activez l'inventaire des modules DLL et des fichiers de scripts. Dans ce cas Kaspersky Security Center recevra les informations relatives aux modules DLL chargés sur l'ordinateur avec l'application installée Kaspersky Endpoint Security, ainsi que les renseignements relatifs aux fichiers contenant les scripts.

  L'activation de l'inventaire des modules DLL et des fichiers de script augmente considérablement la durée d'exécution de la tâche d'inventaire et la taille de la base de données.

  Si le module Contrôle des applications n'est pas installé sur l'ordinateur doté de Kaspersky Endpoint Security, la tâche d'inventaire sur cet ordinateur se solde sur une erreur.

- **Mise à jour**. Kaspersky Endpoint Security actualise les bases et les modules de l'application conformément aux paramètres de mise à jour définis.

- **Restauration de la dernière mise à jour**. Kaspersky Endpoint Security annule la dernière mise à jour des bases de données et des modules.
- **Recherche de virus**. Kaspersky Endpoint Security recherche la présence éventuelle de virus et d'autres programmes dangereux dans les secteurs de l'ordinateur définis via les paramètres de la tâche.
- **Vérification de l'intégrité**. Kaspersky Endpoint Security reçoit les données sur la composition des modules de l'application installés sur l'ordinateur client et vérifie la signature numérique de chacun des modules.
- **Administration des comptes utilisateur de l'Agent d'authentification**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security crée des commandes de suppression, d'ajout ou de modification des comptes utilisateur de l'Agent d'authentification.

Vous pouvez réaliser les opérations suivantes sur les tâches :

- lancer, arrêter, suspendre ou reprendre l'exécution de la tâche ;
- créer des tâches ;
- modifier les paramètres des tâches.

Les autorisations d'accès aux paramètres des tâches de Kaspersky Endpoint Security (lecture, modification, exécution) sont définies pour chaque utilisateur qui a accès au Serveur d'administration de Kaspersky Security Center via les paramètres d'accès aux zones de fonction de Kaspersky Endpoint Security. Pour configurer l'accès aux zones de fonction de Kaspersky Endpoint Security, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration de Kaspersky Security Center.

Configuration du mode d'utilisation des tâches

Pour configurer le mode d'utilisation des tâches dans l'interface locale de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez configurer le mode d'utilisation des tâches dans l'interface locale de Kaspersky Endpoint Security.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.
6. Dans la section **Tâches locales**, choisissez la sous-section **Gestion de la tâche**.
7. Dans le groupe **Gestion de la tâche**, procédez comme suit :
   - Si vous voulez permettre aux utilisateurs d'utiliser les tâches locales dans l'interface et via la ligne de commande de Kaspersky Endpoint Security, cochez la case **Autoriser l'utilisation des tâches locales**.

Si la case est décochée, le fonctionnement des tâches locales est interrompu. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. De même, les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de l'application ou via la ligne de commande.

- Si vous voulez permettre aux utilisateurs de consulter la liste des tâches de groupe, cochez la case **Autoriser l'affichage des tâches de groupe**.
- Si vous voulez permettre aux utilisateurs de modifier les paramètres des tâches de groupe, cochez la case **Autoriser la gestion des tâches de groupe**.

8. Cliquez sur **OK** pour enregistrer les modifications.
9. Appliquez la stratégie.

   Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Création d'une tâche locale

Pour créer une tâche locale, procédez comme suit:

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sélectionnez l'ordinateur pour lequel vous souhaitez créer une tâche locale.
5. Exécutez une des actions suivantes :
   - Dans le menu contextuel de l'ordinateur client, choisissez l'option **Toutes les tâches → Créer une tâche**.
   - Dans le menu contextuel de l'ordinateur client, choisissez l'option **Propriétés** et dans la fenêtre **Propriétés : <nom de l'ordinateur>** qui s'ouvre, cliquez sur le bouton **Ajouter** de l'onglet **Tâches**.
   - Dans la liste déroulante **Exécuter l'action**, choisissez l'option **Créer une tâche**.

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

Création d'une tâche de groupe

Pour créer une tâche de groupe, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :

- Sélectionnez le dossier **Appareils administrés** de l'arborescence de la Console d'administration si vous souhaitez créer une stratégie de groupe pour tous les ordinateurs administrés par Kaspersky Security Center.

- Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients qui vous intéressent.

3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

4. Cliquez sur le bouton **Créer une tâche**.

   L'Assistant de création de tâche démarre.

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

Création d'une tâche pour une sélection d'appareils

Pour créer une tâche pour une sélection d'appareils, procédez comme suit :

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

2. Choisissez le dossier **Tâches** dans l'arborescence de la Console de l'administration.

3. Cliquez sur le bouton **Créer une tâche**.

   L'Assistant de création de tâche démarre.

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

Lancement, arrêt, suspension et reprise de l'exécution d'une tâche

Si l'application Kaspersky Endpoint Security est lancée, vous pouvez lancer/arrêter/suspendre/reprendre l'exécution de la tâche sur cet ordinateur client via Kaspersky Security Center. Si Kaspersky Endpoint Security est arrêté, les tâches en cours d'exécution sont arrêtées et il n'est plus possible de gérer le lancement, l'arrêt, la suspension et la reprise des tâches via Kaspersky Security Center.

Pour lancer, arrêter, suspendre ou reprendre l'exécution d'une tâche locale, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.

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

4. Sélectionnez l'ordinateur client sur lequel vous souhaitez lancer, arrêter, suspendre ou reprendre une tâche locale.

5. Cliquez-droit pour ouvrir le menu contextuel de l'ordinateur client, puis choisissez l'option **Propriétés**.

   La fenêtre des propriétés du poste client s'ouvre.

6. Choisissez la section **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.

7. Sélectionnez la tâche locale que vous voulez lancer, arrêter, suspendre ou reprendre.

8. Exécutez l'action requise pour la tâche à l'aide d'une des méthodes suivantes :

   - Ouvrez le menu contextuel de la tâche locale d'un clic droit et choisissez l'option **Démarrer** / **Arrêter** / **Suspendre** / **Reprendre**.

   - Cliquez sur le bouton / à droite de la liste des tâches locales afin de lancer ou d'arrêter une tâche locale.

   - Procédez comme suit :

     a. Cliquez sur le bouton **Propriétés** sous la liste des tâches locales ou choisissez l'option **Propriétés** dans le menu contextuel de la tâche.

        La fenêtre **Propriétés <nom de la tâche>** s'ouvre.

     b. Sous l'onglet **Général**, cliquez sur le bouton **Démarrer** / **Arrêter**/ **Suspendre** / **Reprendre**.

Pour lancer, arrêter, suspendre ou reprendre une tâche de groupe, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez lancer/arrêter/suspendre/reprendre l'exécution d'une tâche de groupe.

3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

   Les tâches de groupe s'affichent dans la partie droite de la fenêtre.

4. Sélectionnez la tâche de groupe que vous voulez lancer, arrêter, suspendre ou reprendre.

5. Exécutez l'action requise pour la tâche à l'aide d'une des méthodes suivantes :

   - Dans le menu contextuel de la tâche de groupe, sélectionnez l'option **Démarrer** / **Arrêter** / **Suspendre** / **Reprendre**.

   - Cliquez sur le bouton / dans la partie droite de la fenêtre afin de lancer ou d'arrêter la tâche de groupe.

   - Procédez comme suit :

     a. Cliquez sur le lien **Modifier les paramètres de la tâche** dans la partie droite de l'espace de travail de la Console d'administration ou choisissez l'option **Propriétés** dans le menu contextuel de la tâche.

        La fenêtre **Propriétés <nom de la tâche>** s'ouvre.

     b. Sous l'onglet **Général**, cliquez sur le bouton **Démarrer** / **Arrêter**/ **Suspendre** / **Reprendre**.

Pour lancer, arrêter, suspendre ou reprendre l'exécution d'une tâche pour une sélection d'ordinateurs, procédez comme suit :

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

2. Dans le dossier **Tâches** de l'arborescence de la Console d'administration, sélectionnez la tâche pour la sélection d'ordinateurs que vous souhaitez lancer, arrêter, suspendre ou reprendre.

3. Exécutez une des actions suivantes :

   - Dans le menu contextuel de la tâche, choisissez l'option **Démarrer** / **Arrêter** / **Suspendre** / **Reprendre**.
   - Cliquez sur le bouton / dans la partie droite de la fenêtre pour lancer ou arrêter la tâche pour une sélection d'ordinateurs.
   - Procédez comme suit :

     a. Cliquez sur le lien **Modifier les paramètres de la tâche** dans la partie droite de l'espace de travail de la Console d'administration ou choisissez l'option **Propriétés** dans le menu contextuel de la tâche.

     La fenêtre **Propriétés <nom de la tâche>** s'ouvre.

     b. Sous l'onglet **Général**, cliquez sur le bouton **Démarrer** / **Arrêter**/ **Suspendre** / **Reprendre**.

Modification des paramètres de la tâche

Pour modifier les paramètres d'une tâche locale, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sélectionnez l'ordinateur pour lequel vous souhaitez configurer les paramètres de l'application.
5. Cliquez-droit pour ouvrir le menu contextuel de l'ordinateur client, puis choisissez l'option **Propriétés**.

   La fenêtre des propriétés du poste client s'ouvre.
6. Choisissez la section **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.
7. Sélectionnez la tâche locale souhaitée dans la liste.
8. Cliquez sur le bouton **Propriétés**.

   La fenêtre **Propriétés** : **<nom de la tâche locale>** s'ouvre.
9. Pour enregistrer les modifications, dans la fenêtre **Propriétés : <nom de la tâche locale>**, choisissez la section **Paramètres**.
10. Modifiez les paramètres de la tâche locale.
11. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la tâche locale>**, cliquez sur **OK**.
12. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de l'ordinateur>**, cliquez sur **OK**.

Pour modifier les paramètres d'une tâche de groupe, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés**, ouvrez le dossier portant le nom du groupe d'administration souhaité.
3. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

   Les tâches de groupe apparaissent dans l'espace de travail de la Console d'administration.
4. Choisissez la tâche de groupe requise.
5. Cliquez-droit pour ouvrir le menu contextuel de la tâche de groupe, puis choisissez l'option **Propriétés**.

   La fenêtre **Propriétés** : **<nom de la tâche de groupe>** s'ouvre.
6. Pour enregistrer les modifications, dans la fenêtre **Propriétés : <nom de la tâche de groupe>**, choisissez la section **Paramètres**.
7. Modifiez les paramètres de la tâche de groupe.
8. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la tâche de groupe>**, cliquez sur **OK**.

Pour modifier les paramètres de la tâche pour une sélection d'ordinateurs, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Tâches** de l'arborescence de la Console d'administration, sélectionnez la tâche pour la sélection d'ordinateurs dont vous souhaitez modifier les paramètres.
3. Cliquez-droit pour ouvrir le menu contextuel de la tâche de sélection d'ordinateurs, puis choisissez l'option **Propriétés**.

   La fenêtre **Propriétés : <nom de la tâche pour la sélection d'ordinateurs>** s'ouvre.
4. Dans la fenêtre **Propriétés : <nom de la tâche pour une sélection d'ordinateurs>**, sélectionnez la section **Paramètres**.
5. Modifiez les paramètres de la tâche pour la sélection d'ordinateurs.
6. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la tâche pour la sélection des ordinateurs>**, cliquez sur **OK**.

Toutes les sections de la fenêtre des propriétés des tâches, à l'exception de la section **Paramètres**, sont standard pour Kaspersky Security Center. Elles sont décrites en détail dans l'aide de Kaspersky Security Center. La section **Paramètres** contient les paramètres propres à Kaspersky Endpoint Security for Windows. Son contenu dépend de la tâche choisie et de son type.

Paramètres de la tâche d'inventaire

Kaspersky Endpoint Security ne réalise pas l'inventaire des fichiers dont le contenu se trouve dans le stockage Cloud OneDrive.

Vous pouvez configurer les paramètres suivants pour la tâche d'inventaire :

- **Zone d'inventaire**. Ce groupe vous permet de désigner les objets du système de fichiers qui vont être analysés lors de l'inventaire. Ces objets peuvent être des dossiers locaux et réseaux, des disques durs et amovibles ou

l'ensemble de l'ordinateur.

- **Paramètres de la tâche d'inventaire**. Ce groupe permet de configurer les paramètres suivants :
  - **Activer l'analyse de l'ordinateur lorsque celui-ci est inactif**. La case active/désactive la suspension de la tâche d'inventaire si les ressources de l'ordinateur sont occupées. Kaspersky Endpoint Security suspend la tâche d'inventaire si l'ordinateur est déverrouillé.
  - **Inventaire des modules DLL**. La case active/désactive la fonction qui analyse les données sur les modules DLL et transmet les résultats de l'analyse au Serveur d'administration.
  - **Inventaire des fichiers de scripts**. La case active/désactive la fonction qui analyse les données sur les fichiers contenant des scripts et transmet les résultats de l'analyse au Serveur d'administration.
  - **Avancé**. Ce bouton ouvre la fenêtre **Paramètres complémentaires** qui permet de configurer les paramètres suivants :
    - **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. La case active/désactive le mode d'analyse seulement des nouveaux fichiers et de ceux qui ont été modifiés depuis le dernier inventaire.
    - **Ignorer les fichiers si l'analyse dure plus de**. La case active/désactive la restriction de la durée d'analyse d'un fichier. A l'issue du temps indiqué dans le champ de droite, Kaspersky Endpoint Security termine l'analyse du fichier.
    - **Analyser les archives**. La case active/désactive l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE à la recherche de fichiers exécutables.
    - **Analyser les paquets de distribution**. La case active ou désactive l'analyse des paquets de distribution pendant la tâche d'inventaire.
    - **Ne pas décompresser les fichiers composés de grande taille**.

      Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie dans le champ **Taille maximale du fichier**.

      Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille.

      > Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

    - **Taille maximale du fichier**. Kaspersky Endpoint Security suspend uniquement la décompression des fichiers dont la taille dépasse la valeur définie dans ce champ. La valeur est exprimée en mégaoctets.

Administration des stratégies

Cette section explique la création et la configuration des stratégies pour Kaspersky Endpoint Security. Pour en savoir plus sur le concept de gestion des stratégies via l'application Kaspersky Endpoint Security et les stratégies de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

A propos des stratégies

Les stratégies permettent de définir des valeurs identiques pour les paramètres de fonctionnement de Kaspersky Endpoint Security sur tous les postes clients appartenant au groupe d'administration.

Vous pouvez modifier localement la valeur des paramètres définis par la stratégie pour certains ordinateurs du groupe d'administration à l'aide de Kaspersky Endpoint Security. Vous pouvez modifier localement uniquement les paramètres dont la modification n'est pas interdite par la stratégie.

La possibilité de modifier les paramètres de l'application sur l'ordinateur client est déterminée par l'état du "cadenas" associé à ces paramètres dans les propriétés de la stratégie :

- Un cadenas fermé (🔒) signifie :
  - Kaspersky Security Center interdit la modification des valeurs des paramètres associés à ce cadenas depuis l'interface de Kaspersky Endpoint Security sur les ordinateurs client. Kaspersky Endpoint Security utilise des valeurs de paramètres identiques sur tous les ordinateurs client, à savoir celles définies dans les propriétés de la stratégie.
  - Kaspersky Security Center interdit la modification des paramètres associés à ce cadenas dans les propriétés des stratégies pour les sous-groupes d'administration et les Serveurs d'administration secondaires dans lesquelles la fonction **Hériter des paramètres de la stratégie parent** est activée. Les valeurs utilisées pour ces paramètres sont les valeurs définies dans les propriétés de la stratégie de niveau supérieur de la hiérarchie.
- Un cadenas ouvert (🔓) signifie :
  - Kaspersky Security Center autorise la modification des paramètres associés à ces paramètres depuis l'interface de Kaspersky Endpoint Security sur les ordinateurs client. Sur chaque ordinateur client, Kaspersky Endpoint Security fonctionne selon la valeur locale des paramètres, si le module est activé.
  - Kaspersky Security Center autorise la modification des paramètres associés à ce cadenas dans les propriétés des stratégies pour les sous-groupes d'administration et les Serveurs d'administration secondaires dans lesquelles la fonction **Hériter des paramètres de la stratégie parent** est activée. Les valeurs de ces paramètres ne dépendent pas de ce qui figure dans les propriétés de la stratégie de niveau supérieur de la hiérarchie.

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

Les autorisations d'accès aux paramètres de la stratégie (lecture, modification, exécution) sont définies pour chaque utilisateur qui a accès au Serveur d'administration de Kaspersky Security Center, et séparément pour chaque zone de fonction de Kaspersky Endpoint Security. Pour configurer les autorisations d'accès aux paramètres de la stratégie, accédez à la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration de Kaspersky Security Center.

Kaspersky Endpoint Security possède les zones de fonction suivantes :

- Protection principale. Zone de fonctions qui reprend les modules Protection contre les fichiers malicieux, Protection contre les menaces par emails, Protection contre les menaces Internet, Protection contre les menaces réseau, Pare-feu et tâches d'analyse.
- Contrôle des applications. Cette zone reprend le module Contrôle des applications.
- Contrôle des périphériques. Cette zone reprend le module Contrôle des périphériques.
- Chiffrement. Cette zone reprend les modules Chiffrement du disque, Chiffrement des fichiers.
- Zone de confiance. Cette zone reprend la zone de confiance.

- Contrôle Internet. Cette zone reprend le module Contrôle Internet.
- Protection avancée. Zone de fonctions qui reprend les paramètres du KSN et les modules Détection comportementale, Protection contre les Exploits, Prévention des intrusions et Réparation des actions malicieuses.
- Fonction de base. Cette zone reprend les paramètres généraux de l'application qui ne figurent pas dans les autres zones comme la licence, la tâche d'inventaire et de mise à jour des bases et des modules de l'application, l'auto-défense, les paramètres complémentaires de l'application, les rapports et les stockages, les paramètres de protection par mot de passe et de l'interface de l'application.

Vous pouvez réaliser les opérations suivantes sur les stratégies :

- 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 zones de fonction distincte, les paramètres de ces zones ne sont pas accessibles en vue d'une modification.

- supprimer une stratégie ;
- modifier l'état d'une stratégie.

Les informations relatives aux stratégies qui ne concernent pas l'interaction avec Kaspersky Endpoint Security sont reprises dans l'aide de Kaspersky Security Center.

Création d'une stratégie

Pour créer une stratégie, procédez comme suit:

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Exécutez une des actions suivantes :
   - Sélectionnez le dossier **Appareils administrés** de l'arborescence de la Console d'administration si vous souhaitez créer une stratégie pour tous les ordinateurs administrés par Kaspersky Security Center.
   - Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients qui vous intéressent.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Nouvelle stratégie**.
   - Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Générer → Stratégie**.

   L'Assistant de création de la stratégie démarre.

5. Suivez les instructions de l'Assistant de création de stratégie.

Modification des paramètres de la stratégie

Pour modifier les paramètres de la stratégie, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez modifier les paramètres de la stratégie.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.

   Les paramètres de la stratégie pour Kaspersky Endpoint Security comprennent les paramètres des modules et les paramètres de l'application. Les sections **Protection avancée**, **Protection principale** et **Contrôles de sécurité** de la fenêtre **Propriétés : <Nom de la stratégie>** reprennent les paramètres des modules de protection et de contrôle, la section **Chiffrement des données** contient les paramètres de chiffrement du disque, de chiffrement des fichiers, de chiffrement des disques amovibles, la section **Endpoint Sensor** reprend les paramètres du module Endpoint Sensor, la section **Tâches locales** reprend les paramètres des tâches locales et de groupe et la section **Paramètres généraux** reprend les paramètres de l'application.

   Les paramètres du chiffrement des données et des modules de contrôle s'affichent dans les paramètres de la stratégie si les cases correspondantes ont été cochées dans la fenêtre **Configuration de l'interface** de Kaspersky Security Center. Ces cases sont cochées par défaut.
6. Modifiez les paramètres de la stratégie.
7. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.

Indicateur du niveau de protection dans la fenêtre des propriétés de la stratégie

L'indicateur du niveau de protection apparaît dans la partie supérieure de la fenêtre **Propriétés : <Nom de la stratégie>**. L'indicateur peut prendre une des valeurs suivantes :

- **Niveau de protection élevé**. L'indicateur prend cette valeur et devient vert si tous les composants des catégories suivantes sont activés :
  - **Critiques**. Cette catégorie contient les composants suivants :
    - Protection contre les fichiers malicieux.
    - Détection comportementale.

- Protection contre les Exploits.
- Réparation des actions malicieuses.

- **Importants**. Cette catégorie contient les composants suivants :
  - Kaspersky Security Network.
  - Protection contre les menaces Internet.
  - Protection contre les menaces par emails.
  - Prévention des intrusions.

- **Niveau de protection moyen**. L'indicateur prend cette valeur et devient jaune si un composant important est désactivé.
- **Niveau de protection faible**. L'indicateur prend cette valeur et devient rouge dans un des cas suivants :
  - un ou plusieurs composants critiques sont désactivés ;
  - deux ou plusieurs composants importants sont désactivés.

Si l'indicateur s'affiche avec la valeur **Niveau de protection moyen** ou **Niveau de protection faible**, le lien **Plus d'informations** apparaît à droite de l'indicateur. Ce lien permet d'ouvrir la fenêtre **Modules de protection recommandés**. Cette fenêtre permet d'activer n'importe quel module de protection recommandé.

Configuration de l'affichage de l'interface de l'application

Pour configurer l'affichage de la mise à jour de l'application, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez configurer l'affichage de l'interface de l'application.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre **Propriétés** : **<Nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.
   - Cliquez sur lien **Modifier les paramètres de la stratégie** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.
6. Dans la section **Paramètres généraux**, choisissez la sous-section **Interface**.
7. Dans le groupe **Interaction avec l'utilisateur**, exécutez une des actions suivantes :
   - Cochez la case **Afficher l'interface de l'application** si vous souhaitez que les éléments suivants de l'interface s'affichent sur l'ordinateur client :

- le dossier portant le nom de l'application dans le menu **Démarrer** ;
- l'icône de Kaspersky Endpoint Security dans la zone de notification de la barre des tâches de Microsoft Windows ;
- les pops-ups de notification.

Si la case est cochée, l'utilisateur peut consulter les paramètres de l'application depuis l'interface de celle-ci et, s'il possède les autorisations requises, il peut également les modifier.

- Décochez la case **Afficher l'interface de l'application** si vous voulez cacher tous les signes de fonctionnement de Kaspersky Endpoint Security sur l'ordinateur client.

8. Dans le groupe **Interaction avec l'utilisateur**, cochez la case **Interface de l'application simplifiée** si vous voulez que l'interface de l'application simplifiée s'affiche sur l'ordinateur client doté de Kaspersky Endpoint Security.

   La case est accessible si la case **Afficher l'interface de l'application** est cochée.

Chiffrement des données

Si Kaspersky Endpoint Security a été installé sur un ordinateur s'exécutant sous un système d'exploitation Microsoft Windows pour poste de travail, la fonction de chiffrement des données est entièrement disponible. Si l'application Kaspersky Endpoint Security est installée sur un ordinateur qui tourne sous un système d'exploitation Microsoft Windows pour serveurs de fichiers, seul le chiffrement du disque à l'aide de la technologie Chiffrement de disque BitLocker est accessible.

Cette section fournit des informations sur le chiffrement et le déchiffrement des fichiers sur les disques locaux de l'ordinateur, les disques durs et les disques amovibles et explique comment configurer et exécuter le chiffrement et le déchiffrement des données à l'aide de Kaspersky Endpoint Security et du plug-in d'administration de Kaspersky Endpoint Security.

En l'absence d'accès aux données chiffrées, suivez les instructions spéciales sur l'utilisation des données chiffrées (Utilisation des fichiers chiffrés avec la fonction de chiffrement des fichiers limitée, Utilisation des périphériques chiffrés en l'absence d'accès à ceux-ci).

A propos des Coffres-forts

Kaspersky Endpoint Security permet de chiffrer les fichiers et les dossiers enregistrés sur les disques locaux de l'ordinateur et sur les disques amovibles, les disques amovibles et les disques durs en entier. Le chiffrement des données réduit le risque de fuites d'informations en cas de perte ou de vol d'un ordinateur portable, d'un disque amovible ou d'un disque dur ou en cas d'accès d'utilisateurs ou d'applications tierces à ces données.

Si la licence a expiré, l'application ne chiffre pas les nouvelles données et les anciennes données chiffrées restent chiffrées et accessibles. Dans ce cas, le chiffrement de nouvelles données requiert l'activation de l'application selon une nouvelle licence qui autorise l'utilisation du chiffrement.

En cas d'expiration de la licence, de violation des conditions du Contrat de licence Utilisateur final, de suppression de la clé ou de Kaspersky Endpoint Security ou de ses modules de chiffrement de l'ordinateur de l'utilisateur, il n'est pas garanti que les fichiers chiffrés antérieurement le resteront. Cela s'explique par le fait que certaines applications, comme Microsoft Office Word, créent une copie temporaire des fichiers pendant leur modification. Lorsque le fichier d'origine est enregistré, la copie temporaire remplace le fichier d'origine. Par conséquent, en l'absence de la fonction de chiffrement sur l'ordinateur ou en cas d'indisponibilité de celle-ci, le fichier reste non chiffré.

Kaspersky Endpoint Security protège les données de la manière suivante :

- **Chiffrement des fichiers sur les disques locaux de l'ordinateur**. Vous pouvez former des listes à partir de fichiers selon l'extension ou selon les groupes d'extensions ou de dossiers situés sur les disques locaux de l'ordinateur. Vous pouvez aussi créer des règles de chiffrement de fichiers créés par des applications distinctes. Après l'application de la stratégie de Kaspersky Security Center l'application Kaspersky Endpoint Security chiffre et déchiffre les fichiers suivants :

  - les fichiers ajoutés séparément aux listes pour le chiffrement et le déchiffrement ;
  - les fichiers enregistrés dans les dossiers ajouté aux listes pour le chiffrement et le déchiffrement ;
  - les fichiers créés des applications distinctes.

  Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

- **Chiffrement des disques amovibles**. Vous pouvez indiquer la règle de chiffrement par défaut conformément à laquelle l'application exécute la même action sur tous les disques amovibles ou indiquer des règles de chiffrement pour des disques amovibles distincts.

  La priorité d'une règle de chiffrement par défaut est inférieure à celle d'une règle de chiffrement définie pour différents disques amovibles. La priorité des règles de chiffrement définies pour les disques amovibles du modèle de périphérique indiqué est inférieure à celle des règles de chiffrement définies pour les disques amovibles portant un identificateur de périphérique indiqué.

  Afin de sélectionner la règle de chiffrement des fichiers sur le disque amovible, Kaspersky Endpoint Security vérifie si le modèle du périphérique ou son identificateur sont connus. Ensuite, l'application réalise une des opérations suivantes :

  - Si le seul le modèle du périphérique est connu, l'application applique la règle de chiffrement définie pour les disques amovibles de ce modèle, si une telle règle existe.
  - Si seul l'identificateur du périphérique est connu, l'application utilise la règle de chiffrement définie pour les disques amovibles portant cet identificateur de périphérique, si une telle règle existe.
  - Si le modèle du périphérique et son identificateur sont connus, l'application utilise la règle de chiffrement définie pour les disques amovibles portant cet identificateur connu, si une telle règle existe. Si cette règle n'existe pas, mais qu'il existe une règle de chiffrement créée pour les disques amovibles de ce modèle de périphérique, l'application l'applique. Si aucune règle de chiffrement n'est définie pour aucun identificateur de périphérique, ni pour aucun modèle de périphérique, l'application adopte la règle de chiffrement par défaut.
  - Si le modèle et l'identificateur du périphérique sont inconnus, l'application utilise la règle de chiffrement par défaut.

  L'application permet de préparer le disque amovible pour travailler en mode portable avec les fichiers qui sont chiffrés sur ce dernier. Après l'activation du mode portable, l'utilisation des fichiers chiffrés devient accessible sur les disques amovibles connectés à l'ordinateur dont la fonction de chiffrement est inaccessible.

L'application exécute l'action indiquée dans la règle de chiffrement lors de l'application de la stratégie de Kaspersky Security Center.

- **Administration des règles d'accès des applications aux fichiers chiffrés**. Vous pouvez créer pour n'importe quelle application une règle d'accès aux fichiers chiffrés qui interdira l'accès aux fichiers chiffrés ou qui l'autorisera uniquement sous la forme de texte chiffré, soit une séquence de caractères obtenues après l'application du chiffrement.

- **Créer des archives chiffrées**. Vous pouvez créer des archives chiffrées et les protéger par un mot de passe. Pour accéder au contenu de ces archives chiffrées, il faut saisir le mot de passe défini pour protéger l'accès à ces archives. Ces archives peuvent être envoyées en toute sécurité sur le réseau ou sur des disques amovibles.

- **Chiffrement du disque**. Vous pouvez choisir la technologie du chiffrement : Kaspersky Disk Encryption ou le Chiffrement de disque BitLocker (ci-après "BitLocker").

  BitLocker est une technologie qui fait partie du système d'exploitation Windows. Si l'ordinateur est équipé d'un module de plateforme sécurisée (TPM, Trusted Platform Module), BitLocker l'utilise pour conserver les clés de récupération qui permettent d'accéder au disque dur chiffré. Lors du chargement de l'ordinateur, BitLocker sollicite la clé de récupération du disque dur au module de plateforme sécurisée, puis débloque le disque. Vous pouvez configurer l'utilisation du mot de passe et/ou d'un code PIN pour accéder aux clés de restauration.

  Vous pouvez désigner une règle de chiffrement du disque par défaut et composer une liste de disques à exclure du chiffrement. Kaspersky Endpoint Security chiffre le disque secteur par secteur après l'application de la stratégie de Kaspersky Security Center. L'application chiffre toutes les sections logiques des disques durs à la fois. Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

  Une fois que les disques durs système auront été chiffrés, l'accès à ceux-ci et le chargement du système d'exploitation lors du prochain démarrage de l'ordinateur seront possibles uniquement après avoir suivi la procédure d'authentification à l'aide de l'Agent d'authentification. Pour ce faire, il faut saisir le mot de passe du token ou de la carte à puce connectés à l'ordinateur ou le nom et le mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur système du réseau local de l'organisation à l'aide des tâches d'administration des comptes utilisateur de l'Agent d'authentification. Ces comptes utilisateur reposent sur les comptes utilisateur Microsoft Windows utilisés pour accéder au système d'exploitation. Vous pouvez administrer les comptes de l'Agent d'authentification et utiliser la technologie (SSO, Single Sign-On) qui permet d'accéder automatiquement au système d'exploitation à l'aide du nom et du mot de passe du compte utilisateur de l'Agent d'Authentification.

  > Si une copie sauvegarde a été créée pour l'ordinateur puis que les données de celui-ci ont été chiffrées et que la copie de sauvegarde de l'ordinateur a été restaurée et les données à nouveau chiffrées, Kaspersky Security crée des doubles des comptes de l'Agent d'authentification. Pour supprimer les doublons, utilisez l'utilitaire klmover avec l'argument `dupfix`. L'utilitaire klmover est fourni avec la distribution de Kaspersky Security Center. Pour en savoir plus sur son fonctionnement, lisez l'aide de Kaspersky Security Center.

  Les disques durs chiffrés sont accessibles uniquement depuis des ordinateurs équipés de l'application Kaspersky Endpoint Security avec la fonction de chiffrement du disque. Cette condition réduit au minimum le risque de fuite d'informations stockées sur le disque dur chiffré en cas d'utilisation de ce disque en dehors du réseau local de l'organisation.

Pour le chiffrement des disques durs et amovibles, vous pouvez utiliser la fonction **Chiffrer uniquement l'espace occupé**. Il est conseillé d'utiliser cette fonction seulement pour les nouveaux périphériques qui n'ont jamais été utilisés. Si vous appliquez le chiffrement à un périphérique déjà utilisé, il est recommandé de chiffrer tout le périphérique. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites.

Avant le chiffrement, Kaspersky Endpoint Security reçoit la carte des secteurs du système de fichiers. Lors du premier flux, ce sont les secteurs occupés par des fichiers au moment du lancement du chiffrement qui seront chiffrés. Dans le deuxième flux, les secteurs chiffrés sont les secteurs dans lesquels une écriture a eu lieu après le début du chiffrement. A la fin du chiffrement, tous les secteurs contenant des données sont chiffrés.

Si l'utilisateur, après le chiffrement, supprime un fichier, alors les secteurs dans lesquels se trouvait ce fichier deviennent disponibles pour d'autres écritures d'informations au niveau du système de fichiers, mais restent chiffrés. Ainsi, au fur et à mesure de l'enregistrement de fichiers sur un nouveau périphérique, en cas de lancement régulier du chiffrement avec la fonction activée **Chiffrer uniquement l'espace occupé**, tous les secteurs de l'ordinateur seront chiffrés après un certain temps.

Les données indispensables au déchiffrement des objets sont offertes par le Serveur d'administration de Kaspersky Security Center qui gère l'ordinateur au moment du chiffrement. Si pour une raison quelconque l'ordinateur contenant les objets chiffrés est géré par un autre Serveur d'administration et que l'accès aux objets chiffrés n'a jamais été effectué, il est possible de résoudre la situation d'une des manières suivantes :

- demander l'accès aux objets chiffrés à l'administrateur du réseau local de l'organisation ;
- restaurer les données sur les périphériques chiffrés à l'aide de l'utilitaire de restauration ;
- restaurer la configuration du Serveur d'administration Kaspersky Security Center qui gérait l'ordinateur au moment du chiffrement à partir de la copie de sauvegarde. Utiliser cette configuration sur le Serveur d'administration qui gérait l'ordinateur avec les objets chiffrés.

L'application crée des fichiers de service pendant le chiffrement. Pour leur sauvegarde, il faut environ 0,5 % d'espace libre non fragmenté sur le disque dur de l'ordinateur. S'il n'y a pas assez d'espace libre non fragmenté sur le disque dur, le chiffrement n'est pas lancé tant que cette condition n'est pas remplie.

La compatibilité entre la fonction de chiffrement du disque de Kaspersky Endpoint Security et Kaspersky Anti-Virus for UEFI n'est pas prise en charge. Kaspersky Anti-Virus for UEFI se lance avant le chargement du système d'exploitation. Lors du chiffrement du disque, l'application découvre l'absence d'un système d'exploitation sur l'ordinateur. Cela entraîne l'arrêt sur échec de Kaspersky Anti-Virus for UEFI.

Le chiffrement de dossiers et de fichiers distincts n'influence pas le fonctionnement Kaspersky Anti-Virus for UEFI.

Restrictions de la fonction de chiffrement

La fonction de chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption n'est pas accessible pour les disques durs qui ne sont pas conformes à la configuration matérielle et logicielle.

Kaspersky Endpoint Security n'est pas compatible avec les configurations suivantes :

- schéma selon lequel le chargeur se trouve sur un disque et le système d'exploitation, sur un autre ;
- logiciel inséré standard UEFI 32 ;
- système avec technologie Intel® Rapid Start Technology et disques avec partition de mise en veille prolongée, même si l'utilisation d'Intel® Rapid Start Technology est désactivée ;
- disques au format MBR comptant plus de quatre partitions étendues ;
- système possédant un fichier de pagination qui ne se trouve pas sur le disque système ;
- système à démarrage multiple avec plusieurs systèmes d'exploitation installés simultanément ;

- sections dynamiques (seules les sections du type principal sont prises en charge) ;
- disques avec moins de 0,5 % d'espace disque libre non fragmenté ;
- disques dont la taille de secteur, différente de 512 ou 4 096 octets, émulent 512 octets ;
- disques hybrides.

Changement de l'algorithme de chiffrement

L'algorithme de chiffrement employé par Kaspersky Endpoint Security pour chiffrer les données dépend des bibliothèques de chiffrement qui sont reprises dans la distribution.

Pour changer d'algorithme de chiffrement, procédez comme suit :

1. Déchiffrez les objets que Kaspersky Endpoint Security avait chiffré avant de lancer la modification de l'algorithme de chiffrement.

   Une fois que l'algorithme de chiffrement a été modifié, les objets chiffrés antérieurement ne sont plus disponibles.

2. Supprimez Kaspersky Endpoint Security.
3. Installez Kaspersky Endpoint Security à l'aide du paquet de distribution de Kaspersky Endpoint Security contenant un algorithme de chiffrement pour un nombre de bits différent.

Activation de l'utilisation de la technologie d'authentification unique (SSO)

La technologie d'authentification unique (SSO) est incompatible avec les fournisseurs d'identifiants tiers.

Pour activer l'utilisation de la technologie d'authentification unique (SSO), procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Paramètres généraux de chiffrement**.
7. Dans la sous-section **Paramètres généraux de chiffrement**, cliquez sur le bouton **Configurer** dans la section **Paramètres de mot de passe**.

Cette action ouvre l'onglet **Agent d'authentification** de la fenêtre **Paramètres des mots de passe de chiffrement**.

8. Cochez la case **Utiliser la technologie d'authentification unique (SSO)**.
9. Cliquez sur le bouton **OK**.
10. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.
11. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Particularités du chiffrement des fichiers

Lors de l'utilisation de la fonctionnalité de chiffrement des fichiers, il faut tenir compte des particularités suivantes :

- Une stratégie de Kaspersky Security Center avec les paramètres définis de chiffrement des disques amovibles est composée pour un groupe défini d'ordinateurs administrés. Par conséquent, le résultat de l'application de la stratégie de Kaspersky Security Center avec chiffrement/déchiffrement des disques amovibles dépend de l'ordinateur auquel le disque amovible a été connecté.
- Kaspersky Endpoint Security ne (dé)chiffre pas les fichiers avec l'état d'accès "lecture seule" qui sont enregistrés sur les disques amovibles.
- Kaspersky Endpoint Security (dé)chiffre les dossiers standards uniquement pour les profils utilisateur locaux du système d'exploitation. Kaspersky Endpoint Security ne (dé)chiffre pas les dossiers standards pour les profils utilisateur itinérant (roaming user profiles), les profils utilisateur obligatoire (mandatory user profiles), les profils utilisateur temporaires (temporary user profiles) et les redirections de dossiers (folder redirection). Les dossiers standards que les experts de Kaspersky recommandent de chiffrer sont les suivants :
  - Mes Documents.
  - Favoris.
  - Fichiers Cookies.
  - Bureau.
  - Fichiers temporaires Internet Explorer.
  - Fichiers temporaires.
  - Fichiers Outlook.
- Kaspersky Endpoint Security ne chiffre pas les fichiers dont la modification peut nuire au fonctionnement du système d'exploitation et des programmes installés. Par exemple, la liste des exclusions du chiffrement inclut les fichiers et les dossiers suivants avec tous les dossiers qui y sont joints :
  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - les fichiers du registre Windows.

La liste des exclusions du chiffrement ne peut pas être consultée et modifiée. Les fichiers et les dossiers de la liste des exclusions du chiffrement peuvent être ajoutés à la liste pour le chiffrement, mais ils ne seront pas chiffrés lors de l'exécution de la tâche de chiffrement des fichiers.

- Les types de périphériques suivants sont pris en charge en guise de disques amovibles :
  - supports branchés via le port USB ;
  - disques durs branchés via le port USB ou FireWire ;
  - disques SSD branchés via le port USB ou FireWire.

Chiffrement du disque

Si Kaspersky Endpoint Security a été installé sur un ordinateur s'exécutant sous un système d'exploitation Microsoft Windows pour poste de travail, le chiffrement peut être réaliser à l'aide de la technologie Chiffrement de disque BitLocker ou de la technologie Kaspersky Disk Encryption. Si l'application Kaspersky Endpoint Security est installée sur un ordinateur s'exécutant sous un système d'exploitation Microsoft Windows pour serveurs de fichiers, seule la technologie Chiffrement de disque BitLocker est accessible.

Cette section décrit le chiffrement du disque et explique comment configurer et exécuter le chiffrement du disque à l'aide de Kaspersky Endpoint Security et du plug-in d'administration de Kaspersky Endpoint Security.

A propos du chiffrement du disque

Kaspersky Endpoint Security prend en charge le chiffrement du disque dans les systèmes de fichiers FAT32, NTFS et exFat.

Avant de lancer la tâche de chiffrement du disque, l'application exécute une série d'analyses visant à confirmer la possibilité d'appliquer le chiffrement au périphérique, y compris une analyse de compatibilité du disque dur système avec l'Agent d'authentification ou avec les modules de chiffrement BitLocker. Pour vérifier la compatibilité, il faut redémarrer l'ordinateur. Après le redémarrage de l'ordinateur, l'application exécute toutes les analyses nécessaires en mode automatique. Si l'analyse de compatibilité réussit, la tâche de chiffrement du disque s'exécute après le démarrage du système d'exploitation et le lancement de l'application. Si durant le processus d'analyse, l'incompatibilité du disque dur système avec l'Agent d'authentification ou avec les modules de chiffrement BitLocker est détectée, il faut redémarrer l'ordinateur à l'aide du bouton (Reset). Kaspersky Endpoint Security consigne les informations relatives à cette incompatibilité. En fonction de ces informations, l'application ne lance pas le chiffrement complet du disque au démarrage du système d'exploitation. Les informations sur cet événement sont affichées dans les rapports de Kaspersky Security Center.

Si la configuration matérielle a été modifiée, l'analyse de la compatibilité du disque dur système avec l'Agent d'authentification ou les modules de chiffrements BitLocker doit être précédée de la suppression des informations sur les incompatibilités obtenues par l'application lors de l'analyse précédente. Pour ce faire, il faut saisir la commande `avp pbatestreset` dans la ligne de commande avant le chiffrement du disque. Si, suite à l'analyse de compatibilité du disque dur système avec l'Agent d'authentification, le système d'exploitation ne démarre pas, il est nécessaire de supprimer les objets et données restants au terme du fonctionnement test de l'Agent d'authentification à l'aide de l'utilitaire de restauration, puis de lancer Kaspersky Endpoint Security et d'exécuter à nouveau la commande `avp pbatestreset`.

Après le lancement du chiffrement du disque, Kaspersky Endpoint Security chiffre tout ce qui est enregistré sur les disques durs.

Si pendant le chiffrement du disque, l'utilisateur éteint ou redémarre l'ordinateur, l'Agent d'authentification est téléchargé avant le prochain démarrage du système d'exploitation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le chiffrement du disque.

Si le système d'exploitation passe en mode d'hibernation (hibernation mode) pendant le chiffrement du disque, l'Agent d'authentification est alors téléchargé lorsque le système d'exploitation sort du mode d'hibernation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le chiffrement du disque.

Si le système d'exploitation passe en mode veille pendant l'exécution de la tâche de chiffrement du disque, Kaspersky Endpoint Security reprend le chiffrement du disque, sans charger l'Agent d'authentification, lorsque le système d'exploitation sort du mode veille.

L'authentification de l'utilisateur dans l'Agent d'authentification peut s'exécuter par deux moyens :

- via la saisie du nom d'utilisateur et du mot de passe du compte utilisateur de l'Agent d'authentification créé par l'administrateur du réseau local de l'organisation via Kaspersky Security Center ;
- via la saisie du mot de passe du token ou de la carte à puce rattaché à l'ordinateur.

  L'utilisation du token ou de la carte à puce est disponible uniquement si les disques durs de l'ordinateur sont chiffrés à l'aide d'un algorithme AES256. Si les disques durs de l'ordinateur ont été chiffrés à l'aide d'un algorithme de chiffrement AES56, le fichier de certificat électronique ne pourra pas être ajouté à la commande.

L'Agent d'authentification prend en charge les dispositions de clavier des langues suivantes :

- Anglais (Royaume-Uni) ;
- Anglais (E-U) ;
- Arabe (Algérie, Maroc, Tunisie, disposition AZERTY) ;
- Espagnol (Amérique latine) ;
- Italien ;
- Allemand (Allemagne et Autriche) ;
- Allemand (Suisse) ;
- Portugais (Brésil, disposition ABNT2) ;
- Russe (pour clavier IBM à 105 touches / Windows avec disposition ЙЦУКЕН) ;
- Turc (disposition QWERTY) ;
- Français (France) ;
- Français (Suisse) ;

- Français (Belgique, disposition AZERTY) ;
- Japonais (pour clavier à 106 touches, disposition QWERTY).

La disposition du clavier devient disponible dans l'Agent d'authentification si elle est ajoutée aux paramètres de langue et aux normes régionales du système d'exploitation. Elle est accessible via l'écran d'accueil de Microsoft Windows.

Si le nom du compte utilisateur de l'Agent d'authentification contient des caractères qui ne peuvent être saisis à l'aide des claviers disponibles dans l'Agent d'authentification, l'accès aux disques durs chiffrés est possible seulement après leur récupération à l'aide de l'utilitaire de restauration ou après la restauration du nom et le mot de passe du compte utilisateur de l'Agent d'authentification.

Kaspersky Endpoint Security fonctionne avec les tokens liseurs de cartes à puces et avec les cartes à puce suivants :

- SafeNet eToken PRO 64K (4.2b) (USB).
- SafeNet eToken PRO 72K Java (USB).
- SafeNet eToken PRO 72K Java (carte à puce).
- SafeNet eToken 4100 72K Java (carte à puce).
- SafeNet eToken 5100 (USB).
- SafeNet eToken 5105 (USB).
- SafeNet eToken 7300 (USB).
- EMC RSA SecurID 800 (USB)
- RuToken ETsP (USB).
- RuToken ETsP (Flash).
- Aladdin-RD JaCarta PKI (USB).
- Aladdin-RD JaCarta PKI (carte à puce).
- Athena IDProtect Laser (USB).
- Gemalto IDBridge CT40 (lecteur).
- Gemalto IDPrime .NET 511.

Chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption

Avant de lancer le chiffrement du disque de l'ordinateur, il est recommandé de s'assurer que l'ordinateur n'est pas infecté. Pour ce faire, lancez une analyse complète ou une analyse des zones critiques de l'ordinateur. Le chiffrement du disque sur un ordinateur infecté par un rootkit peut provoquer le dysfonctionnement de l'ordinateur.

Pour réaliser le chiffrement du disque à l'aide de la technologie Kaspersky Disk Encryption, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement du disque**.
7. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Kaspersky Disk Encryption**.

   L'application de la technologie de chiffrement Kaspersky Disk Encryption est impossible si sur l'ordinateur possède des disques durs chiffrés à l'aide de BitLocker.

8. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Chiffrer tous les disques durs**.

   Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel l'application est installée peut être lancé après le chiffrement de l'ensemble des disques durs.

   Si certains disques durs doivent être exclus du chiffrement, consignez-les dans une liste.

9. Choisissez un des modes de chiffrement suivants :

   - Si vous voulez appliquer le chiffrement uniquement aux secteurs du disque dur qui sont occupés par des fichiers, cochez la case **Chiffrer uniquement l'espace occupé**.

     Si vous appliquez le chiffrement à un disque déjà utilisé, il est recommandé de chiffrer tout le disque. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites. L'utilisation de la fonction **Chiffrer uniquement l'espace occupé** est recommandée pour les nouveaux disques jamais utilisés jusqu'à présent.

   - Si vous voulez appliquer le chiffrement à tout le disque dur, décochez la case **Chiffrer uniquement l'espace occupé**.

     Cette fonction est uniquement applicable aux appareils non chiffrés. Si l'appareil avait été chiffré à l'aide de la fonction **Chiffrer uniquement l'espace occupé**, après l'application de la stratégie en mode **Chiffrer tous les disques durs**, les secteurs qui n'hébergent pas de fichiers ne seront toujours pas chiffrés.

10. Si un problème d'incompatibilité matérielle a été rencontré pendant le chiffrement de l'ordinateur, vous pouvez cocher la case **Utiliser le Legacy USB Support** pour activer la prise en charge des appareils USB pendant l'étape de démarrage initiale de l'ordinateur dans le BIOS.

    L'activation/la désactivation de la fonction Legacy USB Support n'a pas d'impact sur la prise en charge des périphériques USB après le lancement du système d'exploitation.

    Lorsque la fonction Legacy USB Support est activée, l'Agent d'authentification ne prend pas en charge les tokens USB si l'ordinateur fonctionne en mode BIOS. Il est recommandé d'utiliser la fonction uniquement en cas de problèmes d'incompatibilités avec le matériel et seulement sur les ordinateurs où le problème est apparu.

11. Cliquez sur **OK** pour enregistrer les modifications.

12. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Chiffrement du disque à l'aide de la technologie Chiffrement de disque BitLocker

Avant de lancer le chiffrement du disque de l'ordinateur, il est recommandé de s'assurer que l'ordinateur n'est pas infecté. Pour ce faire, lancez une analyse complète ou une analyse des zones critiques de l'ordinateur. Le chiffrement du disque sur un ordinateur infecté par un rootkit peut provoquer le dysfonctionnement de l'ordinateur.

Pour que la technologie Chiffrement de disque BitLocker puisse fonctionner sur les ordinateurs dotés d'un système d'exploitation pour serveur, il faudra peut être installer le module **Chiffrement de disque BitLocker** via l'Assistant d'ajout de rôles.

Pour appliquer le chiffrement du disque à l'aide de la technologie Chiffrement de disque BitLocker, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement du disque**.

7. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Chiffrement de disque BitLocker**.

8. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Chiffrer tous les disques durs**.

   Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel le chiffrement a été réalisé peut être lancé après le chiffrement.

9. Si vous voulez activer l'authentification BitLocker dans un environnement qui précède le lancement des tablettes, cochez la case **Autoriser l'utilisation de l'authentification qui requiert une saisie au clavier avant le démarrage sur les tablettes**.

   Le clavier tactile des tablettes n'est pas accessible dans cet environnement. Pour réaliser une authentification BitLocker sur de telles tablettes, l'utilisateur doit absolument connecter un clavier USB par exemple.

10. Choisissez un des types de chiffrement suivants :

    - Si vous voulez utiliser le chiffrement au niveau matériel, cochez la case **Utiliser le chiffrement au niveau matériel**.
    - Si vous voulez utiliser le chiffrement au niveau logiciel, décochez la case **Utiliser le chiffrement au niveau matériel**.

11. Choisissez un des modes de chiffrement suivants :

    - Si vous voulez appliquer le chiffrement uniquement aux secteurs du disque dur qui sont occupés par des fichiers, cochez la case **Chiffrer uniquement l'espace occupé**.
    - Si vous voulez appliquer le chiffrement à tout le disque dur, décochez la case **Chiffrer uniquement l'espace occupé**.

      Cette fonction est uniquement applicable aux disques durs non chiffrés. Si le disque dur avait été chiffré à l'aide de la fonction **Chiffrer uniquement l'espace occupé**, après l'application de la stratégie en mode **Chiffrer tous les disques durs**, les secteurs qui n'hébergent pas de fichiers ne seront toujours pas chiffrés.

12. Choisissez le mode d'accès aux disques durs chiffrés à l'aide de BitLocker :

    - Si vous voulez utiliser le module TPM pour stocker les clés de chiffrement, choisissez l'option **Utiliser le module de plateforme sécurisée (TPM)**.
    - Si vous n'utilisez pas le module TPM pour le chiffrement du disque, choisissez l'option **Utiliser le mot de passe** et indiquez dans le champ **Longueur minimale du mot de passe** le nombre minimum de caractères que doit contenir le mot de passe.

      La présence du module TPM est obligatoire pour les systèmes d'exploitation Windows 7 et Windows 2008 R2 ou antérieures.

13. Si vous aviez choisi l'option **Utiliser le module de plateforme sécurisée (TPM)** à l'étape précédente, procédez comme suit :

    - Si vous souhaitez définir le code PIN que l'utilisateur devra saisir pour accéder à la clé de chiffrement, cochez la case **Utiliser le code PIN** et indiquez dans le champ **Longueur minimale du code PIN** le nombre

minimum de chiffres que doit contenir le code PIN.

- Si vous souhaitez qu'il soit possible, en l'absence sur l'ordinateur du module TPM, d'accéder aux disques durs chiffrés à l'aide d'un mot de passe, cochez la case **Utiliser le mot de passe si le module de plateforme sécurisée (TPM) n'est pas disponible** et définissez le nombre minimum de caractères que doit contenir le mot de passe dans le champ **Longueur minimale du mot de passe** .

  Dans ce cas, l'accès aux clés de chiffrement sera octroyé après la saisie du mot de passe défini, comme si la case **Utiliser le mot de passe** avait été cochée.

  Si la case **Utiliser le mot de passe si le module de plateforme sécurisée (TPM) n'est pas disponible** n'est pas cochée et si le module TPM n'est pas disponible, le chiffrement du disque n'est pas lancé.

14. Cliquez sur **OK** pour enregistrer les modifications.

15. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'*aide de Kaspersky Security Center*.

Après l'application de la stratégie sur un ordinateur client doté de Kaspersky Endpoint Security, les demandes suivantes apparaissent :

- Si le chiffrement du disque dur a été configuré dans la stratégie de Kaspersky Security Center :
  - En présence d'un module TPM, une fenêtre de saisie d'un code PIN s'ouvre.
  - En l'absence d'un module TPM, une fenêtre de saisie de mot de passe pour l'identification avant le chargement s'ouvre.
- Si la compatibilité avec la norme FIPS (norme fédérale de traitement de l'information) est activée dans le système d'exploitation, une fenêtre de demande de connexion d'un périphérique de stockage de masse pour l'enregistrement du fichier de clé de récupération s'ouvre dans les systèmes d'exploitation Windows 8 et dans les versions antérieures.

En l'absence d'accès aux clés du chiffrement, l'utilisateur peut demander la clé de récupération à l 'administrateur du réseau local de l'organisation (si la clé de la récupération n'avait pas été enregistrée sur le périphérique de stockage de masse ou si elle avait été perdue).

Composition de la liste des disques durs exclus du chiffrement

Vous pouvez composer la liste des exclusions du chiffrement seulement pour la technologie Kaspersky Disk Encryption.

Pour composer la liste des disques durs à exclure du chiffrement, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement du disque**.

7. Dans la liste déroulante **Technologie de chiffrement**, choisissez l'option **Kaspersky Disk Encryption**.

   Le tableau **Ne pas chiffrer les disques durs suivants** reprend les enregistrements relatifs aux disques durs qui ne seront pas chiffrés par l'application. Ce tableau est vide si vous n'avez pas créé de liste de disques durs à exclure du chiffrement.

8. Si vous souhaitez ajouter des disques durs à la liste des disques durs qui ne seront pas chiffrés par l'application, procédez comme suit :

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

      La fenêtre **Ajout de périphériques de la liste Kaspersky Security Center** s'ouvre.

   b. Dans la fenêtre **Ajout de périphériques de la liste Kaspersky Security Center**, définissez les valeurs des paramètres **Nom**, **Ordinateur**, **Type de disque**, **Kaspersky Disk Encryption**.

   c. Cliquez sur le bouton **Actualiser**.

   d. Dans la colonne **Nom**, cochez les cases dans les lignes du tableau qui correspondent aux disques durs que vous souhaitez ajouter à la liste des disques durs exclus du chiffrement.

   e. Cliquez sur le bouton **OK**.

   Les disques durs sélectionnés sont repris dans le tableau **Ne pas chiffrer les disques durs suivants**.

9. Si vous souhaitez supprimer disques durs du tableau des exclusions, sélectionnez une ou plusieurs lignes du tableau **Ne pas chiffrer les disques durs suivants**, puis cliquez sur **Supprimer**.

   Pour sélectionner plusieurs lignes dans le tableau, sélectionnez-les en maintenant la touche **CTRL** enfoncée.

10. Cliquez sur **OK** pour enregistrer les modifications.

Déchiffrement des disques durs

Vous pouvez déchiffrer les disques durs même en l'absence d'une licence valide qui autorise le chiffrement des données.

Pour déchiffrer des disques durs, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement du disque**.

7. Dans la liste déroulante **Technologie de chiffrement** choisissez la technologie à l'aide de laquelle les disques durs ont été chiffrés.

8. Exécutez une des actions suivantes :

   - Dans la liste déroulante **Mode de chiffrement**, cochez la case **Déchiffrer tous les disques durs** si vous souhaitez déchiffrer tous les disques durs chiffrés.

   - Ajoutez au tableau **Ne pas chiffrer les disques durs suivants** les disques durs chiffrés que vous souhaitez déchiffrer.

     Cette option est accessible seulement pour la technologie de chiffrement Kaspersky Disk Encryption.

9. Cliquez sur **OK** pour enregistrer les modifications.

10. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Si, pendant le déchiffrement des disques durs chiffrés à l'aide de la technologie Kaspersky Disk Encryption, l'utilisateur éteint ou redémarre l'ordinateur, l'Agent d'authentification est chargé avant le prochain démarrage du système d'exploitation. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le déchiffrement des disques durs.

Si, pendant le déchiffrement des disques durs chiffrés à l'aide de la technologie Kaspersky Disk Encryption, le système d'exploitation passe en mode d'hibernation (hibernation mode), lorsque le système d'exploitation sortira du mode veille, l'Agent d'authentification sera chargé. Après la procédure d'authentification dans l'agent et après le démarrage du système d'exploitation, Kaspersky Endpoint Security reprend le déchiffrement des disques durs. Après le déchiffrement des disques durs, le mode veille prolongée n'est pas accessible avant le premier redémarrage du système d'exploitation.

Si pendant le déchiffrement des disques durs, le système d'exploitation passe en mode veille, lorsque le système d'exploitation sortira du mode veille, Kaspersky Endpoint Security reprendra le déchiffrement des disques durs sans charger l'Agent d'authentification.

Elimination des erreurs lors de la mise à jour de la fonctionnalité de chiffrement

Lors de la mise à jour depuis une version antérieure de l'application jusqu'à Kaspersky Endpoint Security 11.1.1 for Windows, la fonctionnalité de Chiffrement du disque est mise à jour.

Les erreurs suivantes peuvent surgir lors du lancement de la mise à jour de la fonctionnalité de chiffrement du disque :

- Échec de l'initialisation de la mise à jour.

- Le périphérique est incompatible avec l'Agent d'authentification.

Pour éliminer les erreurs qui sont surviennent au lancement de la mise à jour de la fonctionnalité de chiffrement du disque, réalisez les opérations suivantes dans la nouvelle version :

1. Déchiffrez les disques durs.
2. Chiffrez à nouveau les disques durs.

Lors de la mise à jour de la fonctionnalité de chiffrement du disque, les erreurs suivantes peuvent survenir :

- Échec de la mise à jour.
- Échec de la restauration de la mise à jour de la fonctionnalité de chiffrement.

Pour éliminer les erreurs survenues lors de la mise à jour de la fonctionnalité de chiffrement du disque,

rétablissez l'accès à l'appareil chiffré à l'aide de l'utilitaire de restauration.

Chiffrement des fichiers sur les disques locaux de l'ordinateur

Le chiffrement des fichiers sur les disques locaux de l'ordinateur est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur doté d'un système d'exploitation Microsoft Windows pour postes de travail. Le chiffrement des fichiers sur les disques d'ordinateurs locaux n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur fonctionnant sous Microsoft Windows pour serveurs de fichiers.

Cette section décrit le chiffrement des fichiers sur les disques locaux de l'ordinateur et explique comment configurer et exécuter le chiffrement des fichiers sur les disques locaux de l'ordinateur à l'aide de Kaspersky Endpoint Security et du plug-in d'administration de Kaspersky Endpoint Security.

Lancement du chiffrement des fichiers sur les disques locaux de l'ordinateur

Kaspersky Endpoint Security ne chiffre pas les fichiers dont le contenu se trouve dans le stockage Cloud OneDrive et bloque la copie des fichiers chiffrés dans le stockage Cloud OneDrive si ces fichiers n'ont pas été ajoutés à la règle de déchiffrement.

Kaspersky Endpoint Security prend en charge le chiffrement des fichiers dans les systèmes de fichiers FAT32 et NTFS. Si un disque amovible doté d'un système de fichiers non pris en charge est connecté à l'ordinateur, le chiffrement de ce disque amovible se solde sur une erreur et Kaspersky Endpoint Security lui attribue l'état d'accès "lecture seule".

Pour chiffrer des fichiers sur les disques locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement des fichiers**.
7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Chiffrement**.
8. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Règles par défaut**.
9. Sur l'onglet **Chiffrement**, appuyez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :
   a. Choisissez l'option **Dossiers standards** pour ajouter à la règle de chiffrement des fichiers issus de dossiers de profils d'utilisateurs locaux proposés par les experts de Kaspersky.
      La fenêtre **Sélection des dossiers standards** s'ouvre.
   b. Choisissez l'option **Dossier manuel** pour ajouter le chemin d'accès saisi manuellement à la règle du chiffrement du dossier.
      La fenêtre **Ajout manuel d'un dossier** s'ouvre.
   c. Choisissez l'option **Fichiers selon l'extension** pour ajouter des extensions de fichiers à la règle de chiffrement. Kaspersky Endpoint Security chiffre les fichiers portant les extensions indiquées sur tous les disques locaux de l'ordinateur.
      La fenêtre **Ajout/modification de la liste des extensions de fichiers** s'ouvre.
   d. Choisissez l'option **Fichiers selon des groupes d'extension** pour ajouter des groupes d'extensions de fichiers à la règle de chiffrement. Kaspersky Endpoint Security chiffre les fichiers portant les extensions indiquées dans les groupes d'extensions sur tous les disques locaux de l'ordinateur.
      La fenêtre **Sélection des groupes d'extensions de fichiers** s'ouvre.
10. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.
11. Appliquez la stratégie.
    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Directement après l'application de la stratégie, Kaspersky Endpoint Security chiffre les fichiers repris dans la règle de chiffrement et non repris dans la règle de déchiffrement.

> Si le même fichier est ajouté à la fois dans la règle de chiffrement et dans la règle de déchiffrement, Kaspersky Endpoint Security ne chiffre pas ce fichier si celui-ci n'est pas déchiffré et le déchiffre s'il est chiffré.

Kaspersky Endpoint Security chiffre les fichiers non chiffrés si leurs propriétés (chemin d'accès au fichier/nom du fichier /extension du fichier) satisfont toujours aux critères de la règle du chiffrement après la modification.

Kaspersky Endpoint Security attend que les fichiers soient fermés avant de les chiffrer.

Lorsque l'utilisateur crée un fichier dont les propriétés correspondent aux critères des règles de chiffrement, Kaspersky Endpoint Security le chiffre dès son ouverture.

Si vous déplacez le fichier chiffré dans un autre dossier sur le disque local, le fichier reste chiffré que ce dossier soit couvert ou non par la règle de chiffrement.

Composition des règles d'accès des applications aux fichiers chiffrés

Pour composer des règles d'accès des applications aux fichiers chiffrés, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement des fichiers**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Règles par défaut**.

   Les règles de l'accès fonctionnent uniquement selon le mode **Règles par défaut**. Si après l'application des règles de l'accès en mode **Règles par défaut** vous passez au mode **Laisser tel quel**, Kaspersky Endpoint Security ignorera toutes les règles d'accès. Toutes les applications auront l'accès à tous les fichiers chiffrés.

8. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.
9. Si vous voulez choisir les applications exclusivement dans la liste Kaspersky Security Center, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications de la liste Kaspersky Security Center**.

   La fenêtre **Ajout d'application depuis la liste Kaspersky Security Center** s'ouvre.

   Procédez comme suit :

   a. Définissez les filtres pour afficher la liste des applications dans le tableau. Définissez pour cela les paramètres **Application**, **Éditeur**, **Période d'ajout**, ainsi que les cases du groupe **Groupe**.

   b. Cliquez sur le bouton **Actualiser**.

      Le tableau reprend les applications qui répondent aux filtres définis.

   c. Dans la colonne **Applications**, cochez les cases en regard des applications pour lesquelles vous souhaitez créer des règles d'accès aux fichiers chiffrés.

   d. Dans la liste déroulante **Règle pour les applications**, choisissez la règle qui définira l'accès des applications aux fichiers chiffrés.

   e. Dans la liste déroulante **Action pour les applications sélectionnées auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les règles d'accès aux fichiers chiffrés définies pour les applications indiquées plus haut.

   f. Cliquez sur le bouton **OK**.

Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

10. Si vous voulez choisir les applications manuellement, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications à la main**.

    La fenêtre **Ajout/modification des noms des fichiers exécutables des applications** s'ouvre.

    Procédez comme suit :

    a. Dans le champ de saisie, saisissez le nom ou la liste de noms des fichiers exécutables des applications avec leur extension.

       Vous pouvez également ajouter les noms des fichiers exécutables des applications de la liste de Kaspersky Security Center en cliquant sur le bouton **Ajouter depuis la liste de Kaspersky Security Center**.

    b. Si vous le souhaitez, saisissez une description de la liste des applications dans le champ **Description**.

    c. Dans la liste déroulante **Règle pour les applications**, choisissez la règle qui définira l'accès des applications aux fichiers chiffrés.

    d. Cliquez sur le bouton **OK**.

    Les informations relatives à la règle d'accès des applications aux fichiers chiffrés figurent dans le tableau sous l'onglet **Règles pour les applications**.

11. Cliquez sur **OK** pour enregistrer les modifications.

Chiffrement des fichiers créés et modifiés par des applications distinctes

Vous pouvez créer une règle selon laquelle Kaspersky Endpoint Security chiffrera tous les fichiers créés et modifiés par les applications indiquées dans la règle.

Les fichiers créés ou modifiés par les applications indiquées avant l'application de la règle de chiffrement ne seront pas chiffrés.

Pour configurer le chiffrement des fichiers créés et modifiés par les applications distinctes, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement des fichiers**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Règles par défaut**.

Les règles de chiffrement agissent seulement en mode **Règles par défaut**. Si après l'application des règles de chiffrement en mode **Règles par défaut** vous passez au mode **Laisser tel quel**, Kaspersky Endpoint Security ignorera toutes les règles du chiffrement. Les fichiers qui avaient été chiffrés auparavant resteront toujours chiffrés.

8. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Règles pour les applications**.

9. Si vous voulez choisir les applications exclusivement dans la liste Kaspersky Security Center, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications de la liste Kaspersky Security Center**.

   La fenêtre **Ajout d'application depuis la liste Kaspersky Security Center** s'ouvre.

   Procédez comme suit :

   a. Définissez les filtres pour afficher la liste des applications dans le tableau. Définissez pour cela les paramètres **Application**, **Éditeur**, **Période d'ajout**, ainsi que les cases du groupe **Groupe**.

   b. Cliquez sur le bouton **Actualiser**.

      Le tableau reprend les applications qui répondent aux filtres définis.

   c. Dans la colonne **Applications**, cochez les cases en face des applications dont les fichiers créés doivent être chiffrés.

   d. Dans la liste déroulante **Règle pour les applications** choisissez l'option **Chiffrer tous les fichiers créés**.

   e. Dans la liste déroulante **Action pour les applications sélectionnées auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les règles de chiffrement des fichiers chiffrés définies pour les applications indiquées plus haut.

   f. Cliquez sur le bouton **OK**.

   Les informations sur la règle de chiffrement des fichiers créés et modifiés par les applications choisies s'afficheront dans le tableau de l'onglet **Règles pour les applications**.

10. Si vous voulez choisir les applications manuellement, cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez l'option **Applications à la main**.

    La fenêtre **Ajout/modification des noms des fichiers exécutables des applications** s'ouvre.

    Procédez comme suit :

    a. Dans le champ de saisie, saisissez le nom ou la liste de noms des fichiers exécutables des applications avec leur extension.

       Vous pouvez également ajouter les noms des fichiers exécutables des applications de la liste de Kaspersky Security Center en cliquant sur le bouton **Ajouter depuis la liste de Kaspersky Security Center**.

    b. Si vous le souhaitez, saisissez une description de la liste des applications dans le champ **Description**.

    c. Dans la liste déroulante **Règle pour les applications** choisissez l'option **Chiffrer tous les fichiers créés**.

    d. Cliquez sur le bouton **OK**.

    Les informations sur la règle de chiffrement des fichiers créés et modifiés par les applications choisies s'afficheront dans le tableau de l'onglet **Règles pour les applications**.

11. Cliquez sur **OK** pour enregistrer les modifications.

Composition de la règle de déchiffrement

Pour composer la règle de déchiffrement, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement des fichiers**.
7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Déchiffrement**.
8. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'option **Règles par défaut**.
9. Sur l'onglet **Déchiffrement**, appuyez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :

   a. Choisissez l'option **Dossiers standards** pour ajouter à la règle de déchiffrement des fichiers issus des dossiers des profils d'utilisateurs locaux proposés par les experts de Kaspersky.

   La fenêtre **Sélection des dossiers standards** s'ouvre.

   b. Choisissez l'élément **Dossier manuel** pour ajouter à la règle de déchiffrement le dossier dont le chemin d'accès a été saisi manuellement.

   La fenêtre **Ajout manuel d'un dossier** s'ouvre.

   c. Choisissez l'option **Fichiers selon l'extension** pour ajouter des extensions de fichiers à la règle déchiffrement. Kaspersky Endpoint Security ne chiffre pas les fichiers portant les extensions indiquées sur tous les disques locaux de l'ordinateur.

   La fenêtre **Ajout/modification de la liste des extensions de fichiers** s'ouvre.

   d. Choisissez l'option **Fichiers selon l'extension** pour ajouter des extensions de fichiers distinctes à la règle de déchiffrement. Kaspersky Endpoint Security ne chiffre pas les fichiers portant les extensions indiquées dans les groupes d'extension sur tous les disques locaux des ordinateurs.

   La fenêtre **Sélection des groupes d'extensions de fichiers** s'ouvre.

10. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.
11. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Si le même fichier est ajouté à la fois dans la règle de chiffrement et dans la règle de déchiffrement, Kaspersky Endpoint Security ne chiffre pas ce fichier si celui-ci n'est pas déchiffré et le déchiffre s'il est chiffré.

Déchiffrement des fichiers sur les disques locaux de l'ordinateur

Pour déchiffrer des fichiers sur les disques locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, choisissez l'option **Chiffrement des fichiers**.
7. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Chiffrement**.
8. Excluez de la liste de chiffrement les fichiers et les dossiers que vous ne souhaitez pas déchiffrer. Pour ce faire, sélectionnez les fichiers dans la liste et dans le menu contextuel du bouton **Supprimer**, choisissez l'option **Supprimer la règle et déchiffrer les fichiers**.

   Vous pouvez supprimer simultanément plusieurs éléments de la liste pour le chiffrement. Pour ce faire, maintenez la touche **CTRL** enfoncée et d'un clic gauche, sélectionnez les éléments, puis dans le menu contextuel du bouton **Supprimer**, choisissez l'option **Supprimer la règle et déchiffrer les fichiers**.

   Les fichiers et dossiers supprimés de la liste de chiffrement sont ajoutés automatiquement à la liste de déchiffrement.
9. Composez la liste des fichiers à déchiffrer.
10. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.
11. Appliquez la stratégie.

Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Dès que la stratégie a été appliquée, Kaspersky Endpoint Security déchiffre les fichiers chiffrés ajoutés à la liste de déchiffrement.

Kaspersky Endpoint Security déchiffre les fichiers chiffrés si leurs paramètres (chemin d'accès au fichier, nom du fichier, extension du fichier) changent et répondent dès lors aux paramètres des objets ajoutés à la liste de déchiffrement.

Kaspersky Endpoint Security attend que les fichiers soient fermés avant de les déchiffrer.

Création d'archives chiffrées

Lors de l'ajout à une archive chiffrée d'un fichier dont le contenu se trouve dans le stockage cloud OneDrive, Kaspersky Endpoint Security télécharge le contenu du fichier, puis le chiffre.

Lors de la création d'archives chiffrées, Kaspersky Endpoint Security ne compresse pas les fichiers.

Pour créer une archive chiffrée, procédez comme suit :

1. Sur l'ordinateur doté de Kaspersky Endpoint Security et de la fonction de chiffrement des fichiers, sélectionnez les fichiers et/ou dossiers que vous souhaitez ajouter à l'archive chiffrée dans n'importe quel gestionnaire de fichiers. Cliquez-droit pour ouvrir leur menu contextuel.

2. Sélectionnez l'option **Créer une archive chiffrée** dans le menu contextuel.

   La boîte de dialogue standard de Microsoft Windows **Sélection du chemin pour l'enregistrement de l'archive chiffrée** s'ouvre.

3. Dans la boîte de dialogue standard de Microsoft Windows **Sélection du chemin pour l'enregistrement de l'archive chiffrée**, sélectionnez un point de destination pour enregistrer le paquet chiffré sur le disque amovible. Cliquez sur le bouton **Enregistrer**.

   La fenêtre **Création d'une archive chiffrée** s'ouvre.

4. Dans la fenêtre **Création d'une archive chiffrée**, saisissez le mot de passe, puis confirmez-le.

5. Cliquez sur le bouton **Générer**.

   La création de l'archive chiffrée est lancée. A l'issue du processus, une archive chiffrée auto-extractible protégée par mot de passe est créée sur le disque amovible à l'emplacement indiqué.

Si vous annulez la création d'une archive chiffrée, Kaspersky Endpoint Security réalise les opérations suivantes :

1. Il interrompt la copie des fichiers dans l'archive et terminent toutes les opérations de chiffrement de l'archive qui sont en cours.

2. Il supprime tous les fichiers temporaires créés pendant la création et le chiffrement de l'archive ainsi que le fichier de l'archive chiffrée lui-même.

3. Il signale l'arrêt forcé de la création de l'archive chiffrée.

Décompression d'archives chiffrées

Pour décompresser une archive chiffrée, procédez comme suit :

1. Dans n'importe quel gestionnaire de fichiers, sélectionnez un paquet chiffré. Cliquez pour lancer l'Assistant de décompression.

   La fenêtre **Saisie du mot de passe** s'ouvre.

2. Saisissez le mot de passe qui protège l'archive chiffrée.

3. Dans la fenêtre **Saisie du mot de passe**, cliquez sur **OK**.

   Si le mot de passe saisi est correct, alors la fenêtre Windows standard **Parcourir les dossiers** s'ouvre.

4. Dans la fenêtre Microsoft Windows standard **Parcourir les dossiers**, sélectionnez le dossier de décompression de l'archive chiffrée, puis cliquez sur **OK**.

   La décompression de l'archive chiffrée dans le dossier indiqué est lancé.

Si l'archive chiffrée a déjà été décompressée dans le dossier sélectionné, les fichiers de cette archive seront écrasés lors de la nouvelle décompression.

Si vous annulez la décompression de l'archive chiffrée, Kaspersky Endpoint Security réalise les opérations suivantes :

1. L'application arrête le déchiffrement de l'archive et interrompt toutes les opérations de copie des fichiers depuis l'archive chiffrée, le cas échéant.
2. Tous les fichiers temporaires créés pendant le déchiffrement et la décompression de l'archive chiffrée sont supprimés, tout comme tous les fichiers qui avaient déjà été copiés depuis l'archive chiffrée dans le dossier cible.
3. L'application signale l'arrêt forcé de la décompression de l'archive chiffrée.

Chiffrement des disques amovibles

Le chiffrement des disques amovibles est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur doté d'un système d'exploitation Microsoft Windows pour postes de travail. Le chiffrement des disques amovibles n'est pas disponible si Kaspersky Endpoint Security est installé sur un ordinateur doté d'un système d'exploitation Microsoft Windows pour serveurs de fichiers.

Cette section décrit le chiffrement des disques amovibles et explique comment configurer et exécuter le chiffrement à l'aide de Kaspersky Endpoint Security et le plug-in d'administration de Kaspersky Endpoint Security.

Lancement du chiffrement des disques amovibles

Pour chiffrer des disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Chiffrement des disques amovibles**.
7. Dans la liste déroulante **Mode de chiffrement**, sélectionnez l'action par défaut à effectuer par Kaspersky Endpoint Security sur tous les lecteurs amovibles connectés aux ordinateurs du groupe d'administration sélectionné :
   - **Chiffrer tout le disque amovible**. Si vous choisissez cette option, lors de l'application de la stratégie de Kaspersky Security Center avec les paramètres de chiffrement des disques amovibles définis, Kaspersky

Endpoint Security chiffre secteur par secteur le contenu des disques amovibles. De cette façon, non seulement les fichiers stockés sur le disque local sont chiffrés, mais aussi les systèmes fichiers des disques amovibles, y compris les noms des fichiers et les structures des dossiers sur les disques amovibles. Kaspersky Endpoint Security ne chiffre pas les disques amovibles déjà chiffrés.

Cette option de chiffrement est assurée par la fonction de chiffrement du disque de l'application Kaspersky Endpoint Security.

- **Chiffrer tous les fichiers**. Si vous choisissez cette option, lors de l'application de la stratégie de Kaspersky Security Center avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security chiffre tous les fichiers enregistrés sur les disques amovibles. Kaspersky Endpoint Security ne chiffre pas les fichiers déjà chiffrés. L'application chiffre les systèmes fichiers des disques amovibles, y compris les noms des fichiers chiffrés et les structures des dossiers.

- **Chiffrer uniquement les nouveaux fichiers**. Si vous choisissez cette option, lors de l'application de la stratégie de Kaspersky Security Center avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security chiffre uniquement les fichiers ajoutés aux disques amovibles ou enregistrés sur les disques durs amovibles et modifiés après la dernière application de la stratégie de Kaspersky Security Center.

- **Déchiffrer tout le disque amovible**. Si vous choisissez cette option, lors de l'application de la stratégie de Kaspersky Security Center avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security déchiffre tous les fichiers chiffrés qui se trouvent sur les disques amovibles ainsi que les systèmes de fichiers de ces disques, s'ils avaient été chiffrés.

  Cette option de chiffrement est assurée non seulement par la fonction de chiffrement des fichiers, mais aussi par la fonction de chiffrement du disque de l'application Kaspersky Endpoint Security.

- **Laisser tel quel**. Si vous choisissez cette option, lors de l'application de la stratégie de Kaspersky Security Center avec les paramètres de chiffrement des disques amovibles définis, Kaspersky Endpoint Security ne chiffre et ne déchiffre pas les fichiers sur les disques amovibles.

Kaspersky Endpoint Security prend en charge le chiffrement des systèmes de fichiers FAT32 et NTFS. Si l'option **Chiffrer tous les fichiers** ou **Chiffrer les nouveaux fichiers uniquement** est sélectionnée et qu'un lecteur amovible avec un système de fichiers non pris en charge est connecté à l'ordinateur, la tâche de chiffrement du lecteur amovible renvoie une erreur et Kaspersky Endpoint Security attribue un statut de lecture seule au lecteur amovible.

8. Créez des règles de chiffrement pour les fichiers sur des lecteurs amovibles dont vous souhaitez chiffrer le contenu.

9. Appliquez la stratégie.

Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Juste après l'application de la stratégie, si l'utilisateur connecte un disque amovible ou qu'un disque amovible est déjà connecté, Kaspersky Endpoint Security signale à l'utilisateur que la règle de chiffrement va être appliquée au disque amovible et que par conséquent, les données du disque amovible seront chiffrées.

Si la règle *Laisser tel quel* est spécifiée pour le chiffrement des données sur un lecteur amovible, l'application n'affiche aucune notification à l'utilisateur.

L'application signale à l'utilisateur que le chiffrement peut durer un certain temps.

L'application demande à l'utilisateur de confirmer l'exécution du chiffrement, puis réalise les opérations suivantes :

- Elle chiffre les données conformément aux paramètres de la stratégie si l'utilisateur confirme la demande de chiffrement.
- Elle ne chiffre pas les données si l'utilisateur rejette la demande de chiffrement et limite l'accès aux fichiers du disque amovible à la lecture.
- Elle ne chiffre pas les données si l'utilisateur ne répond pas à la demande de chiffrement, elle limite l'accès aux fichiers du disque amovible à la lecture et demandera à nouveau la confirmation du chiffrement des données lors de la prochaine application de la stratégie de Kaspersky Security Center ou lors de la prochaine connexion du disque amovible.

Une stratégie de Kaspersky Security Center avec les paramètres définis de chiffrement des données sur les disques amovibles est composée pour un groupe défini d'ordinateurs administrés. Par conséquent, le résultat du chiffrement des données des disques amovibles dépend de l'ordinateur auquel le disque amovible est connecté.

Si l'utilisateur tente de retirer le disque amovible pendant le chiffrement des données, Kaspersky Endpoint Security interrompt le chiffrement et permet le retrait du disque amovible avant la fin du chiffrement.

En cas d'échec du chiffrement du disque amovible, consultez le rapport **Chiffrement des données** dans l'interface de Kaspersky Endpoint Security. L'accès aux fichiers peut être bloqué par une autre application. Dans ce cas, essayez d'éjecter le disque amovible et de le connecter à nouveau à l'ordinateur.

Ajout d'une règle de chiffrement pour les disques amovibles

Pour ajouter une règles de chiffrement pour les disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Chiffrement des disques amovibles**.
7. Cliquez sur le bouton **Ajouter** et dans la liste déroulante, choisissez une des options suivantes :

   - Si vous voulez ajouter des règles de chiffrement pour les disques amovibles qui se trouvent dans la liste des périphériques de confiance du module Contrôle des périphériques, choisissez l'option **De la liste des périphériques de confiance de cette stratégie**.

     La fenêtre **Ajout d'appareils depuis la liste des appareils de confiance** s'ouvre.

   - Si vous voulez ajouter des règles de chiffrement pour les disques amovibles qui se trouvent dans la liste de Kaspersky Security Center, choisissez l'option **Depuis la liste des périphériques de Kaspersky Security**

Center.

La fenêtre **Ajout de périphériques de la liste Kaspersky Security Center** s'ouvre.

8. Si vous sélectionnez **Depuis la liste des appareils de Kaspersky Security Center** au cours de l'étape précédente, précisez les filtres permettant d'afficher les appareils dans le tableau. Pour ce faire, procédez comme suit :

   a. Définissez les valeurs des paramètres **Afficher un tableau des périphériques dont les paramètres suivants ont été définis**, **Nom**, **Ordinateur** et **Kaspersky Disk Encryptio**.

   b. Cliquez sur le bouton **Actualiser**.

9. Dans la liste déroulante **Mode de chiffrement des périphériques sélectionnés**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les fichiers stockés sur les disques amovibles sélectionnés.

10. Cochez la case **Mode portable** si vous souhaitez que Kaspersky Endpoint Security prépare les disques amovibles avant le chiffrement en vue de pouvoir manipuler les fichiers chiffrés qu'ils renferment en cas de connexion en mode portable.

    Le mode portable permet d'utiliser les fichiers chiffrés des disques amovibles sur les ordinateurs lorsque la fonction de chiffrement est inaccessible.

11. Cochez la case **Chiffrer uniquement l'espace occupé** si vous voulez que Kaspersky Endpoint Security chiffre uniquement les secteurs du disque qui sont occupés par des fichiers.

    Si vous appliquez le chiffrement à un disque déjà utilisé, il est recommandé de chiffrer tout le disque. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais dont les informations peuvent toujours être extraites. L'utilisation de la fonction **Chiffrer uniquement l'espace occupé** est recommandée pour les nouveaux disques jamais utilisés jusqu'à présent.

    Si l'appareil avait été chiffré à l'aide de la fonction **Chiffrer uniquement l'espace occupé**, après l'application de la stratégie en mode **Chiffrer tout le disque amovible**, les secteurs qui n'hébergent pas de fichiers ne seront toujours pas chiffrés.

12. Dans la liste déroulante **Action pour les périphériques sélectionnés auparavant**, sélectionnez l'action que Kaspersky Endpoint Security va effectuer sur les règles de chiffrement définies antérieurement pour les disques amovibles :

    - Si vous voulez que la règle de chiffrement du disque amovible créée auparavant reste sans inchangée, choisissez l'option **Ignorer**.
    - Si vous voulez que la règle de chiffrement du disque amovible créée auparavant soit remplacée par une nouvelle règle, choisissez l'option **Actualiser**.

13. Cliquez sur le bouton **OK**.

    Les lignes contenant les paramètres des règles de chiffrement créées s'affichent dans le tableau **Règles personnalisées**.

14. Cliquez sur **OK** pour enregistrer les modifications.

Les règles de chiffrement des disques amovibles ajoutées seront appliquées aux disques amovibles connectés à n'importe quel ordinateur soumis à la stratégie modifiée de Kaspersky Security Center.

Modification de la règle de chiffrement pour les disques amovibles

Pour modifier une règle de chiffrement pour un disque amovible, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Chiffrement des disques amovibles**.
7. Sélectionnez l'entrée de disque amovible qui vous intéresse dans la liste des disques amovibles pour lesquels des règles de chiffrement ont été définies.
8. Cliquez sur le bouton **Définir la règle** pour modifier la règle de chiffrement pour ce disque amovible.

   Le menu contextuel du bouton **Définir la règle** s'ouvre.
9. Dans le menu contextuel du bouton **Définir la règle**, sélectionnez l'action que Kaspersky Endpoint Security va exécuter sur les fichiers du disque amovibles sélectionné.
10. Cliquez sur **OK** pour enregistrer les modifications.

Les règles de chiffrement des disques amovibles modifiées seront appliquées aux disques amovibles connectés à n'importe quel ordinateur soumis à la stratégie modifiée de Kaspersky Security Center.

Activation du mode portable pour utiliser les fichiers chiffrés sur les disques amovibles

Pour activer le mode portable pour utiliser les fichiers chiffrés sur les disques amovibles, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Chiffrement des disques amovibles**.
7. Cochez la case **Mode portable**.

   Le mode portable est disponible uniquement si l'option **Chiffrer tous les fichiers** ou **Chiffrer uniquement les nouveaux fichiers** est sélectionnée dans la liste déroulante **Mode de chiffrement des appareils sélectionnés**.

8. Cliquez sur le bouton **OK**.

9. Appliquez la stratégie.

   Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

10. Connectez le disque amovible à l'ordinateur couvert par la stratégie de Kaspersky Security Center.

11. Confirmez l'opération de chiffrement du disque amovible.

    La fenêtre de création du mot de passe pour le gestionnaire de fichiers portable s'ouvre.

12. Définissez un mot de passe qui respecte les exigences en matière de complexité et confirmez-le.

13. Cliquez sur le bouton **OK**.

    Kaspersky Endpoint Security chiffrera les fichiers sur le disque amovible conformément aux règles de chiffrement définies dans la stratégie de Kaspersky Security Center. Le gestionnaire de fichiers portable pour la manipulation des fichiers chiffrés sera lui aussi enregistré sur le disque amovible.

Après l'activation du mode portable, l'utilisation des fichiers chiffrés devient accessible sur les disques amovibles connectés à l'ordinateur dont la fonction de chiffrement est inaccessible.

Déchiffrement des disques amovibles

Pour déchiffrer des disques amovibles, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Chiffrement des disques amovibles**.

7. Si vous souhaitez déchiffrer tous les fichiers chiffrés présents sur les disques amovibles, sélectionnez, dans la liste déroulante **Mode de chiffrement**, l'action **Déchiffrer tout le disque amovible**.

8. Si vous souhaitez déchiffrer des données enregistrées sur différents disques amovibles, modifiez les règles de chiffrement des disques amovibles dont vous souhaitez déchiffrer les données. Pour ce faire, procédez comme suit :

   a. Sélectionnez l'entrée de disque amovible qui vous intéresse dans la liste des disques amovibles pour lesquels des règles de chiffrement ont été définies.

   b. Cliquez sur le bouton **Définir la règle** pour modifier la règle de chiffrement pour ce disque amovible.

      Le menu contextuel du bouton **Définir la règle** s'ouvre.

   c. Dans le menu contextuel du bouton **Définir la règle**, sélectionnez l'option **Déchiffrer tous les fichiers**.

9. Cliquez sur **OK** pour enregistrer les modifications.

10. Appliquez la stratégie.

Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Juste après l'application de la stratégie, si l'utilisateur connecte un disque amovible ou si celui-ci est déjà connecté, Kaspersky Endpoint Security signale à l'utilisateur que la règle de chiffrement va être appliquée au disque amovible conformément à laquelle les fichiers chiffrés enregistrés sur le disque amovible ainsi que le système fichier du disque amovible, s'il est chiffré, seront déchiffrés. L'application signale à l'utilisateur que le déchiffrement peut durer un certain temps.

Une stratégie de Kaspersky Security Center avec les paramètres définis de chiffrement des données sur les disques amovibles est composée pour un groupe défini d'ordinateurs administrés. Par conséquent, le résultat du déchiffrement des données sur les disques amovibles dépend de l'ordinateur auquel le disque amovible est connecté.

Si l'utilisateur tente de retirer le disque amovible pendant le déchiffrement des données, Kaspersky Endpoint Security interrompt le déchiffrement des données et permet le retrait du disque amovible avant la fin du déchiffrement.

En cas d'échec du déchiffrement du disque amovible, consultez le rapport de **Chiffrement des données** dans l'interface de Kaspersky Endpoint Security. L'accès aux fichiers peut être bloqué par une autre application. Dans ce cas, essayez d'éjecter le disque amovible et de le connecter à nouveau à l'ordinateur.

Utilisation de l'Agent d'authentification

Si les disques durs système sont chiffrés, l'Agent d'authentification est chargé avant le démarrage du système d'exploitation. L'Agent d'authentification permet de réaliser la procédure d'authentification pour obtenir l'accès aux disques durs système chiffrés et pour démarrer le système d'exploitation.

Le système d'exploitation est chargé après la réussite de l'authentification. Lors des prochains redémarrage du système d'exploitation, il faudra suivre à nouveau la procédure d'authentification.

Il est possible que l'utilisateur ne puisse pas passer la procédure d'authentification. Par exemple, l'authentification est impossible si l'utilisateur a oublié les identifiants de l'Agent d'authentification ou le mot de passe du token ou de la carte à puce ou encore, s'il a perdu le token ou la carte à puce.

Si l'utilisateur a oublié les identifiants de l'Agent d'authentification ou le mot de passe du token ou de la carte à puce, il devra contacter l'administrateur du réseau local de l'entreprise pour la récupération de ces derniers.

Si l'utilisateur perd le token ou la carte à puce, l'administrateur doit ajouter le fichier du certificat électronique du token ou de la carte à puce de remplacement à la commande de création d'un compte utilisateur d'Agent d'authentification. Ensuite, l'utilisateur doit suivre la procédure d'obtention de l'accès aux appareils chiffrés ou de restauration des données sur les appareils chiffrés.

Utilisation du token et de la carte à puce lors de l'utilisation de l'Agent d'authentification

L'authentification en vue de À l'accès aux disques durs cryptés peut être réalisée à l'aide d'un token ou d'une carte à puce. Il faut pour cela ajouter le fichier du certificat électronique du token ou de la carte à puce dans la commande de création d'un compte utilisateur de l'Agent d'authentification.

L'utilisation du token ou de la carte à puce est disponible uniquement si les disques durs de l'ordinateur sont chiffrés à l'aide d'un algorithme AES256. Si les disques durs de l'ordinateur ont été chiffrés à l'aide d'un algorithme de chiffrement AES56, le fichier de certificat électronique ne pourra pas être ajouté à la commande.

Pour ajouter le fichier de certificat électronique du token ou de la carte à puce à la commande de création d'un compte utilisateur de l'Agent d'authentification, il faut d'abord l'enregistrer à l'aide d'une application tierce prévue pour l'administration des certificats.

Le certificat du token ou de la carte à puce doit posséder les propriétés suivantes :

- Le certificat doit être conforme à la norme X.509, tandis que le fichier de certificat doit avoir le codage DER.

  Si le certificat électronique du token ou de la carte à puce ne remplit pas cette condition, le plug-in d'administration ne charge pas le fichier de ce certificat dans la commande de création d'un compte utilisateur de l'Agent d'authentification et affiche une erreur.

- De même, le paramètre `KeyUsage`, qui définit le but du certificat, doit avoir la valeur `keyEncipherment` ou `dataEncipherment`.

  Si le certificat électronique du token ou de la carte à puce ne remplit pas cette condition, le plug-in d'administration charge le fichier de ce certificat dans la commande de création d'un compte utilisateur de l'Agent d'authentification avec un avertissement.

- Le certificat contient une clé RSA d'une longueur minimale de 1 024 bits.

  Si le certificat électronique du token ou de la carte à puce ne remplit pas cette condition, le plug-in d'administration ne charge pas le fichier de ce certificat dans la commande de création d'un compte utilisateur de l'Agent d'authentification et affiche une erreur.

Modification des textes d'aide de l'Agent d'authentification

Avant de modifier les textes d'aide de l'Agent d'authentification, prenez connaissance de la liste des caractères autorisés dans l'environnement préalable au chargement.

Pour modifier les textes d'aide de l'Agent d'authentification, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Paramètres généraux de chiffrement**.
7. Cliquez sur le bouton **Aide** dans le groupe **Modèles**.

La fenêtre **Textes d'aide de l'Agent d'authentification** s'ouvre.

8. Procédez comme suit :

   - Sélectionnez l'onglet **Authentification** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de saisie des identifiants.
   - Sélectionnez l'onglet **Modification du mot de passe** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de modification du mot de passe du compte utilisateur de l'Agent d'authentification.
   - Sélectionnez l'onglet **Restauration du mot de passe** si vous voulez modifier le texte d'aide affiché dans la fenêtre de l'Agent d'authentification à l'étape de restauration du mot de passe du compte utilisateur de l'agent d'authentification.

9. Modifiez les textes d'aide.

   Si vous voulez restaurer le texte original, cliquez sur le bouton **Par défaut**.

   > Vous pouvez saisir un texte d'aide qui contient 16 lignes maximum. Chaque ligne peut compter au maximum 64 caractères.

10. Cliquez sur le bouton **OK**.
11. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.

Restrictions de prise en charge des caractères dans les textes d'aide de l'Agent d'authentification

L'environnement préalable au chargement prend en charge les caractères Unicode suivants :

- alphabet latin général (0000 - 007F) ;
- suppléments Latin-1 (0080 - 00FF) ;
- latin étendu A (0100 - 017F) ;
- latin étendu B (0180 - 024F) ;
- lettres modificatives avec chasse (02B0 - 02FF) ;
- diacritiques (0300 - 036F) ;
- grec et copte (0370 - 03FF) ;
- cyrillique (0400 - 04FF) ;
- hébreu (0590 - 05FF) ;
- arabe (0600 - 06FF) ;
- latin étendu additionnel (1E00 - 1EFF) ;

- caractères de ponctuation (2000 - 206F) ;
- symboles monétaires (20A0 - 20CF) ;
- symboles de type lettre (2100 - 214F) ;
- formes géométriques (25A0 - 25FF) ;
- formes B de présentation arabes (FE70 - FEFF).

Les caractères qui ne figurent pas dans cette liste ne sont pas pris en charge dans l'environnement préalable au démarrage. Il est déconseillé d'utiliser de tels caractères dans les textes d'aide de l'agent d'authentification.

Sélection du niveau de traçage de l'Agent d'authentification

L'application consigne dans le fichier de traçage les informations de service sur le fonctionnement de l'Agent d'authentification, ainsi que les informations relatives aux actions réalisées par l'utilisateur dans l'Agent d'authentification.

Pour modifier le niveau de traçage de l'Agent d'authentification, procédez comme suit :

1. Directement après le démarrage de l'ordinateur doté de disques durs chiffrés, appuyez sur la touche **F3** afin d'ouvrir la fenêtre de configuration de l'Agent d'authentification.
2. Sélectionnez le niveau de traçage souhaité dans la fenêtre de configuration des paramètres de l'Agent d'authentification :
   - **Disable debug logging (default)**. Si vous choisissez cette option, l'application ne consigne pas dans le fichier de traçage les informations relatives aux événements survenus pendant le fonctionnement de l'Agent d'authentification.
   - **Enable debug logging**. Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification.
   - **Enable verbose logging**. Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations détaillées relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification.

     Le niveau de détail des entrées dans ce cas est plus élevé qu'au niveau **Enable debug logging**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

   - **Enable debug logging and select serial port**. Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations relatives au fonctionnement de l'Agent d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification et les transmet également via le port COM.

     Si l'ordinateur avec les disques durs chiffrés est connecté à un autre ordinateur via le port COM, les événements survenus pendant le fonctionnement de l'Agent d'authentification peuvent être étudiés l'aide de cet ordinateur.

   - **Enable verbose debug logging and select serial port**. Si vous choisissez cette option, l'application consigne dans le fichier de traçage les informations détaillées relatives au fonctionnement de l'Agent

d'authentification et aux actions réalisées par l'utilisateur dans l'Agent d'authentification et les transmet également via le port COM.

Le niveau de détails des entrées dans ce cas est plus élevé qu'au niveau **Enable debug logging and select serial port**. Un niveau de détail élevé peut ralentir le chargement de l'Agent d'authentification et du système d'exploitation.

L'écriture dans le fichier de traçage de l'Agent d'authentification a lieu si l'ordinateur est doté de disques durs chiffrés ou si le chiffrement du disque est en cours.

Le fichier de traçage de l'Agent d'authentification n'est pas transmis à Kaspersky comme les autres fichiers de traçage de l'application. Le cas échéant, vous pouvez envoyer le fichier de traçage de l'Agent d'authentification à Kaspersky pour analyse.

Administration des comptes utilisateur de l'Agent d'authentification

Les outils suivants de Kaspersky Security Center permettent de gérer les comptes utilisateur de l'Agent d'authentification :

- Tâche de groupe d'administration des comptes de l'Agent d'authentification. Cette tâche permet de gérer les comptes utilisateur de l'Agent d'authentification pour un groupe de postes client.
- Tâche locale **Chiffrement de l'ensemble du support, administration des comptes**. Elle permet de gérer les comptes utilisateur de l'Agent d'authentification pour des postes clients séparés.

Pour configurer les paramètres de la tâche d'administration des comptes utilisateur de l'Agent d'authentification, procédez comme suit :

1. Créez (Création d'une tâche locale, Création d'une tâche de groupe) une tâche de gestion des comptes de l'Agent d'authentification.
2. Ouvrez la section **Paramètres** dans la fenêtre **Propriétés : <nom de la tâche d'administration des comptes de l'Agent d'authentification>**.
3. Ajoutez des commandes de création de comptes utilisateur de l'Agent d'authentification.
4. Ajoutez des commandes de modification de comptes utilisateur de l'Agent d'authentification.
5. Ajoutez des commandes de suppression de comptes utilisateur de l'Agent d'authentification.
6. Si besoin, modifiez les commandes ajoutées pour administrer les comptes utilisateur de l'Agent d'authentification. Pour ce faire, sélectionnez une commande dans le tableau **Commandes d'administration des comptes utilisateur de l'Agent d'authentification**, puis cliquez sur le bouton **Modifier**.
7. Si besoin, supprimez les commandes ajoutées pour administrer les comptes utilisateur de l'Agent d'authentification. Pour ce faire, sélectionnez au moins une commande dans le tableau **Commandes d'administration des comptes utilisateur de l'Agent d'authentification**, puis cliquez sur le bouton **Supprimer**.

Pour sélectionner plusieurs lignes dans le tableau, sélectionnez-les en maintenant la touche **CTRL** enfoncée.

8. Cliquez sur le bouton **OK** dans la fenêtre des propriétés de la tâche afin d'enregistrer les modifications introduites.

9. Exécutez la tâche.

Les commandes d'administration des comptes utilisateur de l'Agent d'authentification ajoutées à la tâche seront exécutées.

Ajout d'une commande de création d'un compte utilisateur de l'Agent d'authentification

Pour ajouter une commande de création d'un compte utilisateur de l'Agent d'authentification, procédez comme suit :

1. Ouvrez la section **Paramètres** dans la fenêtre **Propriétés : <nom de la tâche d'administration des comptes de l'Agent d'authentification>**.

2. Cliquez sur le bouton **Ajouter** et, dans la liste déroulante, choisissez l'option **Commande d'ajout de compte**.

   La fenêtre **Ajout d'un compte utilisateur** s'ouvre.

3. Dans le champ **Ajout d'un compte utilisateur** de la fenêtre **Compte Windows**, indiquez le nom du compte Microsoft Windows à partir duquel le compte de l'Agent d'authentification sera créé.

   Pour ce faire, saisissez le nom du compte manuellement ou cliquez sur le bouton **Sélectionner**.

4. Si vous avez saisi manuellement le nom d'un compte Microsoft Windows, cliquez sur le bouton **Autoriser** pour déterminer l'identifiant de sécurité (SID) du compte.

   Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

   La définition de l'identificateur de sécurité du compte utilisateur Microsoft Windows lors de l'ajout de la commande de création d'un compte utilisateur de l'Agent d'authentification peut être pratique afin de vérifier l'exactitude du nom de compte utilisateur Microsoft Windows saisi manuellement. Si le compte utilisateur Microsoft Windows saisi n'existe pas sur l'ordinateur ou dans le domaine de confiance pour lequel la tâche locale **Chiffrement de l'ensemble du support, administration des comptes**, alors la tâche d'administration des comptes de l'Agent d'authentification se solde sur une erreur.

5. Cochez la case **Remplacer le compte existant** si vous souhaitez qu'un compte utilisateur portant ce nom déjà saisi pour cet Agent de l'authentification soit remplacé par le compte ajouté.

   Cette étape est accessible si vous ajoutez une commande de création d'un compte utilisateur de l'Agent d'authentification dans les propriétés de la tâche de groupe d'administration des comptes utilisateur de l'Agent d'authentification. Cette étape n'est pas disponible si vous ajoutez une commande de création d'un compte utilisateur de l'Agent d'authentification dans les propriétés de la tâche locale **Chiffrement du disque, administration des comptes utilisateur**.

6. Dans le champ **Nom d'utilisateur**, saisissez le nom du compte utilisateur de l'Agent d'authentification à saisir lors de la procédure d'authentification pour accéder aux disques durs chiffrés.

7. Cochez la case **Autoriser l'ouverture de session par mot de passe**, si vous souhaitez que l'application demande le mot de passe du compte utilisateur de l'Agent d'authentification lors de l'authentification pour l'accès aux disques durs chiffrés.

8. Si vous avez coché la case **Autoriser l'ouverture de session par mot de passe** à l'étape précédente :

   a. Dans le champ **Mot de passe**, saisissez le mot de passe du compte de l'Agent d'authentification à saisir lors de la procédure d'authentification pour accéder aux disques durs chiffrés.

   b. Dans le champ **Confirmation du mot de passe**, confirmez le mot de passe du compte de l'Agent d'authentification saisi à l'étape précédente.

   c. Exécutez une des actions suivantes :

   - Sélectionnez l'option **Modifier le mot de passe à la première authentification** si vous voulez que l'application affiche une demande de modification de mot de passe à l'utilisateur qui passe l'authentification sous le compte indiqué la commande pour la première fois.

   - Dans le cas contraire, sélectionnez l'option **Ne pas exiger le changement du mot de passe**.

9. Cochez la case **Autoriser l'ouverture de session par le certificat** si vous souhaitez que l'application exige la connexion du jeton ou de la carte à puce à l'ordinateur lors de l'authentification pour accéder aux disques durs chiffrés.

10. Si vous avez coché la case **Autoriser l'ouverture de session par certificat** à l'étape précédente, cliquez sur le bouton **Parcourir** et sélectionnez le fichier du certificat électronique du token ou de la carte à puce dans la fenêtre **Sélectionner le fichier du certificat**.

11. Le cas échéant, saisissez dans le champ **Description de la commande** des informations sur le compte utilisateur de l'Agent d'authentification indispensables pour utiliser la commande.

12. Exécutez une des actions suivantes :

    - Choisissez l'option **Autoriser l'authentification** si vous souhaitez que l'application autorise l'accès à l'authentification dans l'Agent d'authentification pour l'utilisateur qui travaille sous le compte utilisateur repris dans la commande.

    - Choisissez l'option **Interdire l'authentification** si vous souhaitez que l'application interdise l'accès à l'authentification dans l'Agent d'authentification pour l'utilisateur qui travaille sous le compte utilisateur repris dans la commande.

13. Dans la fenêtre **Ajout d'un compte utilisateur**, cliquez sur **OK**.

Ajout d'une commande pour la modification d'un compte utilisateur de l'Agent d'authentification

Pour ajouter une commande de modification d'un compte utilisateur de l'Agent d'authentification, procédez comme suit :

1. Dans la section **Paramètres** de la fenêtre **Propriétés : <nom de la tâche d'administration des comptes de l'Agent d'authentification>**, ouvrez le menu contextuel du bouton **Ajouter** et sélectionnez l'élément **Commande de modification de compte**.

   La fenêtre **Modification du compte utilisateur** s'ouvre.

2. Dans le champ **Compte Windows** de la fenêtre **Modification du compte utilisateur**, indiquez le nom du compte utilisateur Microsoft Windows à partir duquel le compte utilisateur de l'Agent d'authentification que vous souhaitez modifier a été créé. Pour ce faire, saisissez le nom du compte manuellement ou cliquez sur le bouton **Sélectionner**.

3. Si vous avez saisi manuellement le nom d'un compte utilisateur Microsoft Windows, cliquez sur le bouton **Autoriser** pour déterminer l'identifiant de sécurité (SID) du compte utilisateur.

   Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

   La définition de l'identificateur de sécurité du compte utilisateur Microsoft Windows lors de l'ajout de la commande de modification d'un compte utilisateur de l'Agent d'authentification peut être pratique pour vérifier l'exactitude du nom de compte utilisateur Microsoft Windows saisi manuellement. Si le compte utilisateur Microsoft Windows indiqué n'existe pas ou appartient à un domaine non approuvé, la tâche de groupe pour l'administration des comptes de l'Agent d'authentification se termine par une erreur.

4. Cochez la case **Modifier le nom d'utilisateur** et saisissez le nouveau nom pour le compte utilisateur de l'Agent d'authentification si vous souhaitez que l'application Kaspersky Endpoint Security remplace le nom de l'utilisateur par celui repris dans le champ ci-dessous pour tous les comptes utilisateur de l'Agent d'authentification créés sur la base du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

5. Cochez la case **Modifier les paramètres de l'ouverture de session par mot de passe** si vous souhaitez pouvoir modifier les paramètres d'entrée par mot de passe.

6. Cochez la case **Autoriser l'ouverture de session par mot de passe**, si vous souhaitez que l'application demande le mot de passe du compte utilisateur de l'Agent d'authentification lors de l'authentification pour l'accès aux disques durs chiffrés.

7. Si vous avez coché la case **Autoriser l'ouverture de session par mot de passe** à l'étape précédente :

   a. Dans le champ **Mot de passe**, saisissez le nouveau mot de passe du compte de l'Agent d'authentification.

   b. Dans le champ **Confirmation du mot de passe**, confirmez le mot de passe saisi à l'étape précédente.

8. Cochez la case **Modifier la règle de changement du mot de passe lors de l'authentification dans l'Agent d'authentification** et saisissez le nouveau mot de passe pour le compte utilisateur de l'Agent d'authentification si vous souhaitez que l'application Kaspersky Endpoint Security remplace le mot de passe par celui repris dans le champ ci-dessous pour tous les comptes de l'Agent d'authentification créés à partir du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

9. Définissez la valeur du paramètre de modification du mot de passe lors de l'authentification dans l'Agent d'authentification.

10. Cochez la case **Modifier les paramètres de l'ouverture de session par certificat** si vous souhaitez pouvoir modifier les paramètres d'entrée par certificat électronique du token ou carte à puce.

11. Cochez la case **Autoriser l'ouverture de session par le certificat**, si vous souhaitez que l'application demande de saisir le mot de passe du token ou de la carte à puce connecté à l'ordinateur lors de l'authentification pour l'accès aux disques durs chiffrés.

12. Si vous avez coché la case **Autoriser l'ouverture de session par certificat** à l'étape précédente, cliquez sur le bouton **Parcourir** et sélectionnez le fichier du certificat électronique du token ou de la carte à puce dans la fenêtre **Sélectionner le fichier du certificat**.

13. Cochez la case **Modifier la description de la commande** et modifiez la description si vous souhaitez que l'application Kaspersky Endpoint Security modifie la description de la commande pour tous les comptes utilisateur de l'Agent d'authentification créés sur la base du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

14. Cochez la case **Modifier la règle d'accès à l'authentification dans l'Agent d'authentification** si vous souhaitez que l'application Kaspersky Endpoint Security remplace la règle d'accès de l'utilisateur à l'authentification dans l'Agent d'authentification par la valeur ci-dessous pour tous les comptes utilisateur de l'Agent d'authentification créés à partir du compte utilisateur Microsoft Windows portant le nom repris dans le champ **Compte Windows**.

15. Définissez la règle d'accès à l'authentification dans l'Agent d'authentification.

16. Dans la fenêtre **Modification du compte utilisateur**, cliquez sur **OK**.

Ajout d'une commande pour la suppression d'un compte utilisateur de l'Agent d'authentification

Pour ajouter une commande de suppression du compte utilisateur de l'Agent d'authentification, procédez comme suit :

1. Dans la section **Paramètres** de la fenêtre **Propriétés : <nom de la tâche d'administration des comptes de l'Agent d'authentification>**, ouvrez le menu contextuel du bouton **Ajouter** et sélectionnez **Commande de suppression de compte**.

   La fenêtre **Suppression du compte utilisateur** s'ouvre.

2. Dans le champ **Compte Windows** de la fenêtre **Suppression du compte utilisateur**, indiquez le nom du compte utilisateur Microsoft Windows à partir duquel le compte utilisateur de l'Agent d'authentification que vous souhaitez supprimer a été créé. Pour ce faire, saisissez le nom du compte manuellement ou cliquez sur le bouton **Sélectionner**.

3. Si vous avez saisi manuellement le nom d'un compte utilisateur Microsoft Windows, cliquez sur le bouton **Autoriser** pour déterminer l'identifiant de sécurité (SID) du compte utilisateur.

   Si vous ne définissez pas l'identificateur de sécurité à l'aide du bouton **Autoriser**, celui-ci sera défini lors de l'exécution de la tâche sur l'ordinateur.

   > La définition de l'identificateur de sécurité du compte utilisateur Microsoft Windows lors de l'ajout de la commande de suppression d'un compte utilisateur de l'Agent d'authentification peut être pratique pour vérifier l'exactitude du nom de compte utilisateur Microsoft Windows saisi manuellement. Si le compte utilisateur Microsoft Windows indiqué n'existe pas ou appartient à un domaine non approuvé, la tâche de groupe pour l'administration des comptes de l'Agent d'authentification se termine par une erreur.

4. Dans la fenêtre **Suppression du compte utilisateur**, cliquez sur **OK**.

Restauration des identifiants de l'Agent d'authentification

> Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

Pour restaurer le nom et le mot de passe du compte utilisateur de l'Agent d'authentification, procédez comme suit :

1. Avant le démarrage du système d'exploitation sur l'ordinateur comportant les disques durs chiffrés, l'Agent d'authentification est chargé. Dans l'interface de l'Agent d'authentification, cliquez sur le bouton **Mot de passe**

oublié pour lancer le processus de restauration du nom d'utilisateur et du mot de passe du compte de l'Agent d'authentification.

2. Suivez les instructions de l'Agent d'authentification pour obtenir les blocs de la requête afin de restaurer le nom et le mot de passe du compte utilisateur de l'Agent d'authentification.

3. Dictez le contenu des groupes de demande à l'administrateur du réseau local de l'entreprise ainsi que le nom de l'ordinateur.

4. Entrez les sections de la réponse à la demande de restauration du nom d'utilisateur et du mot de passe du compte de l'Agent d'authentification qui ont été générées et vous ont été fournies par l'administrateur du réseau local.

5. Saisissez le nouveau mot de passe pour le compte utilisateur de l'Agent d'authentification et sa confirmation.

   Le nom du compte utilisateur de l'Agent d'authentification est défini à l'aide des groupes de réponse à la demande de restauration du nom d'utilisateur et du mot de passe de l'Agent d'authentification.

Après la saisie et la confirmation du nouveau mot de passe du compte de l'Agent d'authentification, le mot de passe sera enregistré, et l'accès aux disques durs chiffrés sera octroyé.

Réponse à la demande de récupération des identifiants de l'Agent d'authentification de l'utilisateur

Pour former et transmettre à l'utilisateur des groupes de réponse à la demande de récupération du nom et du mot de passe du compte utilisateur de l'Agent d'authentification, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur de l'utilisateur ayant demandé la restauration du nom d'utilisateur et du mot de passe du compte de l'Agent d'authentification.

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

4. Dans l'onglet **Appareils**, sélectionnez l'ordinateur de l'utilisateur qui a demandé la restauration du nom et du mot de passe du compte de l'Agent d'authentification et effectuez un clic droit pour ouvrir le menu contextuel.

5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.

   La fenêtre **Autoriser l'accès en mode hors ligne** s'ouvre.

6. Dans la fenêtre **Autoriser l'accès en mode hors ligne**, choisissez l'onglet **Agent d'authentification**.

7. Dans la section **Algorithme de chiffrement utilisé**, sélectionnez le type d'algorithme de chiffrement.

8. Sélectionnez le nom du compte utilisateur de l'Agent d'authentification, créé pour l'utilisateur à l'origine de la demande de récupération du nom et du mot de passe du compte utilisateur de l'Agent d'authentification, dans la liste déroulante **Compte**.

9. Dans la liste déroulante **Disque dur**, choisissez le disque dur chiffré auquel il faut rétablir l'accès.

10. Dans le groupe **Codes de l'utilisateur**, saisissez les groupes de demande dictés par l'utilisateur.

    Les contenus des sections de réponse à la demande de l'utilisateur de restaurer le nom et le mot de passe du compte utilisateur de l'Agent d'authentification s'affichent alors dans le champ **Clé d'accès**.

11. Dictez le contenu des groupes de réponse à l'utilisateur.

Consultation des informations relatives au chiffrement des données

Cette section explique comment consulter les informations relatives aux données chiffrées.

A propos des états de chiffrement

Pendant le chiffrement et le déchiffrement des données, Kaspersky Security Center reçoit de Kaspersky Endpoint Security des informations sur l'application des paramètres de chiffrement sur les postes clients.

Chaque ordinateur peut avoir un des états de chiffrement suivants :

- *Aucune stratégie de chiffrement définie*. Aucune stratégie de chiffrement de Kaspersky Security Center n'a été attribuée à l'ordinateur.
- *En cours d'application d'une stratégie*. Le chiffrement et/ou le déchiffrement des données est en cours sur l'ordinateur.
- *Erreur*. Une erreur s'est produite lors du chiffrement et/ou du déchiffrement des données sur l'ordinateur.
- *Redémarrage requis*. Pour initialiser ou terminer le chiffrement ou le déchiffrement des données sur l'ordinateur, il faut redémarrer le système d'exploitation.
- *Conforme à la stratégie*. Le chiffrement des données sur l'ordinateur est exécuté conformément aux paramètres de chiffrement indiqués dans la stratégie de Kaspersky Security Center appliquée à l'ordinateur.
- *Annulé par l'utilisateur*. L'utilisateur n'a pas confirmé l'exécution de l'opération de chiffrement des fichiers sur le disque amovible.

Consultation des états du chiffrement

Pour consulter les états de chiffrement des données de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur qui vous intéresse.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.

   L'onglet **Périphériques** dans l'espace de travail reprend les propriétés des ordinateurs du groupe d'administration sélectionné.
4. Sous l'onglet **Périphériques** de l'espace de travail, déplacez le curseur au maximum à droite.
5. Si la colonne **État de chiffrement** ne s'affiche pas, procédez comme suit :
   1. Cliquez-droit pour ouvrir le menu contextuel des titres du tableau.

2. Dans le menu contextuel, ouvrez la liste déroulante **Apparence** et choisissez **Ajouter ou supprimer des colonnes**.

   La fenêtre **Ajout ou suppression de colonnes** s'ouvre.

3. Dans la fenêtre **Ajout ou suppression de colonnes**, cochez la case **État de chiffrement**.

4. Cliquez sur le bouton **OK**.

La colonne **État de chiffrement** reprend les états de chiffrement des données pour les ordinateurs du groupe d'administration sélectionné. Cet état est obtenu sur la base des informations relatives au chiffrement des fichiers sur les disques locaux de l'ordinateur et au chiffrement du disque.

Consultation des statistiques de chiffrement sur les volets d'informations de Kaspersky Security Center

Pour consulter les états de chiffrement sur les barres d'informations de Kaspersky Security Center, procédez comme suit :

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

2. Dans l'arborescence de la console, choisissez l'entrée **Serveur d'administration – <Nom de l'ordinateur>**.

3. Dans l'espace de travail situé à droite de l'arborescence de la Console de l'administration, choisissez l'onglet **Statistiques**.

4. Créez une page avec les volets d'informations contenant les statistiques du chiffrement des données. Pour ce faire, procédez comme suit :

   a. Sous l'onglet **Statistiques**, cliquez sur le bouton **Configurer l'apparence**.

      La fenêtre **Propriétés : Statistiques** s'ouvre.

   b. Dans la fenêtre **Propriétés : Statistiques** qui s'ouvre, cliquez sur **Ajouter**.

      La fenêtre **Propriétés : Nouvelle page** s'ouvre.

   c. Saisissez le nom de la page dans la section **Général** de la fenêtre **Propriétés : Nouvelle page**.

   d. Dans la section **Volets d'informations** , cliquez sur **Ajouter**.

      La fenêtre **Nouveau panneau d'informations** s'ouvre.

   e. Dans le groupe **État de la protection** de la fenêtre **Nouveau panneau d'informations**, choisissez l'option **Chiffrement des périphériques**.

   f. Cliquez sur le bouton **OK**.

      La fenêtre **Propriétés : Chiffrement des périphériques** s'ouvre.

   g. Modifiez les paramètres de la barre d'informations en fonction de besoins. Utilisez pour ce faire les options des sections **Apparence** et **Périphériques** de la fenêtre **Propriétés : Chiffrement des périphériques**.

   h. Cliquez sur le bouton **OK**.

   i. Répétez les étapes d à h des instructions et dans la section **État de la protection** de la fenêtre **Nouveau panneau d'informations**, sélectionnez l'option **Chiffrement des disques amovibles**.

Les barres d'informations ajoutées figurent dans la liste **Barres d'informations** de la fenêtre **Propriétés : Nouvelle page**.

j. Dans la fenêtre **Propriétés : Nouvelle page**, cliquez sur **OK**.

Le nom des pages contenant les barres d'informations créées aux étapes antérieures apparaît dans la liste **Pages** de la fenêtre **Propriétés : Statistiques**.

k. Dans la fenêtre **Propriétés : Statistiques**, cliquez sur **Fermer**.

5. Sous l'onglet **Statistiques**, ouvrez la page créée aux étapes antérieures des instructions.

Les barres d'informations qui reprennent les états de chiffrement des ordinateurs et des disques amovibles s'affichent.

Consultation des erreurs de chiffrement des fichiers sur les disques locaux de l'ordinateur

Pour consulter les erreurs de chiffrement des fichiers sur les disques durs locaux de l'ordinateur, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration où se trouve l'ordinateur de l'utilisateur pour lequel vous souhaitez consulter la liste des erreurs de chiffrement des fichiers.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sous l'onglet **Périphériques**, sélectionnez l'ordinateur dans la liste et ouvrez le menu contextuel d'un clic droit.
5. Exécutez une des actions suivantes :
   - Dans le menu contextuel de l'ordinateur, sélectionnez l'option **Protection**.
   - Dans le menu contextuel de l'ordinateur, sélectionnez l'option **Propriétés**. Dans la fenêtre **Propriétés: <nom de l'ordinateur>** qui s'ouvre, sélectionnez la section **Endpoint Protection**.
6. Dans la section **Endpoint Protection** de la fenêtre **Propriétés: <nom de l'ordinateur>** à l'aide du lien **Consulter les erreurs de chiffrement des données**, ouvrez la fenêtre **Erreurs de chiffrement des données**.

   Celle-ci reprend les informations relatives aux erreurs de chiffrement des fichiers sur les disques durs locaux de l'ordinateur. Si l'erreur a été corrigée, Kaspersky Security Center supprime les informations qui la concernent dans la fenêtre **Erreurs de chiffrement des données**.

Consultation du rapport sur le chiffrement des données

Pour consulter le rapport sur le chiffrement des données, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.

3. Cliquez sur le bouton **Nouveau modèle de rapport**.

   L'Assistant de création du modèle du rapport démarre.

4. Suivez les instructions de l'Assistant de création du modèle de rapport. Dans la section **Autre** de la fenêtre **Sélection du type de modèle du rapport**, sélectionnez une des options suivantes :

   - **Rapport de l'état de chiffrement des appareils administrés**.
   - **Rapport de l'état de chiffrement des appareils mémorisés**.
   - **Rapport sur les erreurs de chiffrement de fichiers**.
   - **Rapport sur le blocage de l'accès aux fichiers chiffrés**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.

5. Choisissez le modèle de rapport créé aux étapes précédentes.

6. Dans le menu contextuel du modèle, sélectionnez l'option **Afficher le rapport**.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Utilisation des fichiers chiffrés avec la fonction de chiffrement des fichiers limitée

Lors de l'application de la stratégie de Kaspersky Security Center et du chiffrement postérieur des fichiers, Kaspersky Endpoint Security reçoit la clé de chiffrement indispensable pour l'accès direct aux fichiers chiffrés. L'utilisateur, connecté sous n'importe quel compte utilisateur Windows actif au moment du chiffrement des fichiers, bénéficie, grâce à la clé de chiffrement, d'un accès direct aux fichiers chiffrés. L'utilisateur connecté sous un compte Windows inactif au moment du chiffrement des fichiers doit se connecter à Kaspersky Security Center pour pouvoir accéder aux fichiers chiffrés.

Les fichiers chiffrés peuvent être inaccessibles dans les cas suivants :

- Des clés de chiffrement existent sur l'ordinateur de l'utilisateur, mais il n'y a aucune connexion à Kaspersky Security Center pour pouvoir utiliser des clés. Dans ce cas, l'utilisateur doit solliciter l'accès aux fichiers chiffrés à l'administrateur du réseau local de l'organisation.

  En l'absence de communication avec Kaspersky Security Center il faut :

  - Demander une clé d'accès pour accéder aux fichiers chiffrés sur les disques durs de l'ordinateur ;
  - Demander une clé d'accès aux fichiers chiffrés de chaque disque amovible pour accéder aux fichiers chiffrés sur les disques amovibles.

- Les modules de chiffrement ont été supprimés de l'ordinateur de l'utilisateur. Dans ce cas, l'utilisateur peut ouvrir les fichiers chiffrés sur les disques locaux et les disques amovibles, mais le contenu des fichiers s'affiche comme chiffré.

  L'utilisateur peut travailler avec les fichiers chiffrés dans les conditions suivantes :

  - Les fichiers se trouvent dans des archives chiffrées créées sur l'ordinateur à l'aide de l'application Kaspersky Endpoint Security installée.

- Les fichiers se trouvent sur des disques amovibles pour lesquels le fonctionnement en mode portable est autorisé.

Accès aux fichiers chiffrés en l'absence de connexion à Kaspersky Security Center

Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

Pour pouvoir accéder aux fichiers chiffrés en l'absence de connexion à Kaspersky Security Center, procédez comme suit :

1. Sollicitez le fichier chiffré auquel vous souhaitez accéder.

   En l'absence de connexion à Kaspersky Security Center au moment où le fichier est sollicité, Kaspersky Endpoint Security crée un fichier de requête d'accès à tous les fichiers chiffrés enregistrés sur les disques locaux de l'ordinateur, si vous aviez sollicité un fichier enregistré sur un disque local. Kaspersky Endpoint Security crée un fichier de requête d'accès à tous les fichiers chiffrés enregistrés sur un disque amovible si vous aviez sollicité un fichier enregistré sur un disque amovible. La fenêtre **L'accès au fichier est interdit** s'ouvre.

2. Envoyez la requête d'accès aux fichiers chiffrés portant l'extension kesdc à l'administrateur du réseau local de l'organisation. Pour ce faire, exécutez une des actions suivantes :

   - Cliquez sur le bouton **Envoyer par email** afin d'envoyer le fichier de requête d'accès aux fichiers chiffrés par courrier électronique à l'administrateur du réseau local de l'organisation.

   - Cliquez sur le bouton **Enregistrer** afin d'enregistrer le fichier de requête d'accès aux fichiers chiffrés et de le transmettre à l'administrateur du réseau local de l'entreprise d'une autre façon.

3. Recevez le fichier clé d'accès aux fichiers chiffrés, créé et envoyé par l'administrateur du réseau local de l'entreprise.

4. Vous pouvez activer la clé d'accès aux fichiers chiffrés par l'un des moyens suivants :

   - Dans n'importe quel gestionnaire de fichiers, sélectionnez le fichier clé d'accès aux fichiers chiffrés. Et double-cliquez pour l'ouvrir.

   - Procédez comme suit :

     a. Ouvrez la fenêtre principale de Kaspersky Endpoint Center.

     b. Cliquez sur le bouton .

        La fenêtre **Événements** s'ouvre.

     c. Sélectionnez l'onglet **État de l'accès aux fichiers et périphériques**.

        L'onglet affiche la liste de toutes les demandes d'accès aux fichiers chiffrés.

     d. Choisissez la requête pour laquelle vous avez obtenu le fichier clé d'accès aux fichiers chiffrés.

     e. Cliquez sur le bouton **Parcourir** afin de charger le fichier clé d'accès aux fichiers chiffrés obtenu.

        La fenêtre standard de Microsoft Windows **Sélection du fichier clé d'accès** s'ouvre.

f. Dans la fenêtre standard Microsoft Windows **Sélection du fichier clé d'accès**, sélectionnez le fichier portant l'extension kesdr envoyé par l'administrateur du réseau local de l'organisation et dont le nom correspond au nom du fichier du fichier clé d'accès correspondant.

g. Cliquez sur le bouton **Ouvrir**.

h. Dans la fenêtre **Événements**, cliquez sur **OK**.

Kaspersky Endpoint Security octroie l'accès à tous les fichiers chiffrés enregistrés sur les disques locaux de l'ordinateur, si le fichier de requête d'accès a été créé lors de l'accès à un fichier enregistré sur le disque local de l'ordinateur. Kaspersky Endpoint Security octroie l'accès à tous les fichiers chiffrés enregistrés sur le disque amovible si le fichier de requête d'accès a été créé lors de l'accès à un fichier enregistré sur un disque amovible. Pour pouvoir accéder aux fichiers chiffrés enregistrés sur d'autres disques amovibles, il faut obtenir les clés d'accès propres à ces disques amovibles.

Octroi à l'utilisateur de l'accès aux fichiers chiffrés en l'absence de connexion à Kaspersky Security Center

Pour permettre à l'utilisateur d'accéder aux fichiers chiffrés en l'absence de connexion à Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur de l'utilisateur qui a sollicité l'accès aux fichiers chiffrés.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sous l'onglet **Périphériques**, sélectionnez l'ordinateur qui a sollicité l'accès aux fichiers chiffrés et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.

   La fenêtre **Autoriser l'accès en mode hors ligne** s'ouvre.
6. Dans la fenêtre **Autoriser l'accès en mode hors ligne**, choisissez l'onglet **Chiffrement**.
7. Sous l'onglet **Chiffrement**, cliquez sur **Parcourir**.

   La fenêtre standard de Microsoft Windows **Choix du fichier de requête** s'ouvre.
8. Dans la fenêtre **Choix du fichier de requête**, indiquez le chemin d'accès au fichier de requête obtenu de l'utilisateur, puis cliquez sur **Ouvrir**.

   Kaspersky Security Center crée le fichier clé d'accès aux fichiers chiffrés. L'onglet **Chiffrement** reprend les informations relatives à la demande de l'utilisateur.
9. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Envoyer par email** afin d'envoyer le fichier clé d'accès aux fichiers chiffrés à l'utilisateur par courrier électronique.
   - Cliquez sur le bouton **Enregistrer** afin d'enregistrer le fichier clé d'accès aux fichiers chiffrés et de le transmettre à l'utilisateur d'une autre façon.

Modification des modèles de messages pour l'octroi de l'accès aux fichiers chiffrés

Pour modifier les modèles de messages pour l'octroi de l'accès aux fichiers chiffrés, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Chiffrement des données**, sélectionnez la sous-section **Paramètres généraux de chiffrement**.
7. Dans le groupe **Modèles**, cliquez sur le bouton **Modèles**.
   La fenêtre **Modèles** s'ouvre.
8. Procédez comme suit :
   - Si vous souhaitez modifier le modèle du message de l'utilisateur, sélectionnez l'onglet **Message de l'utilisateur**. Lorsque l'utilisateur tente d'accéder au fichier chiffré alors que la clé d'accès à ceux-ci ne figure pas sur l'ordinateur, la fenêtre **Accès au fichier refusé** s'ouvre. Quand vous cliquez sur le bouton **Envoyer par email** de la fenêtre **Accès au fichier refusé**, le message de l'utilisateur se rédige automatiquement. Ce message est envoyé à l'administrateur du réseau local de l'entreprise avec un fichier de demande d'accès aux fichiers chiffrés.
   - Si vous souhaitez modifier le modèle du message pour l'administrateur, sélectionnez l'onglet **Message de l'administrateur**. Ce message est composé automatiquement lorsque vous cliquez sur le bouton **Envoyer par email** dans la fenêtre **Demande d'accès aux fichiers chiffrés**. L'utilisateur le reçoit une fois qu'il a obtenu l'accès aux fichiers chiffrés.
9. Modifiez le modèle de message.
   Vous pouvez utiliser le bouton **Par défaut** et la liste déroulante **Variable**.
10. Cliquez sur le bouton **OK**.
11. Pour enregistrer vos modifications, dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur **OK**.

Utilisation des périphériques chiffrés en l'absence d'accès à ceux-ci.

Obtention de l'accès au périphérique chiffrés

L'utilisateur peut devoir solliciter l'accès aux périphériques chiffrés dans les cas suivants :

- Le disque dur a été chiffré sur un autre ordinateur.

- L'ordinateur est privé de la clé de chiffrement pour le périphérique (par exemple, lors de la première sollicitation d'un disque amovible chiffré sur cet ordinateur) et il n'y a pas de communication avec Kaspersky Security Center.

  Après que l'utilisateur a activé la clé d'accès au périphérique chiffré, Kaspersky Endpoint Security enregistre la clé de chiffrement sur l'ordinateur de l'utilisateur et octroie l'accès à ce périphérique pour les requêtes suivantes, même en l'absence de communication avec Kaspersky Security Center.

L'obtention de l'accès aux périphériques chiffrés s'opère de la manière suivante :

1. L'utilisateur crée via l'interface de l'application Kaspersky Endpoint Security la requête d'accès au fichier avec l'extension kesdc et la transmet à son administrateur du réseau local de l'organisation.
2. L'administrateur crée le fichier clé d'accès dans la Console d'administration de Kaspersky Security Center avec l'extension kesdr et la transmet à l'utilisateur.
3. L'utilisateur applique la clé d'accès.

Restauration des données sur les périphériques chiffrés.

Pour utiliser les périphériques chiffrés, l'utilisateur peut utiliser l'utilitaire de restauration des périphériques chiffrés (ci-après, l'utilitaire de restauration). Ce besoin peut se présenter dans les situations suivantes :

- Échec de la procédure d'obtention de l'accès à l'aide de la clé d'accès
- Absence des modules de chiffrement sur l'ordinateur avec l'appareil chiffré

Les données nécessaires à la restauration de l'accès aux appareils à l'aide de l'utilitaire de restauration se trouvent pendant quelque temps dans la mémoire de l'ordinateur de l'utilisateur en clair. Pour réduire la probabilité d'un accès non autorisé à ces données, il est conseillé d'exécuter la restauration de l'accès aux périphériques chiffrés sur des ordinateurs de confiance.

La restauration des données sur les périphériques chiffrés s'opère de la manière suivantes :

1. L'utilisateur crée une requête d'accès au fichier à l'aide de l'utilitaire de restauration et transmet ce fichier portant l'extension fdertc à l'administrateur du réseau local de l'organisation.
2. L'administrateur crée le fichier clé d'accès dans la Console d'administration de Kaspersky Security Center avec l'extension fdertr et la transmet à l'utilisateur.
3. L'utilisateur applique la clé d'accès.

Pour restaurer les données sur les disques durs système chiffrés, l'utilisateur peut également indiquer les identifiants de l'Agent d'authentification dans l'utilitaire de restauration. Si les métadonnées du compte utilisateur de d'Agent d'authentification sont endommagées, l'utilisateur devra réaliser la procédure de restauration à l'aide de la requête d'accès au fichier.

Avant de restaurer les données sur les appareils chiffrés, il est conseillé d'annuler l'application de la stratégie de Kaspersky Security Center ou de désactiver le chiffrement dans les paramètres de la stratégies de Kaspersky Security Center sur l'ordinateur sur lequel la procédure va être exécutée. Ceci permet d'éviter un nouveau chiffrement du périphérique.

Obtention de l'accès aux périphériques chiffrés via l'interface de l'application

Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

Pour obtenir l'accès aux périphériques chiffrés via l'interface de l'application, procédez comme suit :

1. Sollicitez le périphérique chiffré auquel vous souhaitez accéder.

   La fenêtre **L'accès aux données est interdit** s'ouvre.

2. Envoyez la requête d'accès au fichier au périphérique chiffré portant l'extension kesdc à l'administrateur du réseau local de l'organisation. Pour ce faire, exécutez une des actions suivantes :

   - Cliquez sur le bouton **Envoyer par email** afin d'envoyer la requête d'accès au fichier chiffré par courrier électronique à l'administrateur du réseau local de l'organisation.
   - Cliquez sur le bouton **Enregistrer** afin d'enregistrer la requête d'accès au fichier chiffré et de la transmettre à l'administrateur du réseau local de l'entreprise d'une autre façon.

   Si vous avez fermé la fenêtre **L'accès aux données est interdit**, sans avoir enregistré la requête d'accès au fichier ou sans l'avoir envoyée à l'administrateur du réseau local de l'organisation, vous pouvez le faire à tout moment dans la fenêtre **Événements** de l'onglet **État de l'accès aux fichiers et périphériques**. Pour ouvrir cette fenêtre, cliquez sur le bouton dans la fenêtre principale de l'application.

3. Recevez et enregistrez le fichier clé d'accès au périphérique chiffré, créé et envoyé par l'administrateur du réseau local de l'entreprise.

4. Vous pouvez activer la clé d'accès au périphérique chiffré à l'aide d'un des moyens suivants :

   - Dans n'importe quel gestionnaire de fichiers, sélectionnez le fichier clé d'accès au périphérique chiffré et double-cliquez pour l'ouvrir.
   - Procédez comme suit :

     a. Ouvrez la fenêtre principale de Kaspersky Endpoint Center.

     b. Cliquez sur le bouton pour ouvrir la fenêtre **Événements**.

     c. Sélectionnez l'onglet **État de l'accès aux fichiers et périphériques**.

     L'onglet affiche la liste de toutes les demandes d'accès aux fichiers chiffrés et aux disques amovibles.

     d. Choisissez la requête pour laquelle vous avez obtenu le fichier clé d'accès périphérique chiffré.

     e. Cliquez sur le bouton **Parcourir** afin de charger le fichier clé d'accès au périphérique chiffré obtenu.

     La fenêtre standard de Microsoft Windows **Sélection du fichier clé d'accès** s'ouvre.

     f. Dans la fenêtre standard Microsoft Windows **Sélection du fichier clé d'accès**, sélectionnez le fichier portant l'extension kesdr envoyé par l'administrateur du réseau local de l'organisation et dont le nom correspond au nom de la requête d'accès correspondante au périphérique chiffré.

g. Cliquez sur le bouton **Ouvrir**.

h. Dans la fenêtre **État de l'accès aux fichiers et périphériques**, cliquez sur **OK**.

Ainsi, Kaspersky Endpoint Security octroie l'accès au périphérique chiffré.

Octroi de l'accès aux appareils chiffrés à l'utilisateur

Pour octroyer à l'utilisateur l'accès au périphérique chiffré, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur de l'utilisateur qui a sollicité l'accès au périphérique chiffré.
3. Dans l'espace de travail, sélectionnez l'onglet **Périphériques**.
4. Sous l'onglet **Périphériques**, sélectionnez l'ordinateur qui a sollicité l'accès au périphérique chiffré et d'un clic droit, ouvrez le menu contextuel.
5. Dans le menu contextuel, choisissez l'option **Autoriser l'accès en mode hors ligne**.

   La fenêtre **Autoriser l'accès en mode hors ligne** s'ouvre.
6. Dans la fenêtre **Autoriser l'accès en mode hors ligne**, choisissez l'onglet **Chiffrement**.
7. Sous l'onglet **Chiffrement**, cliquez sur **Parcourir**.

   La fenêtre standard de Microsoft Windows **Choix du fichier de requête** s'ouvre.
8. Dans la fenêtre **Choix du fichier de requête**, indiquez le chemin d'accès à la requête d'accès au fichier obtenue de l'utilisateur, puis cliquez sur Ouvrir.
9. Cliquez sur le bouton **Ouvrir**.

   Kaspersky Security Center formera le fichier clé d'accès au périphérique chiffré avec l'extension kesdr. L'onglet **Chiffrement** reprend les informations relatives à la demande de l'utilisateur.
10. Exécutez une des actions suivantes :

    - Cliquez sur le bouton **Envoyer par email** afin d'envoyer le fichier clé d'accès aux fichiers chiffrés à l'utilisateur par courrier électronique.
    - Cliquez sur le bouton **Enregistrer** afin d'enregistrer le fichier clé d'accès au périphérique chiffré et de le transmettre à l'utilisateur d'une autre façon.

Remise à l'utilisateur de la clé de récupération pour les disques durs chiffrés à l'aide de BitLocker

Pour remettre à l'utilisateur la clé de récupération pour le disque dur système chiffré à l'aide de BitLocker, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration auquel appartient l'ordinateur de l'utilisateur qui a sollicité l'accès au disque chiffré.

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

4. Sous l'onglet **Appareils**, sélectionnez l'ordinateur appartenant à l'utilisateur qui a sollicité l'accès au disque chiffré.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Autoriser l'accès en mode hors ligne**.

   La fenêtre **Autoriser l'accès en mode hors ligne** s'ouvre.

6. Dans la fenêtre **Autoriser l'accès en mode hors ligne**, choisissez l'onglet **Accès au disque système avec protection BitLocker**.

7. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération**.

   Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

8. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Pour transmettre à l'utilisateur la clé de récupération de l'accès pour un disque dur hors système chiffré à l'aide de BitLocker, procédez comme suit :

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

2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé → Chiffrement et protection des données → Appareils chiffrés**.

   Dans la zone de travail, la liste des périphériques chiffrés s'affiche.

3. Dans l'espace de travail, choisissez l'appareil chiffré auquel vous souhaitez restaurer l'accès.

4. D'un clic-droit, ouvrez le menu contextuel et choisissez l'option **Obtenir l'accès au périphérique dans Kaspersky Endpoint Security for Windows**.

   Cette action ouvre la fenêtre **Restauration de l'accès au disque chiffré à l'aide de BitLocker**.

5. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération**.

   Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

6. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Création du fichier exécutable de l'utilitaire de restauration

Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

Pour créer un fichier exécutable de l'utilitaire de restauration, procédez comme suit :

1. Dans la fenêtre principale de l'application cliquez sur **Support Technique** situé dans le coin inférieur gauche de la fenêtre principale de l'application.
2. Dans la fenêtre **Support**, cliquez sur le bouton **Restauration d'un appareil chiffré**.

   L'utilitaire de restauration des périphériques chiffrés est lancé.
3. Dans la fenêtre de l'utilitaire de restauration, cliquez sur le bouton **Créer un utilitaire de restauration portable**.

   La fenêtre **Création d'un utilitaire de restauration portable** s'ouvre.
4. Dans la fenêtre **Enregistrer dans**, saisissez manuellement le chemin d'accès au dossier où sera enregistré le fichier exécutable de l'utilitaire de restauration ou cliquez sur le bouton **Parcourir**.
5. Dans la fenêtre **Création d'un utilitaire de restauration portable**, cliquez sur **OK**.

   Le fichier exécutable de l'utilitaire de restauration fdert.exe sera conservé dans le dossier indiqué.

Restauration des données sur les périphériques chiffrés à l'aide de l'utilitaire de restauration

Ces instructions s'adressent aux utilisateurs de postes client dotés de l'application Kaspersky Endpoint Security.

Pour restaurer l'accès au périphérique chiffré à l'aide de l'utilitaire de restauration, procédez comme suit :

1. Lancez l'utilitaire de restauration par l'un des moyens suivants :

   - Cliquez sur le bouton **Support Technique** dans la fenêtre principale de l'application Kaspersky Endpoint Security pour ouvrir la fenêtre **Support Technique**, puis cliquez sur le bouton **Restauration d'un périphérique chiffré**.
   - Exécutez le fichier exécutable fdert.exe de l'utilitaire de restauration. Ce fichier est créé par Kaspersky Endpoint Security.
2. Dans la fenêtre de l'utilitaire de restauration dans la liste déroulante **Sélectionnez un périphérique**, sélectionnez le périphérique chiffré auquel vous souhaitez restaurer l'accès.
3. Cliquez sur le bouton **Analyser** pour que l'utilitaire puisse définir l'action à exécuter sur le périphérique chiffré : débloquer ou déchiffrer.

   Si la fonction de chiffrement de Kaspersky Endpoint Security est disponible sur l'ordinateur, l'utilitaire de restauration propose de débloquer le périphérique. Lors du déblocage, l'appareil n'est pas déchiffré. Il est simplement possible d'y accéder directement. Si la fonction de chiffrement de Kaspersky Endpoint Security n'est pas disponible sur l'ordinateur, l'utilitaire de restauration propose de déchiffrer le périphérique.
4. Si vous voulez importer des informations de diagnostic, procédez comme suit :

a. Cliquez sur le bouton **Sauvegarder le diagnostic**.

La fenêtre **Règlement sur l'octroi de données** s'ouvre.

b. Prenez connaissance des dispositions du Règlement sur l'octroi de données et acceptez-le en cliquant sur le bouton **OK**

La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvre.

c. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le dossier dans lequel vous voulez enregistrer l'archive avec les fichiers contenant les informations de diagnostic.

5. Cliquez sur le bouton **Réparer le MBR** si le diagnostic du système du disque dur chiffré a généré un message qui vous signale des problèmes liés au secteur de démarrage principal (MBR) du périphérique.

La réparation du secteur de démarrage principal peut accélérer la récupération d'informations indispensables au déblocage ou au déchiffrement du périphérique.

6. Appuyez sur le bouton **Débloquer** ou **Déchiffrer** en fonction des résultats du diagnostic.

La fenêtre **Paramètres de déblocage du périphérique** ou **Paramètres de déchiffrement du périphérique** s'ouvre.

7. Si vous voulez restaurer les données avec l'aide du compte utilisateur de l'Agent d'authentification, procédez comme suit :

a. Choisissez l'option **Utiliser les paramètres du compte utilisateur de l'Agent d'authentification**.

b. Dans les champs **Nom** et **Mot de passe**, indiquez les identifiants de l'Agent d'authentification.

Cette méthode est disponible uniquement en cas de restauration des données sur le disque dur système. Si le disque dur système ont été endommagées ou si vous avez oublié les données du compte utilisateur de l'Agent d'authentification, il faudra obtenir une clé d'accès auprès de l'administrateur du réseau local de l'organisation pour restaurer les données sur le périphérique chiffré.

8. Si vous voulez restaurer les données à l'aide de la clé d'accès, procédez comme suit :

a. Choisissez l'option **Désigner manuellement la clé d'accès au périphérique**.

b. Appuyez sur le bouton **Obtenir la clé d'accès**.

La fenêtre **Obtenir la clé d'accès au périphérique** s'ouvre.

c. Appuyez sur le bouton **Enregistrer** et choisissez le dossier dans lequel vous allez enregistrer la requête d'accès au fichier avec l'extension fdertc.

d. Transmettez la requête d'accès au fichier à l'administrateur du réseau local de l'organisation.

Ne fermez pas la fenêtre **Obtenir la clé d'accès au périphérique** tant que vous n'aurez pas reçu la clé d'accès. Si vous ouvrez à nouveau cette fenêtre, la clé d'accès créée antérieurement par l'administrateur ne pourra pas être appliquée.

e. Recevez et enregistrez le fichier clé créé et transmis par l'administrateur du réseau local de l'organisation.

f. Cliquez sur le bouton **Télécharger** et dans la fenêtre qui s'ouvre choisissez le fichier clé d'accès portant l'extension fdertr.

9. Si vous déchiffrer le périphérique, la fenêtre **Paramètres de déchiffrement du périphérique** permet de définir les paramètres restant du déchiffrement. Pour ce faire, procédez comme suit :

- Indiquez la zone du déchiffrement :
  - Si vous voulez déchiffrer tout le périphérique, choisissez l'option **Déchiffrer tout le périphérique**.
  - Si vous voulez déchiffrer une partie des données sur le périphérique, choisissez l'option **Déchiffrer certains secteurs du périphérique** et définissez les limites de la zone de déchiffrement à l'aide des champs **Début** et **Fin**.
- Choisissez l'emplacement de l'enregistrement des données déchiffrées :
  - Si vous voulez que les données du périphérique original soient écrasées par les données déchiffrées, décochez la case **Déchiffrement dans le fichier d'image de disque**.
  - Si vous voulez enregistrer les données déchiffrées séparément des données originales chiffrées, cochez la case **Déchiffrement dans le fichier d'image de disque** et à l'aide du bouton **Parcourir**, indiquez le chemin de l'emplacement où il faudra enregistrer le fichier au format VHD.

10. Cliquez sur le bouton **OK**.

Le déblocage/le déchiffrement du périphérique est lancé.

Réponse à la demande de l'utilisateur sur la restauration des données sur les périphériques chiffrés

Pour créer et transmettre à l'utilisateur le fichier clé d'accès à l'appareil chiffré, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé → Chiffrement et protection des données → Appareils chiffrés**.
3. Dans l'espace de travail, choisissez le périphérique chiffré pour lequel vous voulez créer un fichier clé l'accès, puis, dans le menu contextuel du périphérique, choisissez l'option **Obtenir l'accès au périphérique dans Kaspersky Endpoint Security for Windows**.

   Si vous n'êtes pas certain de connaître l'ordinateur pour lequel la requête d'accès au fichier a été créée, choisissez dans l'arborescence de la console d'administration le dossier **Avancé → Chiffrement et protection des données**, puis, dans l'espace de travail, cliquez sur le lien **Obtenir la clé de chiffrement du périphérique dans Kaspersky Endpoint Security for Windows**.

   La fenêtre **Octroi de l'accès à l'appareil** s'ouvre.

4. Choisissez l'algorithme de chiffrement à utiliser. Choisissez une des options suivantes :
   - **AES256**, si l'application Kaspersky Endpoint Security sur l'ordinateur où le périphérique a été chiffré a été installée à l'aide d'un paquet de la distribution situé dans le dossier aes256 ;
   - **AES56**, si l'application Kaspersky Endpoint Security sur l'ordinateur où le périphérique a été chiffré a été installée à l'aide d'un paquet de distribution situé dans le dossier aes56.
5. Cliquez sur le bouton **Parcourir**.

   La fenêtre standard de Microsoft Windows **Choix du fichier de requête** s'ouvre.

6. Dans la fenêtre **Choix du fichier de requête**, indiquez le chemin d'accès à la requête d'accès au fichier avec l'extension fdertc obtenue de l'utilisateur.

7. Cliquez sur le bouton **Ouvrir**.

   Kaspersky Security Center formera le fichier clé d'accès au périphérique chiffré avec l'extension fdertr.

8. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Envoyer par email** afin d'envoyer le fichier clé d'accès aux fichiers chiffrés à l'utilisateur par courrier électronique.

   - Cliquez sur le bouton **Enregistrer** afin d'enregistrer le fichier clé d'accès au périphérique chiffré et de le transmettre à l'utilisateur d'une autre façon.

Restauration de l'accès aux données chiffrées en cas de panne du système d'exploitation

La restauration de l'accès aux données en cas de panne du systèmes d'exploitation est disponible uniquement pour le chiffrement des fichiers (FLE). Il est impossible de restaurer l'accès aux données en cas de chiffrement du disque (FDE).

Pour restaurer l'accès aux données chiffrées en cas de panne du système d'exploitation, procédez comme suit :

1. Réinstallez le système d'exploitation sans formater le disque dur.

2. Installez Kaspersky Endpoint Security.

3. Établissez la connexion entre l'ordinateur et le Serveur d'administration de Kaspersky Security Center qui gère l'ordinateur pendant le chiffrement des données.

   L'accès aux données chiffrées sera octroyé sous les mêmes conditions que celles en vigueur avant la panne du système d'exploitation.

Création d'un disque de dépannage du système d'exploitation

Un disque de dépannage peut être utile quand, pour une raison quelconque, l'accès au disque dur système chiffré n'est pas possible et que le système d'exploitation ne peut être chargé.

Vous pouvez charger une image du système d'exploitation Windows à l'aide du disque de dépannage et restaurer l'accès au disque dur système chiffré à l'aide de l'utilitaire de restauration repris dans l'image du système d'exploitation.

Pour créer un disque de dépannage du système d'exploitation, procédez comme suit :

1. Créez le fichier exécutable de l'utilitaire de restauration des périphériques chiffrés.

2. Créez l'image utilisateur de l'environnement de pré-installation Windows. Pendant cette procédure, ajoutez l'image du fichier exécutable de l'utilitaire de restauration des périphériques chiffrés.

3. Placez l'image utilisateur de l'environnement de pré-installation Windows sur un support amovible tel qu'un CD ou d'un disque amovible.

   Les instructions relatives à la création de l'image utilisateur de l'environnement de pré-installation Microsoft figurent dans l'aide de Microsoft (par exemple, sur le site de Microsoft TechNet).

Contrôle des applications

Cette section contient des informations sur le Contrôle des applications et les instructions sur la configuration des paramètres du module.

Présentation du Contrôle des applications

Le composant Contrôle des applications surveille les tentatives de démarrage des applications par les utilisateurs et régit le démarrage des applications à l'aide des *règles de Contrôle des applications*.

Le lancement des applications dont aucun paramètre ne respecte les règles de Contrôle des applications est régi par le mode sélectionné de fonctionnement du module. Le mode *Liste noire* est sélectionné par défaut. Ce mode permet à n'importe quel utilisateur de lancer n'importe quelle application. Quand l'utilisateur tente de lancer une application interdite par les règles de Contrôle des applications, Kaspersky Endpoint Security bloque le lancement de cette application (si l'action **Appliquer les règles** a été choisie) ou enregistre les informations relatives au lancement de l'application dans le rapport (si l'action **Tester les règles** a été choisie).

Toutes les tentatives de l'utilisateur visant à lancer des applications sont consignées dans des rapports.

Administration des règles du Contrôle des applications

Cette section contient des informations sur la configuration du Contrôle des applications à l'aide de Kaspersky Security Center ainsi que des recommandations sur l'utilisation optimale du Contrôle des applications.

Récupération des informations relatives aux applications installées sur les ordinateurs des utilisateurs

Pour créer des règles optimales pour le Contrôle des applications, il est conseillé de s'informer sur les applications utilisées par les ordinateurs du réseau local de l'entreprise. Pour ce faire, vous pouvez obtenir les informations suivantes :

- les éditeurs, les versions et les localisations des applications utilisées dans le réseau local de l'entreprise ;
- la fréquence des mises à jour des applications ;
- les stratégies d'utilisation des applications adoptées dans l'entreprise (il peut s'agir de stratégies de sécurité ou de stratégies d'administration) ;
- l'emplacements des stockages des distributions des applications.

Pour récupérer les informations relatives aux applications utilisées sur les ordinateurs du réseau local de l'entreprise, vous devez utiliser les données présentées dans les dossiers **Registre des applications** et **Fichiers exécutables**. Les dossiers **Registre des applications** et **Fichiers exécutables** font partie du dossier **Administration des applications** de l'arborescence de la Console d'administration de Kaspersky Security Center.

Le dossier **Registre des applications** contient la liste des applications détectées sur les postes clients par l'Agent d'administration installé sur ces postes.

Le dossier **Fichiers exécutables** contient la liste des fichiers exécutables lancés à un moment ou l'autre sur les postes clients ou détectés pendant l'exécution de la tâche d'inventaire pour Kaspersky Endpoint Security.

Après avoir ouvert la fenêtre des propriétés de l'application sélectionnée dans le dossier **Registre des applications** ou **Fichiers exécutables**, vous pouvez obtenir les informations générales sur l'application ou sur ses fichiers exécutables ainsi que consulter la liste des ordinateurs sur lesquels cette application est installée.

*Pour ouvrir la fenêtre des propriétés des applications dans le dossier **Registre des applications**, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Administration des applications** → **Registre des applications**.
3. Sélectionnez l'application.
4. Dans le menu contextuel de l'application, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés <nom de l'application>** s'ouvre.

*Pour ouvrir la fenêtre des propriétés du fichier exécutable dans le dossier **Fichiers exécutables**, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Administration des applications** → **Fichiers exécutables**.
3. Choisissez le fichier exécutable.
4. Dans le menu contextuel du fichier exécutable, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés <nom du fichier exécutable>** s'ouvre.

Création des catégories d'applications

Pour simplifier la création de règles de Contrôle des applications, vous pouvez créer des catégories d'applications.

Il est conseillé de créer une catégorie "Applications pour le travail" qui reprend la sélection standard d'applications utilisées dans l'entreprise. Si différents groupes d'utilisateurs utilisent différentes sélections d'applications, vous pouvez créer une catégorie d'applications distincte pour chaque groupe d'utilisateurs.

Pour créer ou modifier une catégorie d'applications, procédez comme suit :

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

2. Dans l'arborescence de la Console de l'administration, choisissez le dossier **Avancé** → **Administration des applications** → **Catégories d'applications**.

3. Dans la zone de travail, cliquez sur **Créer une catégorie**.

   L'Assistant de création de catégories personnalisée s'ouvre.

4. Suivez les instructions de l'Assistant de création de catégories personnalisées.

Étape 1. Sélection du type de catégorie

Cette étape permet de choisir un des types suivants de catégories d'applications :

- **Catégorie enrichie manuellement**. Si vous avez choisi ce type de catégorie, vous pouvez définir à l'étape "Configuration des conditions d'inclusion des applications dans une catégorie" et à l'étape "Configuration des conditions d'exclusion des applications hors d'une catégorie" les critères selon lesquels les fichiers exécutables sont repris dans la catégorie créée.

- **Catégorie qui contient les fichiers exécutables des appareils sélectionnés**. Si vous avez choisi ce type de catégorie, vous pourrez à l'étape "Paramètres" désigner l'appareil dont les fichiers exécutables doivent se retrouver dans la catégorie.

- **Catégorie qui contient les fichiers exécutables du dossier sélectionné**. Si vous avez choisi ce type de catégorie, vous pourrez à l'étape "Dossier de stockage" désigner le dossier dont les fichiers exécutables seront repris automatiquement dans la catégorie créée.

  Lors de la création de la catégorie enrichie automatiquement, Kaspersky Security Center réalise l'inventaire des formats de fichiers suivants : EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX et SCR.

Étape 2. Saisie du nom de la catégorie personnalisée

Indiquez à cette étape le nom de la catégorie d'applications.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 3. Configuration des conditions d'inclusion des applications dans une catégorie

Cette étape n'est pas proposée si vous avez choisi le type de catégorie **Catégorie enrichie manuellement**.

A cette étape, dans la liste déroulante **Ajouter**, sélectionnez une ou plusieurs des conditions suivantes d'ajout des applications dans la catégorie :

- **De la liste des fichiers exécutables**. Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.

- **Des propriétés du fichier**. Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des application à la catégorie personnalisée.

- **Métadonnées des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les métadonnées de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.

- **Hash des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les hash de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.

- **Certificats des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables signés par les certificats. Kaspersky Security Center désigne les certificats de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.

  Il est déconseillé d'utiliser les conditions dont les propriétés ne définissent pas le paramètre **Empreinte du certificat**.

- **Métadonnées des fichiers de l'installateur MSI**. Choisissez le package d'installation MSI. Kaspersky Security Center désigne les métadonnées des fichiers exécutables contenus dans ce package d'installation MSI en tant que condition d'ajout des applications à la catégorie personnalisée.

- **Sommes de contrôle des fichiers du programme d'installation mis de l'application**. Choisissez le package d'installation au format MSI. Kaspersky Security Center désigne les hash des fichiers exécutables contenus dans ce package d'installation MSI en tant que condition d'ajout des applications à la catégorie personnalisée.

- **Catégorie KL**. Indiquez la catégorie KL en tant que condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.

  Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.

- **Dossier de l'application**. Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.

- **Certificats du stockage de certificats**. Sélectionnez les certificats de signature des fichiers exécutables en guise de condition d'ajout des applications à la catégorie personnalisée.

  Il est déconseillé d'utiliser les conditions dont les propriétés ne définissent pas le paramètre **Empreinte du certificat**.

- **Type de support**. Indiquez le type de périphérique de stockage (tous les disques durs et les disques amovibles ou uniquement les disques amovibles) en tant que condition d'ajout des applications à la catégorie utilisateur.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 4. Configuration des conditions d'exclusions des applications hors d'une catégorie

Cette étape n'est pas proposée si vous avez choisi le type de catégorie **Catégorie enrichie manuellement**.

Les applications renseignées à cette étape sont exclues de la catégorie, même si ces applications avaient été renseignées à l'étape "Configuration des conditions d'inclusion des applications dans une catégorie".

A cette étape, dans la liste déroulante **Ajouter**, sélectionnez une des conditions suivantes d'exclusion des applications hors de la catégorie :

- **De la liste des fichiers exécutables**. Ajoutez les applications de la liste des fichiers exécutables sur l'appareil client dans la catégorie personnalisée.
- **Des propriétés du fichier**. Indiquez les données détaillées des fichiers exécutables en tant que condition d'ajout des application à la catégorie personnalisée.
- **Métadonnées des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les métadonnées de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Hash des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables. Kaspersky Security Center désigne les hash de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Certificats des fichiers du dossier**. Choisissez le dossier sur l'appareil client qui contient les fichiers exécutables signés par les certificats. Kaspersky Security Center désigne les certificats de ces fichiers exécutables en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Métadonnées des fichiers de l'installateur MSI**. Choisissez le package d'installation MSI. Kaspersky Security Center désigne les métadonnées des fichiers exécutables contenus dans ce package d'installation MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Sommes de contrôle des fichiers du programme d'installation mis de l'application**. Choisissez le package d'installation au format MSI. Kaspersky Security Center désigne les hash des fichiers exécutables contenus dans ce package d'installation MSI en tant que condition d'ajout des applications à la catégorie personnalisée.
- **Catégorie KL**. Indiquez la catégorie KL en tant que condition d'ajout d'applications à la catégorie personnalisée. Une *catégorie KL* est une liste d'applications qui ont des attributs de thèmes communs. La liste est actualisée par les experts de Kaspersky. Par exemple, la catégorie KL "Suites bureautiques" reprend les applications des suites Microsoft Office, Adobe Acrobat et d'autres.

  Vous pouvez choisir toutes les catégories KL afin de composer une liste étendue d'applications de confiance.
- **Dossier de l'application**. Choisissez le dossier sur l'appareil client. Kaspersky Security Center ajoute les fichiers exécutables de ce dossier à la catégorie personnalisée.
- **Certificats du stockage de certificats**. Sélectionnez les certificats de signature des fichiers exécutables en guise de condition d'ajout des applications à la catégorie personnalisée.
- **Type de support**. Indiquez le type de périphérique de stockage (tous les disques durs et les disques amovibles ou uniquement les disques amovibles) en tant que condition d'ajout des applications à la catégorie utilisateur.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 5. Paramètres

Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui contient les fichiers exécutables des appareils sélectionnés**.

A cette étape, cliquez sur le bouton **Ajouter** et indiquez les ordinateurs dont les fichiers exécutables vont être ajoutés par Kaspersky Security Center à la catégorie d'applications. Kaspersky Security Center ajoute à la catégorie d'applications tous les fichiers exécutables des ordinateurs indiqués et repris dans le dossier **Fichiers exécutables**.

Cette étape permet également de configurer les paramètres suivants :

- algorithme de calcul du hash par l'application Kaspersky Security Center. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :
  - La case **Calculer SHA-256 pour les fichiers de la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows versions ultérieures)**.
  - La case **Calculer MD5 pour les fichiers de la catégorie (pris en charge dans les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- la case **Synchroniser les données avec le stockage du Serveur d'administration**. Cochez cette case si vous voulez que Kaspersky Security Center nettoie périodiquement la catégorie d'applications et y ajoute tous les fichiers exécutables des ordinateurs indiqués présentés dans le dossier **Fichiers exécutables**.

  Si la case **Synchronisation des données avec le stockage du Serveur d'administration** est décochée, Kaspersky Security Center ne va pas modifier la catégorie d'applications après sa création.
- Champ **Période d'analyse (h)**. Ce champ permet de définir le délai, en heures, à l'issue duquel Kaspersky Security Center nettoie la catégorie d'applications et y ajoute tous les fichiers exécutables des ordinateurs qui figurent dans le dossier **Fichiers exécutables**.

  Le champ est accessible quand la case **Synchronisation des données avec le stockage du Serveur d'administration** est cochée.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 6. Dossier du stockage

Cette étape est disponible si vous avez sélectionné le type de catégorie **Catégorie qui contient les fichiers exécutables du dossier sélectionné**.

Dans le cadre de cette étape, cliquez sur le bouton **Parcourir** et indiquez le dossier dans lequel Kaspersky Security Center doit exécuter la recherche de fichiers exécutables en vue d'un ajout automatique à la catégorie d'applications.

Cette étape permet également de configurer les paramètres suivants :

- La case **Inclure les bibliothèques de liens dynamiques (DLL) dans la catégorie**. Cochez cette case si vous voulez que la catégorie d'applications accueille les bibliothèques de liens dynamiques (fichiers au format DLL) et que le composant Contrôle des applications enregistre les actions de ces bibliothèques lancées dans le système.

  Lorsque des fichiers DLL sont ajoutés à une catégorie d'applications, il se peut que les performances de Kaspersky Security Center diminuent.
- Case **Inclure les données sur les scripts dans la catégorie**. Cochez cette case si vous voulez que la catégorie d'applications reprenne les données sur les scripts et que les scripts ne soient pas bloqués par le composant Protection contre les menaces Internet.

Lorsque les données sur les scripts sont ajoutées à une catégorie d'applications, il se peut que les performances de Kaspersky Security Center diminuent.

- algorithme de calcul du hash par l'application Kaspersky Security Center. Pour sélectionner l'algorithme, il faut cocher au moins une des cases suivantes :
  - La case **Calculer SHA-256 pour les fichiers de la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows versions ultérieures)**.
  - La case **Calculer MD5 pour les fichiers de la catégorie (pris en charge dans les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- la case **Forcer la recherche de modifications dans le dossier**. Cochez cette case si vous voulez que Kaspersky Security Center recherche à intervalle régulier des fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications.

  Si la case **Forcer la recherche de modifications dans le dossier** est décochée, Kaspersky Security Center recherche des fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications uniquement en cas de modification, d'ajout ou de suppression de fichiers dans ce dossier.
- Champ **Période d'analyse (h)**. Ce champ permet de définir, en heures, la période à l'issue de laquelle Kaspersky Security Center recherche la présence de fichiers exécutables dans le dossier d'enrichissement automatique des catégories d'applications.

  Le champ est accessible si la case **Forcer la recherche de modifications dans le dossier** est cochée.

Pour poursuivre avec l'Assistant d'installation, cliquez sur le bouton **Suivant**.

Étape 7. Création d'une catégorie personnalisée

Pour quitter l'Assistant d'installation de l'application, cliquez sur **Terminer**.

Ajout à une catégorie d'applications de fichiers exécutables issus du dossier Fichiers exécutables

Le dossier **Fichiers exécutables** affiche la liste des fichiers exécutables détectés sur les ordinateurs. Kaspersky Endpoint Security compose la liste des fichiers exécutables après l'exécution de la tâche d'inventaire.

*Pour jouter des fichiers du dossier **Fichiers exécutables** à la catégorie d'applications, procédez comme suit :*

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Avancé** de l'arborescence de la Console d'administration, dans le dossier **Administration des applications**, sélectionnez le dossier **Fichiers exécutables**.
3. Dans l'espace de travail, choisissez les fichiers exécutables que vous voulez ajouter à la catégorie d'applications.
4. Cliquez-droit pour ouvrir le menu contextuel des fichiers exécutable sélectionnés et sélectionnez l'option **Ajouter à la catégorie**.

   La fenêtre **Sélectionnez la catégorie d'applications** s'ouvre.
5. Dans la fenêtre **Choisissez la catégorie des applications**, procédez comme suit :

- Choisissez dans la partie supérieure de la fenêtre une des options suivantes :
  - **Créer une catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.
  - **Ajouter les règles à la catégorie indiquée**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.
- Dans le groupe **Type de la règle**, sélectionnez une des options suivantes :
  - **Ajouter aux règles d'inclusion**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.
  - **Ajouter aux règles d'exclusion**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.
- Dans le groupe **Type d'informations sur le fichier**, choisissez une des options suivantes :
  - **Données du certificat (ou SHA-256 pour les fichiers sans certificat)**.
  - **Données du certificat (les fichiers sans certificat sont ignorés)**.
  - **Uniquement SHA-256 (les fichiers sans SHA-256 sont ignorés)**.
  - **Uniquement MD5 (pour la compatibilité avec Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Cliquez sur le bouton **OK**.

Ajout à une catégorie d'applications de fichiers exécutables liés à des événements

Pour ajouter à la catégorie d'applications des fichiers exécutables associés aux événements du module Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.
3. Choisissez la sélection d'événements relatives aux fonctionnement du module Contrôle des applications (Consultation des événements à l'issue du fonctionnement du module Contrôle des applications, Consultation des événements à l'issue du fonctionnement d'essai du module Contrôle des applications) dans la liste déroulante **Événements de la sélection**.
4. Cliquez sur le bouton **Lancer la sélection**.
5. Choisissez les événements associés aux fichiers exécutables que vous souhaitez ajouter à la catégorie d'applications.
6. Cliquez-droit pour ouvrir le menu contextuel des événements sélectionnés et choisissez l'option **Ajouter à la catégorie**.

   La fenêtre **Sélectionnez la catégorie d'applications** s'ouvre.

7. Dans la fenêtre **Choisissez la catégorie des applications**, procédez comme suit :

   - Choisissez dans la partie supérieure de la fenêtre une des options suivantes :

     - **Créer une catégorie d'applications**. Sélectionnez cette option si vous souhaitez créer une catégorie d'applications et y ajouter des fichiers exécutables.

     - **Ajouter les règles à la catégorie indiquée**. Choisissez cette option si vous voulez choisir la catégorie d'applications existante et y ajouter des fichiers exécutables.

   - Dans le groupe **Type de la règle**, sélectionnez une des options suivantes :

     - **Ajouter aux règles d'inclusion**. Choisissez cette option si vous voulez créer les conditions d'ajout des fichiers exécutables à la catégorie d'applications.

     - **Ajouter aux règles d'exclusion**. Choisissez cette option si vous voulez créer les conditions d'exclusion des fichiers exécutables de la catégorie d'applications.

   - Dans le groupe **Type d'informations sur le fichier**, choisissez une des options suivantes :

     - **Données du certificat (ou SHA-256 pour les fichiers sans certificat)**.

     - **Données du certificat (les fichiers sans certificat sont ignorés)**.

     - **Uniquement SHA-256 (les fichiers sans SHA-256 sont ignorés)**.

     - **Uniquement MD5 (pour la compatibilité avec Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Cliquez sur le bouton **OK**.

Ajout et modification des règle de Contrôle des applications à l'aide de Kaspersky Security Center

Pour ajouter ou modifier une règle de Contrôle des applications à l'aide de Kaspersky Security Center, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Contrôles de sécurité**, sélectionnez **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

7. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.

- Pour modifier une règle existante, sélectionnez-la dans la liste et cliquez sur le bouton **Modifier**.

La fenêtre **Règle de Contrôle des applications** s'ouvre.

8. Exécutez une des actions suivantes :

   a. Si vous voulez créer une catégorie, procédez comme suit :

      1. Cliquez sur le bouton **Créer une catégorie**.

         L'Assistant de création de catégories personnalisée s'ouvre.

      2. Suivez les instructions de l'Assistant de création de catégories personnalisées.

      3. De la liste déroulante **Catégorie**, choisissez la catégorie d'applications créée.

   b. Si vous voulez modifier une catégorie existante, procédez comme suit :

      1. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée que vous voulez modifier.

      2. Cliquez sur le bouton **Propriétés**.

         La fenêtre **Propriétés <nom de la catégorie>** s'ouvre.

      3. Modifier les paramètres de la catégories d'applications sélectionnée.

      4. Cliquez sur le bouton **OK**.

   c. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée sur la base de laquelle vous souhaitez créer la règle.

9. Cliquez sur le bouton **Ajouter** dans le tableau **Sujets et leurs droits**.

   La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

10. Dans la fenêtre **Sélectionnez Utilisateurs ou Groupes**, composez la liste des utilisateurs et/ou des groupes d'utilisateurs que vous souhaitez autoriser à lancer les applications qui appartiennent à la catégorie sélectionnée.

11. Dans le tableau **Sujets et leurs droits**, réalisez les opérations suivantes :

    - Si vous voulez permettre aux utilisateurs et/ou aux groupes d'utilisateurs de lancer des applications qui appartiennent à la catégorie sélectionnée, cochez la case **Autoriser** sur les lignes requises.

    - Si vous voulez interdire aux utilisateurs et/ou aux groupes d'utilisateurs de lancer des applications qui appartiennent à la catégorie sélectionnée, cochez la case **Interdire** sur les lignes requises.

12. Cochez la case **Interdire aux autres utilisateurs** si vous voulez que l'application interdise le lancement des applications, appartenant à la catégorie choisie à tous les utilisateurs qui ne figurent pas dans la colonne **Sujet** et qui n'appartiennent pas aux groupes d'utilisateurs indiqués dans la colonne **Sujet**.

13. Cochez la case **Programmes de mise à jour de confiance** si vous souhaitez que les qui appartiennent à la catégories d'applications sélectionnée soient considérées comme des applications de mise à jour de confiance par Kaspersky Endpoint Security et qu'il les autorise à créer d'autres fichiers exécutables dont le lancement sera autorisé à l'avenir.

Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutables créés par les programmes de mise à jour de confiance migre également.

14. Cliquez sur le bouton **OK**.

15. Cliquez sur le bouton **Appliquer** dans le groupe **Contrôle des applications** de la fenêtre des propriétés de la stratégie.

Modification de l'état de la règle de Contrôle des applications via Kaspersky Security Center

Pour modifier l'état de la règle de Contrôle des applications, procédez comme suit :

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

2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

4. Sélectionnez la stratégie qu'il vous faut.

5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.

6. Dans la section **Contrôles de sécurité**, sélectionnez **Contrôle des applications**.

   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.

7. Dans la colonne **État**, cliquez-gauche pour ouvrir le menu contextuel et sélectionnez un des éléments suivants :

   - **Activé**. Cet état signifie que la règle est utilisée pendant le fonctionnement du module Contrôle des applications.
   - **Désactivée**. Cet état signifie que la règle n'est pas utilisée pendant le fonctionnement du module Contrôle des applications.
   - **Test**. L'état signifie que Kaspersky Endpoint Security autorise toujours le lancement des applications soumises à la règle, mais enregistre les informations relatives au lancement de ces applications dans le rapport.

     L'état **Test** permet de désigner l'action semblable à l'option **Tester les règles** pour une partie des règles quand l'option **Appliquer les règles** a été choisie dans la liste déroulante **Action**.

8. Cliquez sur le bouton **Appliquer**.

Test des règles de Contrôle des applications via Kaspersky Security Center

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles. Quand le test des règles de Contrôle des applications est activé, Kaspersky Endpoint Security ne bloque pas les applications dont le lancement est interdit par le Contrôle des applications, mais envoie des notifications de lancement au Serveur d'administration.

Pour analyser le fonctionnement des règles de Contrôle des applications, il faut étudier les événements sur la base des résultats du fonctionnement du module Contrôle des applications survenus dans Kaspersky Security Center. Si aucune des applications indispensables au travail de l'utilisateur de l'ordinateur n'affiche des événements d'interdiction de lancement en mode test, les règles créées sont correctes. Dans le cas contraire, il est conseillé de préciser les paramètres des règles que vous avez créées, de créer des règles complémentaires ou de supprimer des règles existantes.

Le mode activé par défaut est le mode d'interdiction pour les actions du Contrôle des applications.

Pour activer le test des règles de Contrôle des applications ou sélectionner une action d'interdiction du Contrôle des applications dans Kaspersky Security Center, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Dans la section **Contrôles de sécurité**, sélectionnez **Contrôle des applications**.
   Les paramètres du module Contrôle des applications s'afficheront dans la partie droite de la fenêtre.
7. Dans la liste déroulante **Mode de contrôle** choisissez une des options suivantes :
   - **Liste noire**, si vous voulez autoriser le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'interdiction ;
   - **Liste blanche**, si vous voulez interdire le lancement de toutes les applications, à l'exception des applications reprises dans les règles d'autorisation.
8. Exécutez une des actions suivantes :
   - Si vous voulez activer le mode de test pour les règles de Contrôle des applications, choisissez l'option **Tester les règles** dans la liste **Action**.
   - Si vous voulez activer le mode d'interdiction pour les règles de Contrôle des applications, choisissez l'option **Appliquer les règles** dans la liste **Action**.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Consultation des événements à l'issue du fonctionnement d'essai du module Contrôle des applications

Pour consulter les événements survenus sur Kaspersky Security Center suite au fonctionnement du composant Contrôle des applications en mode de test, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.
3. Cliquez sur le bouton **Créer une sélection**.

   La fenêtre **Propriétés <nom de la sélection>** s'ouvre.
4. Ouvrez la section **Événements**.
5. Cliquez sur le bouton **Effacer tout**.
6. Dans le tableau **Événements**, cochez les cases **Lancement de l'application interdit en mode test** et **Lancement de l'application autorisé en mode test**.
7. Cliquez sur le bouton **OK**.
8. Dans la liste déroulante **Événements de la sélection**, choisissez la sélection créée.
9. Cliquez sur le bouton **Lancer la sélection**.

Rapport sur les applications interdites en mode d'essai

Pour consulter le rapport sur les applications interdites en mode d'essai, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.

   L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. A l'étape **Sélection du type de modèle du rapport**, sélectionnez **Autre → Rapport sur les applications interdites en mode d'essai**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.
5. Lancez le processus de formation du rapport, défini aux étapes antérieures, d'une des manières suivantes :

   - Dans le menu contextuel du rapport, sélectionnez l'option **Afficher le rapport**.
   - Cliquez sur lien **Afficher le rapport** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.
   - Ouvrez le rapport d'un double-clic.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Consultation des événements à l'issue du fonctionnement du module Contrôle des applications

Pour consulter les événements survenus dans Kaspersky Security Center à l'issue du fonctionnement du composant Contrôle des applications, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.
3. Cliquez sur le bouton **Créer une sélection**.

   La fenêtre **Propriétés <nom de la sélection>** s'ouvre.
4. Ouvrez la section **Événements**.
5. Cliquez sur le bouton **Effacer tout**.
6. Dans le tableau **Événements**, cochez la case **Le lancement de l'application est interdit**.
7. Cliquez sur le bouton **OK**.
8. Dans la liste déroulante **Événements de la sélection**, choisissez la sélection créée.
9. Cliquez sur le bouton **Lancer la sélection**.

Rapport sur les applications interdites

Pour consulter le rapport sur les applications interdites, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.

   L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. A l'étape **Sélection du type de modèle du rapport**, sélectionnez **Autre → Rapport sur les applications interdites**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.
5. Lancez le processus de formation du rapport, défini aux étapes antérieures, d'une des manières suivantes :

   - Dans le menu contextuel du rapport, sélectionnez l'option **Afficher le rapport**.
   - Cliquez sur lien **Afficher le rapport** qui se trouve dans la partie droite de l'espace de travail de la Console d'administration.

- Ouvrez le rapport d'un double-clic.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Meilleures pratiques de mise en œuvre du mode de liste blanche

Cette section fournit des recommandations sur la mise en œuvre du mode de liste blanche.

Planification de l'introduction du mode de liste blanche

Dans le cadre de la planification de l'introduction du mode de liste blanche, il est recommandé d'exécuter les actions suivantes :

1. Créer les types de regroupement suivants :

   - Groupes d'utilisateurs. Les groupes d'utilisateurs pour lesquels il faut autoriser l'utilisation de différentes sélections d'applications.

   - Groupes d'administration. Un ou plusieurs groupes d'ordinateurs auxquels Kaspersky Security Center va appliquer le mode de liste blanche. Il est indispensable de créer plusieurs groupes d'ordinateurs si différents paramètres du mode de liste blanche sont appliquées à ces groupes.

2. Composer la liste des applications dont le lancement doit être autorisé.

   Avant de créer la liste, il est conseillé de réaliser les opérations suivantes :

   1. Lancer la tâche de l'inventaire.

      Les informations relatives à la création, à la modification des paramètres et au lancement de la tâche d'inventaire sont accessibles dans la section Gestion des tâches.

   2. Consulter la liste des fichiers exécutables.

Configuration du mode de liste blanche

Lors de la configuration du mode de liste blanche, il est conseillé d'exécuter les opérations suivantes :

1. Créer les catégories d'applications contenant les applications dont il faut autoriser le lancement.

   Vous pouvez choisir un des modes suivants de création d'une catégorie d'applications :

   - **Catégorie enrichie manuellement (Étape 3.Configuration des conditions d'inclusion des applications dans une catégorie, Étape 4. Configuration des conditions d'exclusion des applications hors d'une catégorie)**. Vous pouvez enrichir cette catégorie manuellement en utilisant les conditions suivantes :

     - Métadonnées du fichier. Si vous utilisez cette condition, Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables qui possèdent les métadonnées indiquées.

     - Hash du fichier. Si vous utilisez cette condition, Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables qui possèdent le hash indiqué.

L'utilisation de cette condition exclut la possibilité d'installer automatiquement les mises à jour car les fichiers de différentes versions auront un hash différent.

- Certificat du fichier. Si vous utilisez cette condition, Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables signés par le certificat indiqué.
- Catégorie KL. Si vous utilisez cette condition, Kaspersky Security Center ajoute à la catégorie des applications toutes les applications qui appartiennent à la catégorie KL indiquée.
- Dossier de l'application. Si vous utilisez cette condition, Kaspersky Security Center ajoute à la catégorie des applications tous les fichiers exécutables de ce dossier.

L'utilisation de la condition Dossier de l'application n'est pas sans risques car le lancement de n'importe quelle application depuis le dossier indiqué est autorisé. Il est conseillé d'appliquer les règles qui utilisent les catégories d'applications avec la condition « Dossier de l'application » uniquement aux utilisateurs pour lesquels il faut absolument autoriser l'installation automatique des mises à jour.

Vous pouvez ajouter aussi manuellement à la catégorie d'applications les fichiers exécutables du dossier **Fichiers exécutables**.

- **Catégorie qui contient les fichiers exécutables du dossier sélectionné**. Vous pouvez indiquer le dossier qui contient les fichiers exécutables qui vont se retrouver automatiquement dans la catégorie d'applications créée.
- **Catégorie qui contient les fichiers exécutables des appareils sélectionnés**. Vous pouvez indiquer l'ordinateur dont tous les fichiers exécutables vont se retrouver automatiquement dans la catégories d'applications créée.

Si vous utilisez ce mode de création de catégories d'applications, Kaspersky Security Center tire les informations sur les applications de l'ordinateur de la liste des fichiers exécutables.

2. Sélectionner le mode de la liste blanche pour le composant Contrôle des applications.
3. Créer les règles de Contrôle des applications à l'aide des catégories d'applications créées.

Le mode de la liste blanche prévoie au départ la règle Système d'exploitation et ses modules qui autorise le lancement des applications qui appartiennent à la catégorie KL Applications S.E. ainsi que la règle Programmes de mise à jour de confiance qui autorise le lancement des applications qui appartiennent à la catégorie KL Programmes de mise à jour de confiance. La catégorie KL Applications S.E. reprend les applications qui garantissent le fonctionnement normal du système d'exploitation. La catégorie « Programmes de mise à jour de confiance » des catégories KL reprend les programmes de mise à jour des applications des éditeurs les plus connus. Vous ne pouvez pas supprimer ces règles. Les paramètres de ces règles ne peuvent pas être modifiés. Par défaut, la règle Système d'exploitation et ses modules est activée tandis que la règle Programmes de mise à jour de confiance est désactivée. Le lancement des applications, correspondant aux conditions de déclenchement de ces règles, est autorisé pour tous les utilisateurs.

4. Définir les applications pour lesquelles il faut autoriser l'installation automatique des mises à jour.

   Vous pouvez autoriser l'installation automatique des mises à jour d'une des manières suivantes :

- Désigner la liste étendue des applications autorisées en autorisant le lancement de toutes les applications appartenant à n'importe laquelle des catégories KL.

- Désigner la liste étendue des applications autorisées en autorisant le lancement de tous le applications signées par des certificats.

  Pour autoriser le lancement de toutes les applications signées par des certificats, vous pouvez créer une catégorie avec une condition en fonction du certificat dans laquelle seul le paramètre **Sujet** avec la valeur * est utilisé.

- Pour les règles de contrôle des applications, définir le paramètre **Programmes de mise à jour de confiance**. Si cette case est cochée, Kaspersky Endpoint Security considère les applications reprises dans la règle comme des programmes de mise à jour de confiance. Kaspersky Endpoint Security autorise le démarrage d'applications qui ont été installées ou mises à jour par des applications incluses dans la règle, à condition qu'aucune règle de blocage ne soit appliquée à ces applications.

  Lors de la migration des paramètres de Kaspersky Endpoint Security, la liste des fichiers exécutables créés par les programmes de mise à jour de confiance migre également.

- Créer le dossier et y placer les fichiers exécutables des applications pour lesquelles vous voulez autoriser l'installation automatique des mises à jour. Créer ensuite la catégorie d'applications avec la condition « Dossier de l'application » et indiquer le chemin vers ce dossier. Puis créer une règle d'autorisation et sélectionner cette catégorie.

  L'utilisation de la condition « Dossier de l'application » n'est pas sans risques car le lancement de n'importe quelle application depuis le dossier indiqué est autorisé. Il est conseillé d'appliquer les règles qui utilisent les catégories d'applications avec la condition « Dossier de l'application » uniquement aux utilisateurs pour lesquels il faut absolument autoriser l'installation automatique des mises à jour.

Test du mode de liste blanche

Pour confirmer que les règles de Contrôle des applications ne bloquent pas les applications nécessaires au travail, il est conseillé d'activer le mode de test des règles de Contrôle des applications et d'analyser leur fonctionnement après la création des règles. Quand le mode test est activé, Kaspersky Endpoint Security ne bloque pas les applications dont le lancement est interdit par les règles de Contrôle des applications, mais envoie des notifications de lancement au Serveur d'administration.

Dans le cadre du test du mode de liste blanche, il est recommandé d'exécuter les actions suivantes :

1. Définir la période du test (de quelques jours à deux mois).

2. Activer le test des règles du Contrôle des applications.

3. Analyser les résultats du test en utilisant les événements survenus suite au fonctionnement en mode test du Module de l'application et les rapports sur les applications interdites en mode d'essai.

4. Sur la base des résultats de l'analyse, introduire des modifications dans les paramètres du mode de la liste blanche.

   En particulier, sur la base des résultats du test, vous pouvez ajouter à la catégorie d'applications enrichie manuellement des fichiers exécutables liés aux événements sur le fonctionnement du module Contrôle des applications.

Prise en charge du mode de liste blanche

Après avoir sélectionné l'action d'interdiction du Contrôle des applications, il est conseillé de maintenir la prise en charge du mode de liste blanche de la manière suivante :

- Analyser le fonctionnement des règles de Contrôle des applications à l'aide des événements survenus lors du fonctionnement du Contrôle des applications et des rapports sur les lancements interdits.
- Analyser les demandes d'accès aux applications envoyées par les utilisateurs.
- Analyser les fichiers exécutables inconnus en confirmant leur réputation dans Kaspersky Security Network ou sur le portail Kaspersky Whitelist.
- Avant d'installer les mises à jour pour le système d'exploitation ou pour une application, il convient d'installer ces mises à jour sur le groupe d'ordinateurs d'essai afin de voir comment les règles de Contrôle des applications vont les traiter.
- Ajouter les applications nécessaires aux catégories utilisées dans les règles de Contrôle des applications.

Endpoint Sensor

Cette section contient les informations sur Endpoint Sensor et explique comment activer ou désactiver le module.

A propos d'Endpoint Sensor

Endpoint Sensor est un module de Kaspersky Anti Targeted Attack Platform (KATA). Cette solution a été développée pour détecter en temps utiles les menaces telles que les attaques ciblées.

Le module s'installe sur les ordinateurs client. Sur ces ordinateurs, le module contrôle en permanence les processus, les connexions réseau ouvertes et les fichiers modifiés. Endpoint Sensor transmet les informations au serveur KATA.

Les fonctions du composant sont disponibles pour les systèmes d'exploitation suivants :

- Windows 7 Enterprise Service Pack 1 (32 / 64 bits) ;
- Windows 8.1.1 Enterprise (32 / 64 bits) ;
- Windows 10 RS3 / RS4 / RS5 / 19H1 (32 / 64-bit) ;
- Windows Server 2008 R2 Enterprise (64 bits) ;
- Windows Server 2012 Standard / R2 Standard (64 bits) ;
- Windows Server 2016 Standard (64 bits).

Pour en savoir plus sur le fonctionnement de KATA, *consultez l'aide de Kaspersky Anti Targeted Attack Platform*.

Sur les ordinateurs dotés du module Endpoint Sensor, il faut autoriser la connexion entrante avec le serveur KATA directement, sans passer par un serveur proxy.

Activation et désactivation du module Endpoint Sensor

Pour activer ou désactiver le module Endpoint Sensor, procédez comme suit :

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
4. Sélectionnez la stratégie qu'il vous faut.
5. Ouvrez la fenêtre des propriétés de la stratégie d'un double clic.
6. Choisissez la section **Endpoint Sensor**.
7. Exécutez une des actions suivantes :
   - Si vous voulez activer Endpoint Sensor, cochez la case **Endpoint Sensor**.
   - Si vous voulez désactiver Endpoint Sensor, décochez la case **Endpoint Sensor**.
8. Si vous aviez coché la case à l'étape précédente, procédez comme suit :
   a. Saisissez dans le champ **Adresse du serveur** l'adresse du serveur Kaspersky Anti Targeted Attack Platform qui contient les parties suivantes :
      1. le nom du protocole ;
      2. l'adresse IP ou le nom de domaine complet (FQDN) du serveur ;
      3. le chemin d'accès au collecteur d'événements Windows sur le serveur.
   b. Saisissez dans le champ **Port** le numéro du port utilisé pour la connexion au serveur Kaspersky Anti Targeted Attack Platform.
9. Cliquez sur le bouton **OK**.
10. Appliquez la stratégie.

    Pour en savoir plus sur l'application de la stratégie de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Envoi de messages des utilisateurs sur le serveur Kaspersky Security Center

L'utilisateur peut être amené à envoyer un message à l'administrateur du réseau local de l'entreprise dans les cas suivants :

- Le Contrôle des périphériques a bloqué l'accès au périphérique.

  Le modèle du message de demande d'accès au périphérique bloqué est accessible dans l'interface de Kaspersky Endpoint Security dans la section Contrôle des périphériques.

- Le Contrôle des applications a interdit le lancement de l'application.

  Le modèle du message de demande d'autorisation du lancement de l'application bloquée est accessible dans l'interface de Kaspersky Endpoint Security dans la section Contrôle des applications.

- Le Contrôle Internet a bloqué l'accès à la ressource Internet.

  Le modèle du message de demande d'accès à la ressource Internet bloquée est accessible dans l'interface de Kaspersky Endpoint Security dans la section Contrôle Internet.

Le mode d'envoi des messages, ainsi que le choix du modèle utilisé, dépend de la présence ou non sur l'ordinateur doté de l'application Kaspersky Endpoint Security d'une stratégie active de Kaspersky Security Center et d'une communication avec le Serveur d'administration de Kaspersky Security Center. Les scénarios suivants sont envisageables :

- Si aucune stratégie de Kaspersky Security Center n'est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, le message de l'utilisateur est envoyé à l'administrateur du réseau local de l'organisation par email.

  Les champs du message prennent les valeurs des champs du modèle défini dans l'interface locale de Kaspersky Endpoint Security.

- Si une stratégie Kaspersky Security Center est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, Kaspersky Endpoint Security envoie un message standard au Serveur d'administration de Kaspersky Security Center.

  Dans ce cas, les messages des utilisateurs sont consultables dans le stockage des événements de Kaspersky Security Center. Les champs du message prennent les valeurs des champs du modèle défini dans la stratégie de Kaspersky Security Center.

- Si une stratégie de Kaspersky Security Center pour les utilisateurs autonomes est active sur l'ordinateur doté de l'application Kaspersky Endpoint Security, le mode d'envoi du message dépendra de la connexion avec Kaspersky Security Center :

  - Si une connexion est établie avec Kaspersky Security Center, Kaspersky Endpoint Security envoie le message standard au Serveur d'administration de Kaspersky Security Center.

  - En l'absence de connexion avec Kaspersky Security Center, le message de l'utilisateur est envoyé à l'administrateur du réseau local de l'entreprise par email.

  Dans les deux cas, les champs du message prennent les valeurs des champs du modèle défini dans la stratégie de Kaspersky Security Center.

Consultation des messages des utilisateurs dans le référentiel des événements de Kaspersky Security Center

Les composants Contrôle des applications, Contrôle des périphériques, Contrôle Internet et Contrôle évolutif des anomalies permettent aux utilisateurs du réseau local de l'organisation dont les ordinateurs sont dotés de l'application Kaspersky Endpoint Security d'envoyer des messages à l'administrateur.

L'utilisateur peut envoyer des messages à l'administrateur de deux manières :

- Sous la forme d'un événement dans le référentiel des événements de Kaspersky Security Center.

  L'événement de l'utilisateur est envoyé dans le référentiel des événements du Kaspersky Security Center si la version de l'application Kaspersky Endpoint Security installée sur l'ordinateur de l'utilisateur fonctionne sous une stratégie active.

- Sous la forme d'un message de courrier électronique.

  Les informations de l'utilisateur sont transmises sous la forme de message électronique si l'ordinateur doté de Kaspersky Endpoint Security est couvert par une stratégie ou une stratégie pour les utilisateurs autonomes.

Pour consulter le message de l'utilisateur dans le référentiel des événements de Kaspersky Security Center, procédez comme suit :

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

2. Dans l'entrée **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Événements**.

   L'espace de travail de Kaspersky Security Center affichent tous les événements survenus pendant le fonctionnement de l'application Kaspersky Endpoint Security, y compris les messages envoyés à l'administrateur par les utilisateurs du réseau local de l'organisation.

3. Pour configurer le filtre des événements, il faut choisir l'option **Demandes des utilisateurs** dans la liste déroulante **Événements de la sélection**.

4. Choisissez le message pour l'administrateur.

5. Ouvrez la liste **Propriétés de l'événement** d'une des méthodes suivantes :

   - Cliquez avec le bouton droit sur l'événement. Dans le menu contextuel, choisissez l'option **Propriétés**.

   - Cliquez sur le bouton **Ouvrir la fenêtre des propriétés de l'événement** dans la partie droite de l'espace de travail de la Console d'administration.

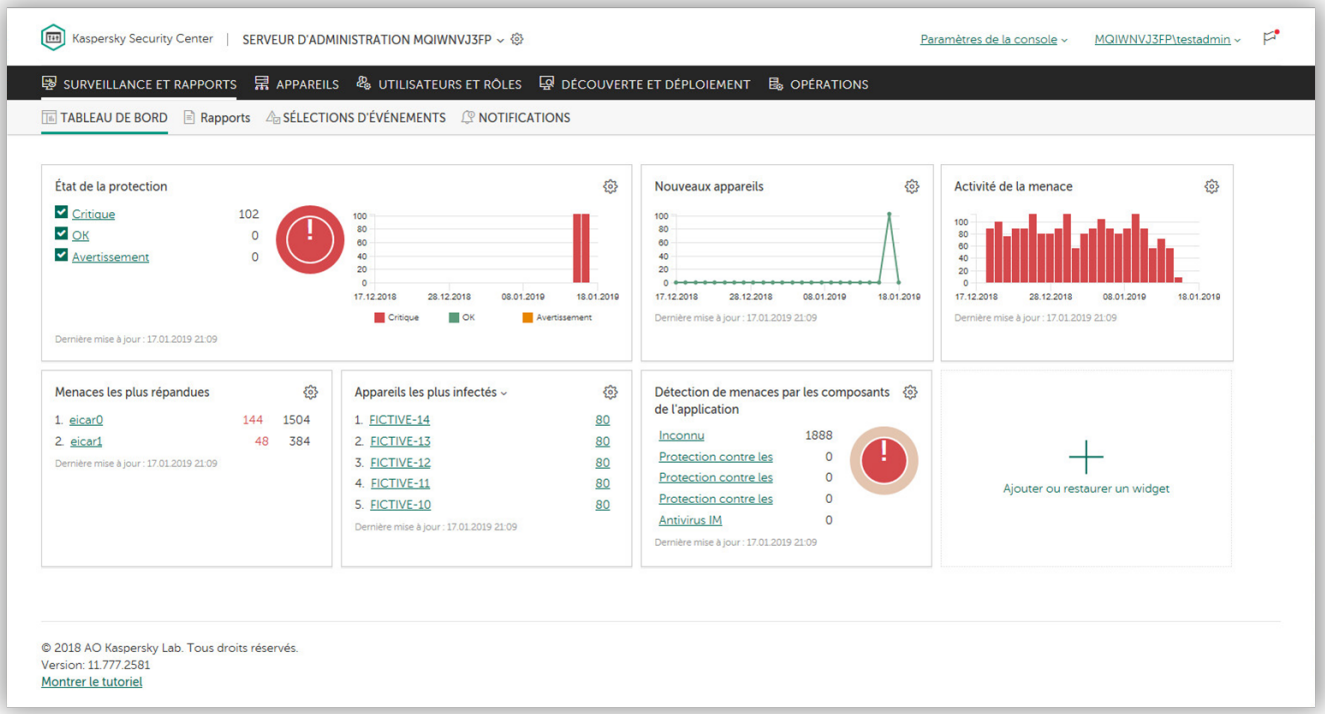
Administration de l'application via Kaspersky Security Center 11 Web Console

Kaspersky Security Center 11 Web Console (ci-après "*Web Console*") est une application (application Internet) prévue pour la réalisation centralisée des principales tâches d'administration et de maintenance des systèmes de protection du réseau de l'organisation. Web Console est un composant de Kaspersky Security Center qui propose une interface utilisateur. Pour obtenir de plus amples informations sur Kaspersky Security Center 11 Web Console, consultez l'*aide de Kaspersky Security Center*.

Web Console permet de réaliser les opérations suivantes :

- contrôler l'état du système de sécurité de votre entreprise ;
- installer des applications de Kaspersky sur les périphériques de votre réseau ;
- administrer les applications installées ;
- consulter les rapports sur l'état du système de la sécurité.

L'administration de l'application Kaspersky Endpoint Security via Web Console et la Console d'administration de Kaspersky Security Center est différente, mais la liste des actions correspond, à l'exception de la fonction de chiffrement des données.



Interface de Kaspersky Security Center 11 Web Console.

A propos du plug-in Internet d'administration de Kaspersky Endpoint Security

Le plug-in Internet d'administration de Kaspersky Endpoint Security (ci-après le *"plug-in Internet"*) assure l'interaction entre Kaspersky Endpoint Security et Kaspersky Security Center 11 Web Console. Le plug-in Internet permet d'administrer Kaspersky Endpoint Security à l'aide des outils suivants : les stratégies, les tâches, ainsi que les paramètres locaux de l'application.

La version du plug-in Internet peut différer de la version de Kaspersky Endpoint Security installée sur l'ordinateur client. Si la version installée du plug-in Internet prévoit moins de fonctions que dans la version installée de Kaspersky Endpoint Security, les paramètres des fonctions manquantes ne sont pas régis par le plug-in Internet. Ces paramètres peuvent être modifiés par l'utilisateur dans l'interface locale de Kaspersky Endpoint Security.

Le plug-in Internet n'est pas installé par défaut dans Kaspersky Security Center 11 Web Console. A la différence du plug-in d'administration pour la Console d'administration de Kaspersky Security Center qui est installé sur le poste de travail de l'administrateur, le plug-in d'administration doit être installé sur un ordinateur doté de Kaspersky Security Center 11 Web Console. Dans ce cas, les fonctions du plug-in Internet sont accessibles à tous les administrateurs qui ont accès à la Web Console dans le navigateur. Vous pouvez consulter la liste des plug-ins Internet installés dans l'interface de Web Console (**Paramètres de la console → Plug-ins**). Pour en savoir plus sur la compatibilité des versions des plug-ins Internet et de Web Console, consultez l'*aide de Kaspersky Security Center*.

Installation d'un plug-in Internet

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

- Installer le plug-in Internet à l'aide de l'assistant de configuration initiale de Kaspersky Security Center 11 Web Console.

  Web Console propose automatiquement de lancer l'Assistant de configuration initiale lors de la première connexion de Web Console au Serveur d'administration. Vous pouvez aussi lancer l'Assistant de configuration initiale dans l'interface de Web Console (**Détection de périphériques et déploiement → Déploiement et cible → Assistant de configuration initiale**). L'Assistant de configuration initiale peut également vérifier l'actualité des plug-ins Internet installés et charger les mises à jour indispensables. Pour en savoir plus sur l'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console, consultez l'*aide de Kaspersky Security Center*.

- Installer le plug-in Internet de la liste des paquets de distribution accessibles dans Web Console.

  Pour installer un plug-in Internet, il faut choisir le paquet de distribution du plug-in Internet Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console → Plug-ins**). La liste des paquets de distribution disponibles se renouvelle automatiquement après l'émission des nouvelles versions des applications de Kaspersky.

- Télécharger les paquets de distribution dans Web Console depuis une source externe.

  Pour installer le plug-in Internet, il faut ajouter l'archive ZIP du paquet de distribution de plug-in de Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console → Plug-ins**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site Internet de Kaspersky.

Mise à jour d'un plug-in Internet

Quand une nouvelle version d'un plug-in Internet apparaît, Web Console affiche la notification *Mises à jour disponibles pour les plug-ins utilisés*. Vous pouvez passer à la mise à jour de la version du plug-in Internet depuis la notification de Web Console. Vous pouvez aussi rechercher la présence éventuelle de mises à jour du plug-in Internet manuellement dans l'interface de Web Console (**Paramètres de la Console → Plug-ins**). La version précédente du plug-in Internet est automatiquement supprimée pendant la mise à jour.

Lors de la mise à jour du plug-in Internet, les composants existants sont conservés (par exemple, les stratégies ou les tâches). Les nouveaux paramètres des composants qui remplissent de nouvelles fonctions de Kaspersky Endpoint Security apparaissent dans les composants existants et affichent une valeur par défaut.

Vous pouvez mettre à jour le plug-in Internet d'une des manières suivantes :

- Mettre à jour le plug-in Internet en ligne dans la liste des plug-ins Internet.

  Pour mettre à jour un plug-in Internet, il faut choisir le paquet de distribution du plug-in Internet Kaspersky Endpoint Security dans l'interface de Web Console et lancer la mise à jour (**Paramètres de la Console → Plug-ins**). Web Console recherche la présence éventuelle de mises à jour sur les serveurs de Kaspersky et télécharge les mises à jour nécessaires.

- Mettre à jour le plug-in Internet depuis un fichier.

  Pour mettre à jour le plug-in Internet, il faut sélectionner l'archive ZIP du paquet de distribution de plug-in de Kaspersky Endpoint Security dans l'interface de Web Console (**Paramètres de la Console → Plug-ins**). Vous pouvez charger le paquet de distribution du plug-in Internet, par exemple, sur le site Internet de Kaspersky. Vous pouvez mettre à jour le plug-in Internet de Kaspersky Endpoint Security seulement jusqu'à une version plus récente. Il est impossible de mettre à jour le plug-in Internet jusqu'à une version plus ancienne.

À l'ouverture de n'importe quel composant (par exemple, une stratégie ou une tâche), le plug-in Internet analyse les informations sur la compatibilité. Si la version du plug-in Internet est égale ou supérieure à la version indiquée dans les informations sur la compatibilité, vous pouvez modifier les paramètres de ce composant. Dans le cas contraire, la modification des paramètres du composant sélectionné via le plug-in Internet est inaccessible. Il est conseillé de mettre à jour le plug-in Internet.

Déploiement de Kaspersky Endpoint Security

Kaspersky Endpoint Security peut être déployé sur des ordinateurs dans le réseau de l'organisation de plusieurs façons. Vous pouvez sélectionner la méthode de déploiement qui convient le mieux à votre organisation ou utiliser plusieurs méthodes de déploiement simultanément. Kaspersky Security Center 11 Web Console prend en charge les principaux moyens de déploiement suivants :

- Installation de l'application à l'aide de l'assistant de déploiement de la protection.

  Mode standard d'installation qui convient si vous êtes satisfaits des paramètres par défaut de Kaspersky Endpoint Security et si votre organisation possède une infrastructure simple qui ne requiert pas de configuration spéciale.

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

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

  1. création du paquet d'installation ;
  2. création de la tâche d'installation à distance.

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

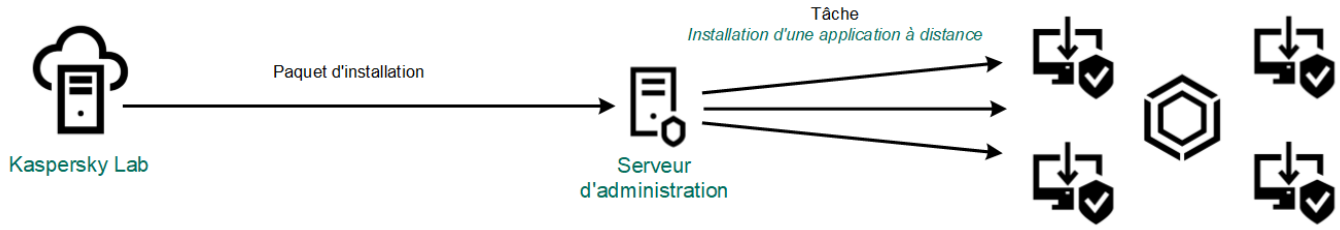
Installation standard de l'application

Pour installer l'application sur les ordinateurs de l'organisation, Kaspersky Security Center 11 Web Console prévoit un assistant de déploiement de la protection. L'assistant de déploiement de la protection comprend les principales actions suivantes :

1. La création du paquet d'installation de Kaspersky Endpoint Security.

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

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



Déploiement de Kaspersky Endpoint Security

Pour déployer Kaspersky Endpoint Security,

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

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

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

Étape 1. Sélection du paquet d'installation

A cette étape, sélectionnez le paquet de Kaspersky Endpoint Security dans la liste des paquets d'installation. Si le paquet d'installation de Kaspersky Endpoint Security ne figure pas dans la liste, vous pouvez charger et créer le paquet via le bouton **Ajouter**. Pour charger le paquet d'installation, il n'est pas nécessaire de chercher et de charger le paquet de la distribution de l'application dans la mémoire de l'ordinateur. Web Console contient la liste des paquets de la distribution situés sur les serveurs de Kaspersky et la création du paquet d'installation est automatique. Kaspersky met à jour la liste après l'émission des nouvelles versions des applications.

Vous pouvez configurer les paramètres des paquets d'installation dans Web Console. Par exemple, vous pouvez sélectionner les composants de l'application qui seront installés sur un ordinateur.

Étape 2. Activation de l'application

Cette étape permet d'ajouter la clé au paquet d'installation pour l'activation de l'application. Cette étape est facultative. Si le stockage de Kaspersky Security Center contient une clé avec la fonction de la diffusion, la clé sera ajoutée automatiquement plus tard. Vous pouvez également activer l'application plus tard à l'aide de la tâche *Ajouter la clé*.

Étape 3. Sélection de l'Agent d'administration

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

Étape 4. Sélection d'ordinateurs pour l'installation

Cette étape permet de sélectionner les ordinateurs sur lesquels l'application Kaspersky Endpoint Security va être installée. Les options suivantes existent :

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

Étape 5. Configuration des paramètres complémentaires

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

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

Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.

Étape 6. Redémarrage de l'ordinateur

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

Étape 7. Suppression des applications incompatibles

Cette étape permet de prendre connaissance de la liste des applications incompatibles et d'en autoriser la suppression. Si des applications incompatibles sont présentes sur l'ordinateur, l'installation de Kaspersky Endpoint Security se solde sur une erreur.

Étape 8. Déplacement dans un groupe d'administration

À cette étape, sélectionnez un groupe d'administration à attribuer aux ordinateurs après l'installation de l'Agent d'administration. Il est nécessaire d'attribuer un groupe d'administration aux ordinateurs pour appliquer des stratégies et des tâches de groupe. Si un ordinateur est déjà attribué à un groupe d'administration, il ne sera pas réattribué. Si vous ne choisissez pas un groupe d'administration, les ordinateurs seront ajoutés au groupe **Appareils non distribués**.

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

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

Étape 10. Lancement de l'installation

Fin de l'Assistant. La tâche d'installation à distance est lancée automatiquement. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci dans la section **Résultats**.

Création du paquet d'installation

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

Pour créer un paquet d'installation, procédez comme suit :

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

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

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

   La liste des paquets de la distribution disponibles sur les serveurs de Kaspersky s'ouvre. La liste se renouvelle automatiquement au fur et à mesure de l'édition de nouvelles versions de l'application.

3. les paramètres locaux de la distribution de l'application Kaspersky Endpoint Security.

   Les informations sur la distribution de Kaspersky Endpoint Security se ferment.

4. Cliquez sur le bouton **Télécharger et créer le paquet d'installation**.

   Le processus de création du paquet d'installation démarre.

Le paquet d'installation est créé et ajouté à la liste sur Web Console. Le paquet d'installation permet d'installer Kaspersky Endpoint Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application. Les paramètres du paquet d'installation sont repris dans le tableau ci-dessous.

Paramètres du paquet d'installation

Section	Description
Modules de protection	Cette section permet de choisir les modules de l'application qui seront disponibles. Vous pouvez modifier la sélection des modules de l'application plus tard à l'aide de la tâche *Modification de la sélection des modules de l'application*. Les composants Protection BadUSB, Endpoint Sensor et les composants de chiffrement des données ne sont pas installés par défaut. Ces composants peuvent être ajoutés dans les paramètres du paquet d'installation. Seuls les composants suivants peuvent être installés sur les ordinateurs tournant sous Windows Server : Protection contre les fichiers malicieux, Pare-feu, Prévention des intrusions, Protection BadUSB et Endpoint Sensor.
Paramètres d'installation	**Ajouter le chemin de l'application dans la variable d'environnement %PATH%**. Vous pouvez ajouter le chemin de l'installation à la variable %PATH du % pour le confort de l'utilisation de l'interface de la ligne de commande. **Ne pas protéger le processus d'installation**. Vous pouvez désactiver la protection de l'installation. La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Endpoint Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. **Garantir la compatibilité avec Citrix PVS**. Vous pouvez activer la prise en charge de Citrix Provisioning Services pour l'installation de Kaspersky Endpoint Security sur une machine virtuelle. **Chemin d'accès au dossier d'installation de l'application**. Vous pouvez modifier le chemin de l'installation de Kaspersky Endpoint Security sur l'ordinateur client. Par défaut l'application s'installe dans le dossier `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security <version>`. **Fichier de configuration**. Vous pouvez charger le fichier qui définit les paramètres de fonctionnement de Kaspersky Endpoint Security. Vous pouvez créer un fichier de configuration dans l'interface locale de l'application.

Création de la tâche d'installation à distance

Pour créer une tâche d'installation à distance, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Périphériques** → **Tâches**.
2. Le tableau des tâches s'ouvre.
3. Cliquez sur le bouton **Ajouter**.

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

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de l'application à cette étape :

1. Dans la liste **Application**, choisissez **Kaspersky Security Center**.
2. Dans la liste **Type de la tâche**, choisissez **Installation à distance de l'application**.
3. Dans le champ **Fonction de la tâche**, saisissez une brève description, par exemple `Installation de Kaspersky Endpoint Security for Windows pour les cadres`.
4. Dans le groupe **Périphériques auxquels la tâche va être affectée**, choisissez la zone d'action de la tâche.

Étape 2. Sélection d'ordinateurs pour l'installation

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

Étape 3. Configuration des paramètres du paquet d'installation

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

1. Choisissez le paquet d'installation de Kaspersky Endpoint Security.
2. Choisissez le paquet d'installation de l'Agent d'administration.

   L'Agent d'administration choisi est celui qui sera installé avec Kaspersky Endpoint Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.
3. Dans le groupe **Forcer le téléchargement du paquet d'installation**, choisissez les outils d'installation de l'application :

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

Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.

4. Dans le champ **Nombre maximum de téléchargements simultanés**, définissez la limite du nombre de requêtes adressées au Serveur d'administration pour le téléchargement du paquet d'installation. La restriction des demandes permet d'éviter la surcharge du réseau.

5. Définissez dans le champ **Nombre de tentatives d'installation** la limite de tentatives d'installation de l'application. Si l'installation Kaspersky Endpoint Security se solde sur une erreur, la tâche lance à nouveau l'installation automatiquement.

6. Le cas échéant, décochez la case **Ne pas installer l'application si elle est déjà installée**. Cela permet, par exemple, d'installer une application d'une version antérieure.

7. Le cas échéant, décochez la case **Vérifier préalablement la version du système d'exploitation**. Cela permet d'éviter le téléchargement du paquet de distribution de l'application si le système d'exploitation de l'ordinateur ne répond pas à la configuration logicielle requise. Si vous êtes certain que le système d'exploitation est conforme à la configuration logicielle requise, vous pouvez ignorer cette vérification.

8. Le cas échéant, cochez la case **Cible de l'installation du paquet d'installation dans les stratégies de groupe Active Directory**. L'installation de Kaspersky Endpoint Security s'opère à l'aide des outils de l'Agent d'administration ou des outils d'Active Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.

9. Le cas échéant, cochez la case **Proposer à l'utilisateur de quitter les applications en cours d'exécution**. L'installation de Kaspersky Endpoint Security requiert des ressources de l'ordinateur. Pour le confort de l'utilisateur, l'assistant d'installation de l'application propose de quitter les applications en cours d'exécution avant de lancer l'installation. Cela permettra d'éviter le ralentissement des autres applications et les échecs possibles de l'ordinateur.

10. Dans le groupe **Comportement des appareil administrés par ce Serveur**, sélectionnez le mode d'installation de Kaspersky Endpoint Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.

Étape 4. Sélection du compte utilisateur pour accéder à l'ordinateur

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Pour installer Kaspersky Endpoint Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 5. Fin de la création de la tâche

Terminez l'assistant en cliquant sur le bouton **Générer**. La nouvelle tâche apparaît dans la liste des tâches. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Modification de la composition de l'application

Pendant la création du paquet d'installation, vous pouvez choisir les modules de Kaspersky Endpoint Security qui seront accessibles. Pour modifier la sélection des modules de Kaspersky Endpoint Security après l'installation de l'application, utilisez la tâche *Modification de la sélection des modules de l'application*. Les modules Protection BadUSB, Endpoint Sensor et les modules de chiffrement des données peuvent être ajoutés uniquement dans les paramètres du paquet d'installation.

Seuls les composants suivants peuvent être installés sur les ordinateurs tournant sous Windows Server : Protection contre les fichiers malicieux, Pare-feu, Prévention des intrusions, Protection BadUSB et Endpoint Sensor.

Pour modifier la sélection de modules d'une application, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows**.

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

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

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

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche, puis cliquez sur **Suivant**.

5. Terminez l'assistant en cliquant sur le bouton **Générer**.

   La nouvelle tâche apparaît dans la liste des tâches.

6. Cliquez sur la tâche **Modification de la sélection des modules de l'application**.

   La fenêtre des propriétés de la tâche s'ouvre.

7. Choisissez l'onglet **Paramètres de l'application**.

8. Choisissez les modules de l'application qui seront accessibles.

9. Le cas échéant, activez la protection par mot de passe pour l'exécution de la tâche :

   a. Cochez la case **Configurer le mot de passe pour modifier la sélection de modules**.

   b. Saisissez l'identifiant de l'utilisateur doté de l'autorisation *Suppression/ modification / restauration de l'application*.

10. Cliquez sur le bouton **Enregistrer**.

11. Cochez la case en regard de la tâche.

12. Cliquez sur le bouton **Démarrer**.

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

Guide de démarrage

Après le déploiement de l'application sur les ordinateurs client, il est nécessaire de réaliser les opérations suivantes pour pouvoir utiliser Kaspersky Endpoint Security depuis Kaspersky Security Center 11 Web Console :

- Créer et configurer une stratégie.

  Les stratégies permettent de définir des valeurs identiques pour les paramètres de fonctionnement de Kaspersky Endpoint Security sur tous les postes clients appartenant au groupe d'administration. L'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console crée automatiquement une stratégie pour Kaspersky Endpoint Security.

- Créer les tâches *Mise à jour* et *Recherche de virus*.

  La tâche *Mise à jour* est nécessaire pour maintenir l'actualité de la protection de l'ordinateur. Lors de l'exécution de la tâche, Kaspersky Endpoint Security met à jour les bases antivirus et les modules de l'application. L'assistant de configuration initiale de Kaspersky Security Center 11 Web Console crée automatiquement la tâche de *mise à jour* pour Kaspersky Endpoint Security.

  La tâche *Recherche de virus* est requise afin de détecter en temps utiles les virus et autres programmes dangereux. La tâche *Recherche de virus* doit être créée manuellement.

Pour exécuter la tâche Recherche de virus, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows**.

   b. Dans la liste **Type de tâche**, choisissez **Recherche de virus**.

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

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

4. Sélectionnez les périphériques conformément à l'option choisie de la zone d'action de la tâche.

5. Cliquez sur le bouton **Suivant**.

6. Terminez l'assistant en cliquant sur le bouton **Générer**.

   La nouvelle tâche apparaît dans le tableau des tâches.

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

   Il est conseillé de planifier l'exécution d'une tâche au moins une fois par semaine.

8. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

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

La recherche de virus est alors exécutée sur les ordinateurs de l'utilisateur conformément à la planification définie.

Activation de Kaspersky Endpoint Security

L'*activation* est une procédure qui consiste à insérer un code dans le logiciel Kaspersky afin d'en activer sa licence. Cette licence donne le droit d'utiliser la version commerciale de l'application pendant la durée de validité de la licence. La procédure d'activation de l'application est incluse avec l'ajout de la clé.

Vous pouvez activer l'application à distance via l'interface de Kaspersky Security Center 11 Web Console des façons suivantes :

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

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

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

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

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

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

Pour activer l'application avec l'aide de la tâche Ajouter une clé, il faut réaliser les opérations suivantes :

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

   Le tableau des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows**.

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

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

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

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche, puis cliquez sur **Suivant**.

5. Sélectionnez la licence que vous souhaitez utiliser pour activer l'application et cliquez sur **Suivant**.

   Vous pouvez ajouter des licences au stockage de clés (**Opérations → Licences**).

6. Lisez attentivement les informations de licence et cliquez sur **Suivant**.

7. Terminez l'assistant en cliquant sur le bouton **Générer**.

   La nouvelle tâche apparaît dans la liste des tâches.

8. Cochez la case en regard de la tâche.

9. Cliquez sur le bouton **Démarrer**.

   Cette action entraîne l'activation de l'application Kaspersky Endpoint Security sur les ordinateurs des utilisateurs.

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

Pour activer l'application via la diffusion sur les ordinateurs d'une clé du stockage de clés du Serveur d'administration de Kaspersky Security Center, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Opérations → Licence**.

2. Ouvrez les propriétés de la clé d'un clic sur le nom du produit auquel la clé se rapporte.

3. Basculez le commutateur **Distribuer la clé automatiquement**.

4. Cliquez sur le bouton **Enregistrer**.

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

Lancement et arrêt de Kaspersky Endpoint Security

Une fois installé sur l'ordinateur de l'utilisateur, Kaspersky Endpoint Security se lance automatiquement. Par la suite, le lancement de Kaspersky Endpoint Security a lieu par défaut directement après celui du système d'exploitation. Vous pouvez contrôler l'état du fonctionnement de l'application à l'aide du widget Internet **État de la protection** dans la section **Surveillance et rapports**.

Pour configurer le lancement de Kaspersky Endpoint Security, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez **Périphériques → Stratégies et profils de stratégie**.

2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez configurer le lancement de l'application.

   La fenêtre des propriétés de la stratégie s'ouvre.

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

4. Choisissez la section **Paramètres généraux**.

5. Cliquez sur le bouton **Paramètres de l'application**.

6. La case **Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur** permet de configurer le lancement de l'application.

7. Cliquez sur le bouton **OK**.

8. Confirmez la modification via le bouton **Enregistrer**.

Pour lancer ou arrêter Kaspersky Endpoint Security à distance, procédez comme suit :

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

2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez lancer ou arrêter Kaspersky Endpoint Security.

   La fenêtre des propriétés de l'ordinateur s'ouvre.

3. Choisissez l'onglet **Applications**.

4. Cochez la case en regard de l'application **Kaspersky Endpoint Security for Windows**.

5. Cliquez sur le bouton **Démarrer** ou **Arrêter**.

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

La mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

Les éléments suivants sont mis à jour sur les ordinateurs des utilisateurs :

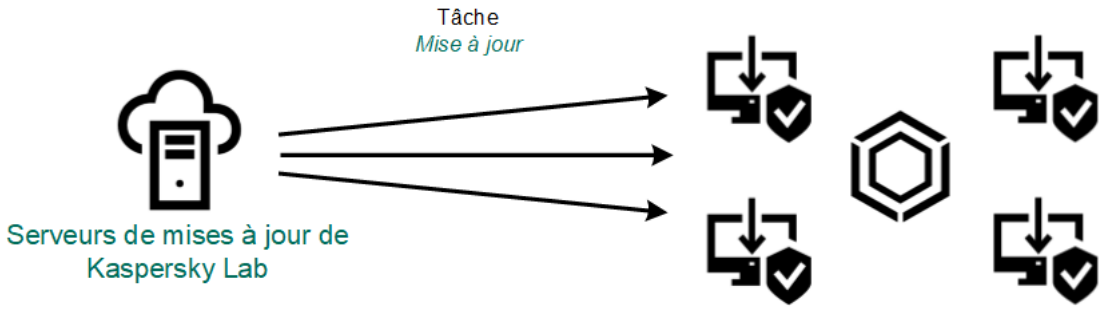
- Bases antivirus. Les bases antivirus contiennent les bases des signatures des programmes malveillants, la description des attaques réseau, les bases des adresses Internet malveillantes et de phishing, les bases des bannières, les bases antispam et d'autres données.

- Modules de l'application. La mise à jour des modules permet d'éliminer les vulnérabilités de l'application et d'améliorer les méthodes de protection de l'ordinateur. Les mises à jour des modules peuvent modifier le comportement des modules de l'application et ajouter de nouvelles fonctions.

Kaspersky Endpoint Security prend en charge les schémas de mise à jour des bases et des modules de l'application suivants :

- Mise à jour depuis les serveurs de Kaspersky

Les serveurs de mises à jour de Kaspersky sont répartis à travers le monde. Ceci garantit la haute fiabilité des mises à jour. Si la mise à jour ne peut pas être exécutée depuis un serveur, Kaspersky Endpoint Security passe au serveur suivant.



Mise à jour depuis les serveurs de Kaspersky

- Mise à jour centralisée.

  La mise à jour centralisée permet de réduire le trafic Internet externe et garantit la commodité du contrôle des mises à jour.

  La mise à jour centralisée se déroule selon les étapes suivantes :

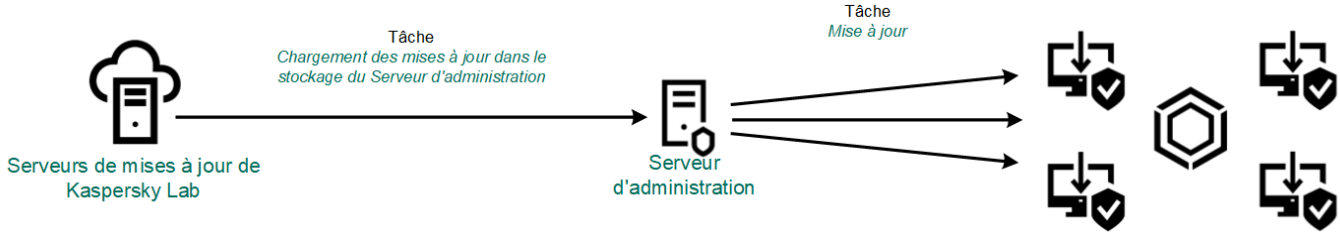
  1. Chargement du paquet de mise à jour dans le stockage au sein du réseau de l'organisation.

     Le chargement du paquet de mise à jour dans le stockage peut s'opérer d'une des manières suivantes :

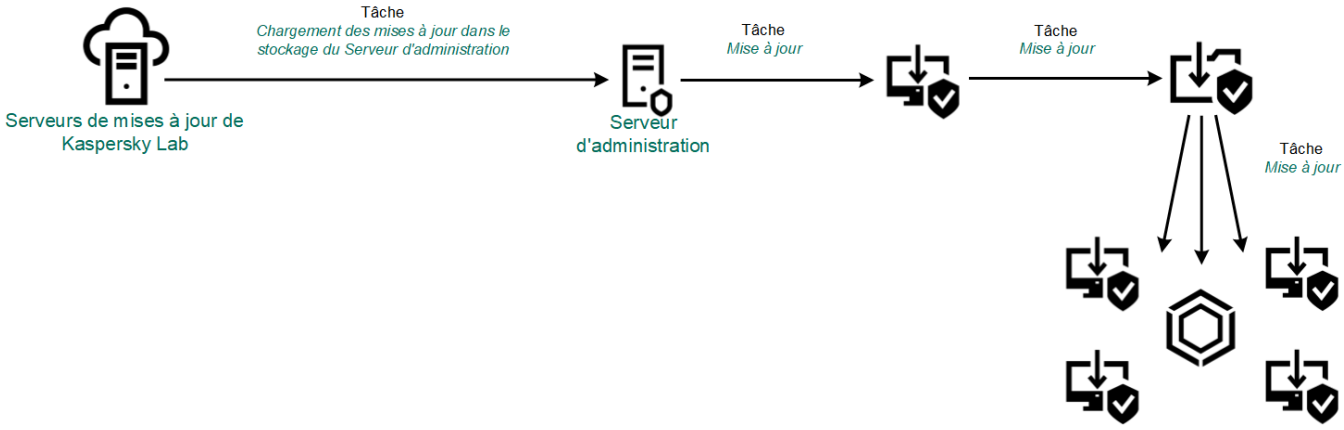
     - Utilisation de la tâche *Télécharger les mises à jour du référentiel* du serveur d'administration.
     - A l'aide de la tâche de Kaspersky Endpoint Security *Mise à jour*. La tâche est prévue pour un des ordinateurs du réseau local de l'organisation. La tâche permet de copier le paquet de mise à jour dans le dossier partagé.
     - A l'aide de Kaspersky Update Utility. Les informations détaillées sur l'utilisation de Kaspersky Update Utility sont reprises *dans la* Base des connaissances de Kaspersky.

  2. Diffusion du paquet de mise à jour sur les ordinateurs client depuis le stockage.

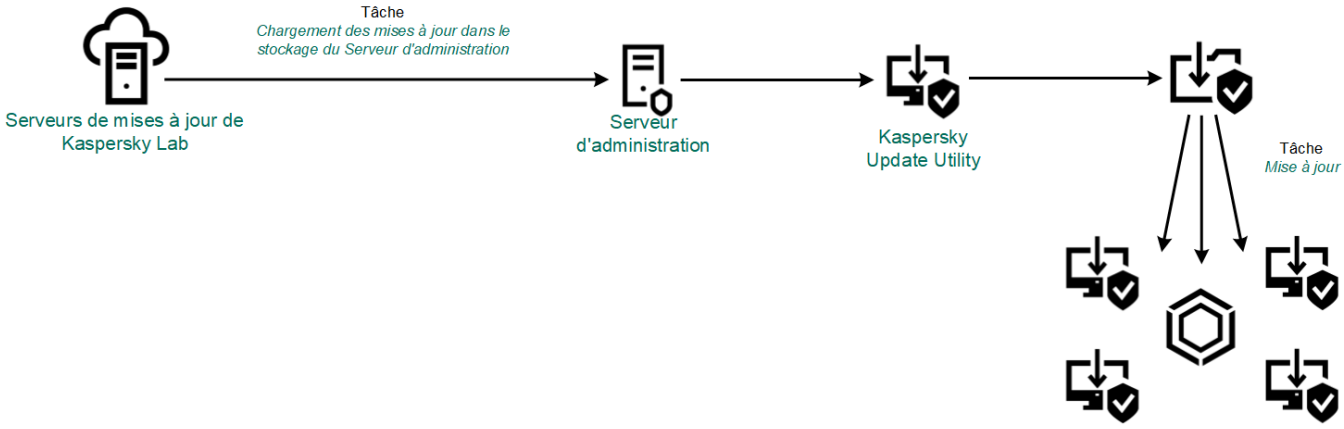
     La diffusion du paquet de mise à jour sur les ordinateurs client est garantie par la tâche *Mise à jour* de Kaspersky Endpoint Security. Vous pouvez créer un nombre illimité de tâches de mise à jour pour chacun des groupes d'administration.



Mise à jour depuis un stockage du serveur



Mise à jour depuis un dossier partagé



Mise à jour à l'aide de Kaspersky Update Utility

La liste des sources des mises à jour contient par défaut le Serveur d'administration de Kaspersky Security Center et les serveurs de mises à jour de Kaspersky. Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés. Si la mise à jour ne peut pas être exécutée depuis une source de mise à jour, Kaspersky Endpoint Security passe automatiquement à la suivante

Le chargement des mises à jour depuis les serveurs de mise à jour de Kaspersky ou d'autres serveurs FTP ou HTTP s'opère selon des protocoles réseau standard. Si l'accès à la source des mises à jour requiert une connexion à un serveur proxy, introduisez les paramètres du serveur proxy dans les propriétés de la stratégie de Kaspersky Endpoint Security.

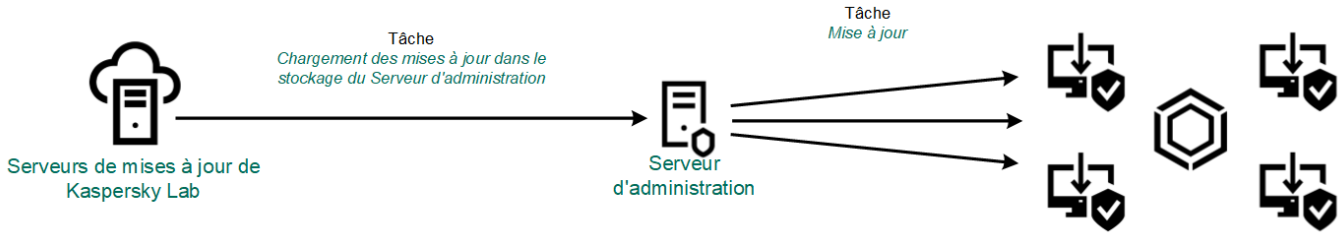
Mise à jour depuis un stockage du serveur

Pour économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local de l'organisation depuis le stockage de serveur. Pour ce faire, Kaspersky Security Center doit charger le paquet de misse à jour dans le stockage (serveur FTP ou HTTP, dossier réseau ou local) des serveurs de mise à jour de Kaspersky. Ainsi, les autres ordinateurs du réseau local de l'organisation pourront recevoir le paquet de mise à jour depuis le stockage de serveur.

La configuration de la mise à jour des bases et des modules de l'application du stockage de serveur comprend les étapes suivantes :

1. Configuration du déplacement du paquet de mise à jour dans le stockage sur le Serveur d'administration (tâche *Chargement des mises à jour dans le stockage du Serveur d'administration*).

2. Configuration de la mise à jour des bases et des modules de l'application depuis le stockage de serveur indiqué sur les autres ordinateurs du réseau local de l'organisation (tâche *Mise à jour*).



Mise à jour depuis un stockage du serveur

Pour configurer le chargement du paquet de mises à jour dans le stockage du serveur, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

2. Cliquez sur la tâche du Serveur d'administration **Chargement des mises à jour dans le stockage du Serveur d'administration**.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Chargement des mises à jour dans le stockage du Serveur d'administration* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console et n'existe qu'en un seul exemplaire.

3. Passez à la section **Paramètres de l'application**.

4. Dans le groupe **Paramètres divers**, cliquez sur le bouton **Configurer**.

5. Saisissez dans le champ **Dossier d'enregistrement des mises à jour**, saisissez l'adresse du serveur FTP ou HTTP ou du dossier réseau ou local dans lequel Kaspersky Security Center copie le paquet de mise à jour récupéré sur les serveurs de mise à jour de Kaspersky.

   Le chemin d'accès à la source des mises à jour est le suivant :

   - S'il s'agit d'un serveur FTP ou HTTP, saisissez l'adresse Internet ou l'adresse IP du site.

     Par exemple, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

     S'il s'agit d'un serveur FTP, vous pouvez indiquer les paramètres d'authentification au format `ftp://<nom d'utilisateur>:<mot de passe>@<hôte>:<port>`.

   - S'il s'agit d'un dossier réseau ou d'un dossier local, saisissez le chemin d'accès complet à ce dossier.

     Par exemple : `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Cliquez sur le bouton **OK**.

7. Confirmez la modification via le bouton **Enregistrer**.

Pour configurer la mise à jour de Kaspersky Endpoint Security depuis le dossier indiqué, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console.

3. Passez à la section **Paramètres de l'application**.
4. Passez à l'onglet **Mode local**.
5. Dans la liste des sources de mises à jour, cliquez sur le bouton **Ajouter**.
6. Dans le champ **Source**, saisissez l'adresse du serveur FTP ou HTTP ou du dossier réseau ou local dans lequel Kaspersky Security Center copie le paquet de mise à jour récupéré sur les serveurs de mise à jour de Kaspersky.

   L'adresse de la source doit correspondre à l'adresse indiquée antérieurement dans le champ **Dossier de stockage des mises à jour** lors de la configuration du téléchargement des mises à jour sur le stockage serveur (cf. l'étape *5 des instructions ci-dessus*).

7. Dans le groupe **Etat**, sélectionnez l'option **Activé(e)**.
8. Cliquez sur le bouton **OK**.
9. Configurez les priorités des source des mises à jour à l'aide des boutons **Monter** et **Descendre**.
10. Cliquez sur le bouton **Enregistrer**.

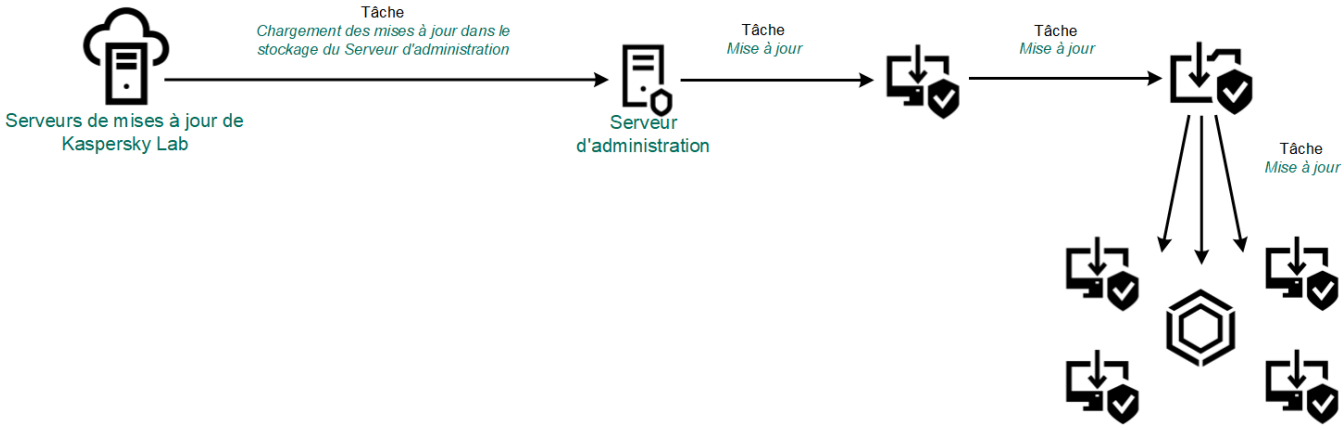
Si la mise à jour ne peut pas être exécutée depuis le premier serveur de mise à jour, Kaspersky Endpoint Security passe automatiquement au serveur suivant.

Mise à jour depuis un dossier partagé

Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour des bases et des modules de l'application sur les ordinateurs du réseau local d'entreprise depuis un dossier partagé. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère les paquets de mise à jour depuis le Serveur d'administration de Kaspersky Security Center ou les serveurs de mises à jour de Kaspersky et copie le paquet de mise à jour dans le dossier partagé. Ainsi, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

La configuration de la mise à jour des bases et des modules de l'application depuis un dossier partagé comprend les étapes suivantes :

1. Activation du mode de copie du paquet des mises à jour vers un dossier partagé sur un des ordinateurs du réseau local d'entreprise.
2. Configuration de la mise à jour des bases et des modules de l'application puis le dossier partagé indiqué sur les autres ordinateurs du réseau local d'entreprise.



Mise à jour depuis un dossier partagé

Pour activer le mode de copie du paquet des mises à jour vers un dossier partagé, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console.

3. Passez à la section **Paramètres de l'application**.

4. Sélectionnez l'onglet **Mode local**.

5. Configurez les sources des mises à jour.

   En guise de sources des mises à jour, vous pouvez utiliser les serveurs de mise à jour de Kaspersky, le Serveur d'administration de Kaspersky Security Center ou d'autres serveurs FTP ou HTTP, ainsi que des dossiers locaux ou réseau.

6. Cochez la case **Copier les mises à jour dans le dossier**.

7. Indiquez dans le champ **Emplacement** le chemin d'accès au dossier partagé.

   Si le champ n'est pas rempli, Kaspersky Endpoint Security copie le paquet de mise à jour dans le dossier `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

8. Cliquez sur le bouton **Enregistrer**.

La tâche *Mise à jour* doit être affectée à un ordinateur qui sera considéré comme la source des mises à jour.

Pour configurer la mise à jour depuis un dossier partagé, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows**.

   b. Dans la liste **Type de tâche**, choisissez **Mise à jour**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, `Mise à jour depuis un dossier partagé`.

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

   La tâche *Mise à jour* doit être attribuée aux ordinateurs restant du réseau local de l'organisation, à l'exception de l'ordinateur considéré comme source de mises à jour.

4. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche, puis cliquez sur **Suivant**.

5. Terminez l'assistant en cliquant sur le bouton **Générer**.

   La nouvelle tâche apparaît dans le tableau des tâches.

6. Cliquez sur la tâche *Mise à jour* créée.

   La fenêtre des propriétés de la tâche s'ouvre.

7. Passez à la section **Paramètres de l'application**.

8. Sélectionnez l'onglet **Mode local**.

9. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Ajouter**.

10. Indiquez dans le champ **Source** le chemin d'accès au dossier partagé.

    L'adresse de la source doit correspondre à l'adresse renseignée au préalable dans le champ **Emplacement** lors de la configuration du mode de copie du paquet de mise à jour dans le dossier partagé (cf. l'*étape 7 des instructions ci-dessus*).

11. Cliquez sur le bouton **OK**.

12. Configurez les priorités des source des mises à jour à l'aide des boutons **Monter** et **Descendre**.

13. Cliquez sur le bouton **Enregistrer**.

Mise à jour en mode mobile

Le *mode mobile* est un mode de fonctionnement de Kaspersky Endpoint Security qui s'applique aux situations où l'ordinateur quitte le périmètre du réseau de l'organisation (*ordinateur déconnecté*). Pour en savoir plus sur les ordinateurs déconnectés et les utilisateurs itinérants, consultez l'*aide de Kaspersky Security Center*.

L'ordinateur déconnecté qui a quitté le réseau de l'organisation ne peut pas se connecter au Serveur d'administration pour la mise à jour des bases et des modules de l'application. Par défaut, la mise à jour des bases et des modules de l'application en mode mobile s'opère uniquement depuis les Serveurs de mise à jour de Kaspersky désignés comme source des mises à jour. L'utilisation du serveur proxy pour la connexion à Internet est définie par la stratégie spéciale pour les utilisateurs autonomes. La stratégies pour les utilisateurs autonomes est créée séparément. Après le passage de Kaspersky Endpoint Security au mode mobile, les tâches de mise à jour sont lancées une fois toutes les deux heures.

Pour configurer les paramètres de mise à jour en mode mobile, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

2. Cliquez sur la tâche **Mise à jour** de Kaspersky Endpoint Security.

   La fenêtre des propriétés de la tâche s'ouvre.

   La tâche *Mise à jour* est créée automatiquement par l'Assistant de configuration initiale de Kaspersky Security Center 11 Web Console.

   Passez à la section **Paramètres de l'application**.

3. Passez à l'onglet **Mode mobile**.

4. Configurez les sources des mises à jour. En guise de sources des mises à jour, vous pouvez utiliser les serveurs de mise à jour de Kaspersky ou d'autres serveurs FTP ou HTTP, ainsi que des dossiers locaux ou réseau.

5. Cliquez sur le bouton **Enregistrer**.

Ainsi, les bases et les modules de l'application sont mis à jour sur les ordinateurs des utilisateurs lors du passage au mode mobile.

Utilisation du serveur proxy lors de la mise à jour

Afin de pouvoir télécharger les mises à jour des bases et des modules de l'application depuis une source des mises à jour, il faudra peut-être définir les paramètres du serveur proxy. S'il existe plusieurs sources des mises à jour, les paramètres du serveur proxy sont appliqués à toutes les sources. Si le serveur proxy n'est pas requis pour certaines sources des mises à jour, vous pouvez désactiver l'utilisation du serveur proxy dans les propriétés de la stratégie. Kaspersky Endpoint Security utilisera également le serveur proxy pour accéder au Kaspersky Security Network et aux serveurs d'activation.

Pour configurer la connexion aux sources des mises à jour via un serveur proxy, procédez comme suit :

1. Dans la fenêtre principale de Web Console, cliquez sur .

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Passez à la section **Paramètres d'accès au réseau Internet**.

3. Cochez la case **Utiliser un serveur proxy**.

4. Configurez les paramètres de connexion au serveur proxy : l'adresse du serveur proxy, le port et les paramètres d'authentification (le nom d'utilisateur et le mot de passe).

5. Cliquez sur le bouton **Enregistrer**.

Pour désactiver l'utilisation du serveur proxy pour un groupe d'administration défini, procédez comme suit :

1. Dans la fenêtre principale de Web Console, choisissez l'onglet **Périphériques → Stratégies et profils de stratégie**.
2. Cliquez sur le nom de la stratégie de Kaspersky Endpoint Security pour les ordinateurs sur lesquels vous souhaitez désactiver l'utilisation du serveur proxy.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Ouvrez l'onglet **Paramètres des applications**.
4. Passez à la section **Paramètres généraux → Paramètres du réseau**.
5. Dans la fenêtre **Paramètres du serveur proxy**, sélectionnez l'option **Ne pas utiliser un serveur proxy**.
6. Cliquez sur le bouton **OK**.
7. Confirmez la modification via le bouton **Enregistrer**.

Gestion de la tâche

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center 11 Web Console, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration ;
- des tâches pour la sélection d'ordinateurs.

Vous pouvez créer n'importe quelle quantité de tâches de groupe, de tâches pour une sélection d'ordinateurs et de tâches locales. Pour en savoir plus sur l'utilisation des groupes d'administration, des sélections d'ordinateurs et des plages d'ordinateurs, consultez l' *aide de Kaspersky Security Center*.

Kaspersky Endpoint Security prend en charge l'exécution des tâches suivantes :

- **Recherche de virus**. Kaspersky Endpoint Security recherche la présence éventuelle de virus et d'autres programmes dangereux dans les secteurs de l'ordinateur définis via les paramètres de la tâche. La tâche *Recherche de virus* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale. Il est conseillé de planifier l'exécution d'une tâche au moins une fois par semaine.
- **Ajouter une clé**. Kaspersky Endpoint Security ajoute la clé pour l'activation des applications, y compris une clé complémentaire. Avant d'exécuter une tâche, confirmez que le nombre d'ordinateurs auxquels la tâche sur lesquels la tâche va être exécutée ne dépasse pas le nombre d'ordinateurs couverts par la licence.
- **Modification de la sélection des modules de l'application**. Kaspersky Endpoint Security installe ou supprime les modules sur les ordinateurs client selon la liste des modules indiquée dans les paramètres de la tâche. Il est impossible de supprimer le module Protection contre les fichiers malicieux. La composition optimale de modules de Kaspersky Endpoint Security permet d'économiser les ressources de l'ordinateur.
- **Inventaire**. Kaspersky Endpoint Security récupère des informations sur tous les fichiers exécutables des applications de l'ordinateur. La tâche *Inventaire* est à charge du module Contrôle des applications. Si le module Contrôle des applications n'est pas installé, la tâche se solde sur un échec.

- **Mise à jour**. Kaspersky Endpoint Security met à jour les bases et les modules de l'application. La tâche *Mise à jour* est obligatoire pour le fonctionnement de Kaspersky Endpoint Security et est créée dans l'Assistant de configuration initiale. Il est recommandé de planifier l'exécution d'une tâche au moins une fois par jour.

- **Restauration de la dernière mise à jour**. Kaspersky Endpoint Security revient à la dernière mise à jour des bases de données et des modules de l'application. Cela peut être nécessaire, par exemple, si les nouvelles bases contiennent des données incorrectes qui pourraient amener Kaspersky Endpoint Security à bloquer une application inoffensive.

- **Vérification de l'intégrité**. Kaspersky Endpoint Security analyse la composition des modules de l'application, vérifie si les modules ont été endommagés ou modifiés et vérifie la signature numérique de chacun d'entre eux.

Les tâches sont lancées sur l'ordinateur uniquement si l'application Kaspersky Endpoint Security est lancée.

Pour créer une tâche, procédez comme suit :

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

   Le tableau des tâches s'ouvre.

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

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, choisissez l'option **Kaspersky Endpoint Security for Windows**.

   b. Dans la liste déroulante **Type de tâche**, choisissez la tâche que vous voulez lancer sur les ordinateurs des utilisateurs.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, `Mise à jour de l'application de comptabilité`.

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

4. Sélectionnez les périphériques conformément à l'option choisie de la zone d'action de la tâche.

5. Cliquez sur le bouton **Suivant**.

6. Terminez l'assistant en cliquant sur le bouton **Générer**.

   La nouvelle tâche apparaît dans le tableau des tâches.

Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. La tâche pour Kaspersky Endpoint Security est créée et lancée selon les paramètres par défaut. Vous pouvez modifier les paramètres de la tâche dans ses propriétés.

La liste des tâches permet de contrôler le résultat de l'exécution de la tâche (colonnes **Etat**, **En cours**, **Terminée**, **Soldé sur une erreur**, **Terminée. Redémarrage requis**). Vous pouvez aussi créer une sélection d'événements pour le contrôle de l'exécution des tâches (**Surveillance et rapports** → **Sélections d'événements**). Pour en savoir plus sur la sélection d'événements, *consultez l'aide de Kaspersky Security Center*. Les résultats de l'exécution des tâches sont enregistrés localement sur l'ordinateur dans le journal des événements Windows et dans les rapports de Kaspersky Endpoint Security.

Administration des stratégies

La *stratégie* est un ensemble de paramètres du fonctionnement de l'application, défini pour un groupe d'administration. Il est possible de configurer plusieurs stratégies avec des valeurs différentes pour une application. Les paramètres de fonctionnement de l'application peuvent varier en fonction des groupes d'administration. Une stratégie propre à l'application peut être créée dans chaque groupe d'administration.

Les paramètres de la stratégie sont transmis aux ordinateurs client à l'aide de l'Agent d'administration lors de la *synchronisation*. Par défaut, le Serveur d'administration exécute la synchronisation directement après une modification des paramètres de la stratégie. La synchronisation s'opère via le port UDP 15000 sur l'ordinateur client. Le Serveur d'administration réalise une synchronisation toutes les 15 minutes. En cas d'échec de la synchronisation après la modification des paramètres d'une stratégie, la prochaine tentative de synchronisation est réalisée selon la planification définie.

Stratégie active et inactive

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

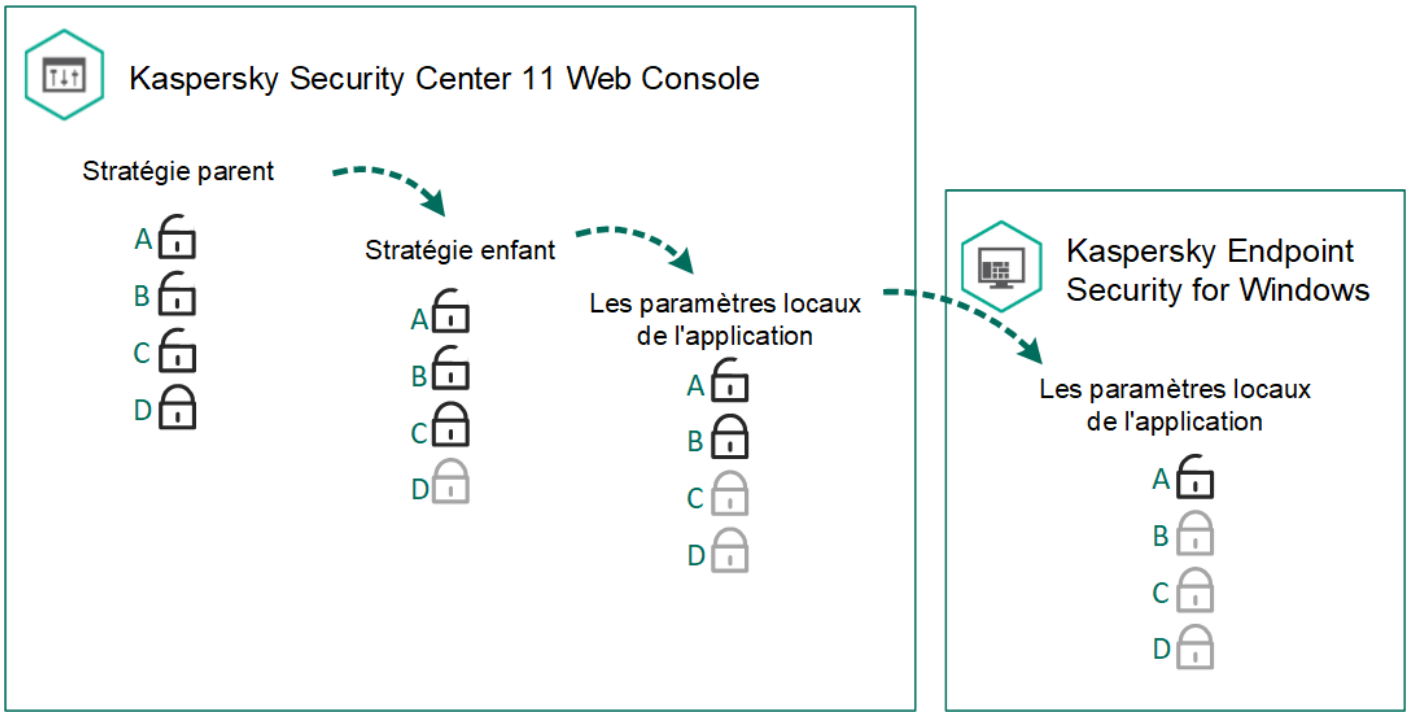
Vous pouvez créer une quantité non limitée de stratégies inactives. Une stratégie inactive n'a aucun impact sur les paramètres de l'application sur les ordinateurs du réseau. Les stratégies inactives sont prévues pour faire face à des situations extraordinaires, comme une attaque de virus. Ainsi, en cas d'attaque via des disques flash, vous pouvez activer une stratégie qui bloque l'accès aux disques flash. Dans ce cas, la stratégie active devient automatiquement inactive.

Stratégie pour les utilisateurs autonomes

La stratégie pour les utilisateurs autonomes est activée quand l'ordinateur quitte le périmètre du réseau de l'organisation.

Hiérarchie des stratégies

Chaque paramètre présenté dans une stratégie possède l'attribut qui indique si la modification de ce paramètre dans les stratégies enfant et dans les paramètres locaux de l'application est autorisée. La *stratégie enfant* est une stratégie de niveau inférieur, à savoir une stratégie pour les sous-groupes d'administration et les Serveur d'administration secondaires. L'attribut fonctionne uniquement seulement si l'héritage des paramètres de la stratégie parent est activé dans la stratégie enfant. Les stratégies pour les utilisateurs absents du bureau n'affectent pas les autres stratégies via la hiérarchie des groupes d'administration.



Hiérarchie des stratégies

Création d'une stratégie

Pour créer une stratégie, procédez comme suit:

1. Dans la fenêtre principale de Web Console, choisissez **Périphériques** → **Stratégies et profils de stratégie**.
2. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de la stratégie démarre.
3. Choisissez l'application Kaspersky Endpoint Security, puis cliquez sur **Suivant**.
4. Lisez la Déclaration de Kaspersky Security Network (KSN) et acceptez-la, puis cliquez sur **Suivant**.
5. Sous l'onglet **Général**, exécutez les actions suivantes :
   - modifier le nom de la stratégie ;
   - Sélectionner l'état d'une stratégie :
     - **Active**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.
     - **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.
     - **Pour les utilisateurs autonomes**. La stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.
   - configurer l'héritage des paramètres :
     - **Hériter des paramètres de la stratégie parent**. Si le commutateur est activé, les paramètres de la stratégie sont hérités de la stratégie du niveau supérieur de la hiérarchie. Les paramètres de la stratégie ne peuvent être modifiés si est activé dans la stratégie parent.

- **Imposer l'héritage des paramètres aux stratégies enfants**. Si le commutateur est activé, les paramètres de la stratégie sont appliqués aux stratégies enfants. Dans les paramètres de la stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée. Les paramètres de la stratégie enfant sont hérités de la stratégie parent, sauf les paramètres accompagnés de . Les paramètres des stratégies enfant ne peuvent pas être modifiés si est activé dans la stratégie parent.

6. L'onglet **Paramètres des applications** permet de configurer les paramètres de la stratégie de Kaspersky Endpoint Security.

7. Cliquez sur le bouton **Enregistrer**.

Les paramètres de Kaspersky Endpoint Security sont configurés sur les ordinateurs client à la synchronisation suivante.

Configuration des paramètres locaux de l'application

Vous pouvez configurer les paramètres de Kaspersky Endpoint Security sur un ordinateur particulier. Il s'agit des *paramètres locaux de l'application*. La modification de certains paramètres peut être impossible. Ces paramètres sont bloqués dans les propriétés de la stratégie.

Pour configurer les paramètres locaux de l'application, procédez comme suit :

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

2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez configurer les paramètres locaux de l'application.

   Les propriétés de l'ordinateur s'ouvrent.

3. Passez à la section **Applications**.

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

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

5. Passez à la section **Paramètres de l'application**.

6. Configurez les paramètres locaux de l'application.

   Les paramètres locaux de l'application sont identiques aux paramètres de la stratégie, excepté les paramètres de chiffrement.

Paramètres de la stratégie

Vous pouvez configurer les paramètres de Kaspersky Endpoint Security à l'aide d'une stratégie. Les informations détaillées sur les modules de l'application sont fournies dans les sous-sections correspondantes.

Kaspersky Security Network

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. *Kaspersky Security Network* est conçu pour recevoir ces données.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Endpoint Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

En fonction de l'emplacement de l'infrastructure, on distingue le KSN global (infrastructure hébergée sur les serveurs de Kaspersky) et le KSN privé.

Après la modification de la licence d'utilisation du KSN local, il faut transmettre les informations relatives à la nouvelle clé au fournisseur de service. Si cette opération n'est pas effectuée, l'échange d'informations avec le KSN privé n'est pas possible.

La participation des utilisateurs à Kaspersky Security Network permet à Kaspersky de récupérer efficacement des informations sur les types et les sources de menaces, de développer des moyens de neutralisation de celles-ci et de réduire le nombre de faux positifs pour les modules de l'application.

Pendant l'utilisation du mode étendu du KSN, l'application envoie automatiquement à KSN les informations statistiques obtenues lors de son fonctionnement. L'application peut également envoyer à Kaspersky des fichiers (ou partie de fichier) pour vérification complémentaire. Il s'agit de fichiers que des individus malintentionnés pourraient utiliser pour nuire à l'ordinateur ou aux données.

Vous pouvez lire des informations plus détaillées sur l'envoi à Kaspersky, le stockage et la destruction des informations statistiques obtenues lors de l'utilisation de KSN dans la Déclaration de Kaspersky Security Network et sur le site Internet de Kaspersky. Le fichier ksn_<ID de la langue>.txt qui contient la Déclaration de Kaspersky Security Network figure dans le kit de distribution.

Pour réduire la charge sur les serveurs de KSN, les spécialistes de Kaspersky peuvent lancer des bases antivirus de l'application qui désactivent temporairement ou limitent en partie la communication dans Kaspersky Security Network. Dans ce cas, l'état de la connexion à KSN apparaît comme *Activé avec des restrictions*.

Les ordinateurs des utilisateurs qui sont administrés par le serveur d'administration Kaspersky Security Center peuvent interagir avec KSN à l'aide du service KSN Proxy.

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur de l'utilisateur peut interroger KSN et transmettre à KSN des informations, même s'il n'a pas d'accès direct à Internet.
- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Pour en savoir plus sur le service KSN Proxy *consultez l'aide de Kaspersky Security Center*.

Les paramètres du service KSN Proxy peuvent être configurés dans les propriétés de la stratégie de *Kaspersky Security Center*.

L'utilisation de Kaspersky Security Network est volontaire. L'application propose d'utiliser le KSN pendant la configuration initiale de l'application. Vous pouvez commencer à utiliser le KSN ou arrêter de l'utiliser à n'importe quel moment.

Paramètres de Kaspersky Security Network

Paramètre	Description

Mode étendu du KSN	Le *mode étendu du KSN* est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Endpoint Security envoie des données supplémentaires à Kaspersky. Quelle que soit la position du commutateur, Kaspersky Endpoint Security utilise KSN pour détecter les menaces.
Mode Cloud	Si le commutateur est activé, Kaspersky Endpoint Security utilise la version allégée des bases antivirus, ce qui réduit la charge sur les ressources du système d'exploitation. Kaspersky Endpoint Security télécharge la version allégée des bases antivirus lors de la première mise à jour après que la case a été cochée. Si le commutateur est désactivé, Kaspersky Endpoint Security utilise la version complète des bases antivirus. Kaspersky Endpoint Security télécharge la version complète des bases antivirus lors de la première mise à jour après que la case a été décochée.
État de l'ordinateur en cas d'indisponibilité de KSN	Liste déroulante dont les éléments déterminent l'état de l'ordinateur dans Web Console quand les serveurs de KSN ne sont pas accessibles (**Périphériques** → **Appareils administrés**).
Utiliser KSN Proxy	Si la case est cochée, Kaspersky Endpoint Security utilise le service KSN Proxy. *KSN Proxy* est un service assurant l'interaction entre l'infrastructure de Kaspersky Security Network et les postes clients sous l'administration du Serveur d'administration.
Utiliser les serveurs de KSN lorsque KSN Proxy est inaccessible	Si la case est cochée, Kaspersky Endpoint Security utilise les serveurs KSN si le service KSN Proxy est inaccessible. Les serveurs KSN peuvent se trouver du côté de Kaspersky en cas d'utilisation du KSN global ou sur des serveurs en cas d'utilisation du KSN privé.

Détection comportementale

Le module Détection comportementale récupère des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent intervenir avec plus d'efficacité.

Le module Détection comportementale utilise des modèles de comportement d'applications dangereux. Les modèles comprennent les séries d'actions des applications que Kaspersky Endpoint Security considère comme dangereuses. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Endpoint Security exécute la réaction choisie. La fonction de Kaspersky Endpoint Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

Paramètres du module Détection comportementale

Paramètre	Description
En cas de détection de l'activité d'une application malveillante	• **Supprimer le fichier**. Si cette option est sélectionnée, Kaspersky Endpoint Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application.

	• **Arrêter le programme**. Si cette option est sélectionnée, Kaspersky Endpoint Security arrête l'application en cas de détection d'une activité malveillante de l'application. • **Notifier**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.
Protection des dossiers partagés contre le chiffrement externe	• Si le commutateur est activé, Kaspersky Endpoint Security analyse l'activité dans les dossiers partagés. Si l'activité correspond à un modèle de comportement dangereux caractéristique du chiffrement externe, Kaspersky Endpoint Security exécute l'action choisie.
En cas de détection du chiffrement externe de dossiers partagés	• **Bloquer la connexion**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté une tentative de modification des fichiers dans les dossiers partagés, bloque l'activité réseau de l'ordinateur à l'origine de la modification et crée des copies de sauvegarde des fichiers modifiés. Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde. • **Notifier**. Si vous avez choisi cette option, Kaspersky Endpoint Security, après avoir détecté une tentative de modification des fichiers dans les dossiers partagés, ajoute les informations relatives à cette tentative de modification des fichiers dans les dossiers partagés à la liste des menaces actives. La protection contre les tentatives de chiffrement externe offerte par Kaspersky Endpoint Security porte uniquement sur les fichiers qui se trouvent sur des supports dotés d'un système de fichiers NTFS et qui ne sont pas chiffrés à l'aide du système EFS.
Bloquer la connexion pendant X minutes	Durée pendant laquelle Kaspersky Endpoint Security bloque l'activité réseau d'un ordinateur distant qui chiffre les dossiers partagés. La valeur par défaut est de 60 minutes.
Exclusions	La liste des ordinateurs pour lesquels les tentatives de chiffrement des dossiers partagés ne sont pas traquées. Pour pouvoir profiter de la liste d'exclusion des ordinateurs de la protection des dossiers partagés contre le chiffrement externe, il faut activer la stratégie d'Audit de l'accès au système. Cette stratégie est désactivée par défaut (pour en savoir plus sur l'activation du service d'audit de l'accès au système, consultez le site de Microsoft).

Protection contre les Exploits

Le module Protection contre les Exploits traque les fichiers exécutables lancés par les applications vulnérables. S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Endpoint Security bloque le lancement de ce fichier. Les informations relatives à l'interdiction du lancement du fichier exécutable sont consignées dans le rapport sur le fonctionnement de la Protection contre les Exploits.

Paramètres du module Protection contre les Exploits

Paramètre	Description
En cas de détection d'un exploit	• **Bloquer l'opération**. Si vous choisissez cette option, Kaspersky Endpoint Security bloque toutes les opérations de cet exploit après la détection de ce dernier. • **Notifier**. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert un exploit ajoute les informations relatives à l'exploit dans la liste des menaces actives.
Protection de la mémoire des processus système	Si le commutateur est activé, Kaspersky Endpoint Security bloque les processus tiers qui tentent d'accéder à la mémoire des processus système.

Prévention des intrusions

Le module Prévention des intrusions (en anglais, HIPS – Host Intrusion Prevention System) empêche l'exécution des actions dangereuses pour le système et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles.

Le module contrôle les applications, y compris l'accès des applications aux ressources protégées (fichiers et dossiers, clés du registre), à l'aide des *privilèges des applications*. Les privilèges des applications représentent un ensemble de restrictions pour différentes actions des applications dans le système d'exploitation et un ensemble de droits d'accès aux ressources de l'ordinateur.

Le module Pare-feu contrôle l'activité réseau des applications.

Au premier lancement de l'application sur l'ordinateur, le module Prévention des intrusions vérifie le niveau de danger de l'application et la place dans un des groupes de confiance. Le groupe de confiance définit les privilèges que Kaspersky Endpoint Security utilise pour contrôler l'activité des applications.

Pour contribuer au fonctionnement plus efficace du module Prévention des intrusions, il est conseillé de participer au Kaspersky Security Network. Les données obtenues à l'aide de Kaspersky Security Network permettent de référer plus précisément les applications à un groupe de confiance ou à un autre, et aussi appliquer les paramètres optimaux pour les privilèges des applications.

Lors du prochain lancement de l'application, la Prévention des intrusions analyse l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les privilèges des applications existants. En cas de modification de l'application, la Prévention des intrusions l'analyse comme s'il s'agissait de sa première exécution.

Paramètres du module Prévention des intrusions

Paramètre	Description
Privilèges des applications	Liste consolidée de toutes les

	applications installées sur les ordinateurs administrés par la stratégie.
Ressources protégées	La liste contient les ressources de l'ordinateur réparties en catégories. Le module Prévention des intrusions contrôle l'accès des autres programmes aux ressources de cette liste. La ressource peut être une catégorie, un fichier ou un dossier, une clé de registre. Si la case en regard de la ressource est cochée, cela signifie qu'elle est protégée par le module Prévention des intrusions.
Mettre à jour les autorisations pour les applications inconnues depuis la base KSN	Si la case est cochée, le module Prévention des intrusions met à jour les privilèges des applications inconnues jusqu'alors à l'aide des bases Kaspersky Security Network.
Faire confiance aux applications dotées d'une signature numérique	Si la case est cochée, le module Prévention des intrusions place les applications dotées d'une signature numérique dans le groupe "De confiance". Si la case est décochée, le module Prévention des intrusions ne considère pas les applications dotées d'une signature numérique comme des applications de confiance et détermine leur groupe de confiance sur la base d'autres paramètres.
Supprimer les droits des applications non lancées depuis plus de X jours	Si la case est cochée, Kaspersky Endpoint Security supprime automatiquement les informations relatives à l'application (groupe de confiance, privilèges d'accès) si les conditions suivantes sont remplies : • Vous avez placé manuellement l'application dans un groupe de confiance ou vous avez configuré manuellement des privilèges d'accès. • L'application n'a plus été lancée depuis une durée déterminée.

	Si le groupe de confiance et les privilèges sont déterminés automatiquement, Kaspersky Endpoint Security supprime les informations relatives à cette application après 30 jours. Il n'est pas possible de modifier la durée de conservation des informations relatives à l'application ou de désactiver la suppression automatique. Au prochain lancement de l'application, Kaspersky Endpoint Security l'examine comme au premier lancement.
Les applications dont le groupe de confiance n'a pas pu être déterminé sont placées automatiquement dans	La liste déroulante dont les éléments déterminent le groupe de confiance dans lequel Kaspersky Endpoint Security va placer l'application inconnue. Vous avez le choix entre les options suivantes : • **Restrictions faibles**. • **Restrictions élevées**. • **Douteuses**.
Les applications lancées avant Kaspersky Endpoint Security for Windows sont automatiquement placées dans le groupe de confiance	La liste déroulante dont les éléments déterminent le groupe de confiance dans lequel Kaspersky Endpoint Security va placer les applications lancées avant Kaspersky Endpoint Security. Vous avez le choix entre les options suivantes : • **Restrictions faibles**. • **Restrictions élevées**. • **Douteuses**. • **De confiance**.

Réparation des actions malicieuses

Le module Réparation des actions malicieuses permet à Kaspersky Endpoint Security d'exécuter le retour à l'état antérieur aux actions des applications malveillantes dans le système d'exploitation.

Lors de la restauration des actions du programme malveillant dans le système d'exploitation, Kaspersky Endpoint Security traite les types suivants d'activité de programme malveillant :

- **Activité de fichiers**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - suppression des fichiers exécutables créés par l'application malveillante (sur tous les supports, sauf les disques réseau) ;
  - suppression des fichiers exécutables créés par les applications dans lesquelles une application malveillante s'est introduite ;
  - restauration des fichiers modifiés ou supprimés par l'application malveillante.

- **Activité sur la base de registre**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - suppression des sections et des clés de registre créées par l'application malveillante ;
  - non-restauration des sections et clés de registre modifiées ou supprimées par l'application malveillante.

- **Activité système**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - arrêt des processus lancés par l'application malveillante ;
  - arrêt des processus dans lesquels l'application malveillante s'est introduite.
  - non-rétablissement des processus arrêtés par l'application malveillante.

- **Activité réseau**

  Kaspersky Endpoint Security réalise les opérations suivantes :

  - interdiction de l'activité réseau de l'application malveillante ;
  - interdiction de l'activité réseau des processus dans lesquels l'application malveillante s'est introduite.

L'annulation des actions de l'application malveillante peut être lancée par le module Protection contre les fichiers malicieux, Détection comportementale ou lors de la recherche de virus.

Le retour à l'état antérieur aux actions du programme malveillant touche un ensemble de données clairement délimité. Cela n'a aucun impact négatif sur le fonctionnement du système d'exploitation, ni sur l'intégrité des informations enregistrées sur l'ordinateur.

Protection contre les fichiers malicieux

Lors de l'ouverture ou du lancement d'un fichier dont le contenu sur OneDrive, Kaspersky Endpoint Security charge et analyse le contenu de ce fichier.

Le module Protection contre les fichiers malicieux permet d'éviter l'infection du système de fichiers de l'ordinateur. La Protection contre les fichiers malicieux est lancée par défaut au démarrage de Kaspersky Endpoint Security. Elle se trouve en permanence dans la mémoire vive de l'ordinateur et analyse les fichiers ouverts et exécutés sur l'ordinateur ainsi que sur les disques montés. Elle recherche les virus et autres applications présentant une menace. L'analyse est exécutée conformément aux paramètres de l'application.

En cas de détection d'une menace dans un fichier, Kaspersky Endpoint Security exécute les actions suivantes :

1. Détermine le type d'objet détecté dans le fichier (comme un *virus* ou un *cheval de Troie*).

2. L'application affiche une notification sur l'objet malveillant détecté dans le fichier (si les notifications sont configurées), et traite le fichier en prenant l'action précisée dans les paramètres du module Protection contre les fichiers malicieux.

Paramètres du module Protection contre les fichiers malicieux

Paramètre	Description
Zone de protection	Contient les objets que le module Protection contre les fichiers malicieux analyse. L'objet de l'analyse peut être un disque dur ou un disque réseau, un dossier, un fichier ou un masque d'un nom de fichier. Le module Protection contre les fichiers malicieux analyse par défaut les fichiers exécutés sur tous les disques durs, les disques amovibles et les disques réseau. Les objets qui figurent par défaut dans la liste de la **zone de protection** ne peuvent être ni modifiés ni supprimés. Si la case en regard du nom de l'objet est cochée, il est analysé par le module Protection contre les fichiers malicieux.
Action en cas de détection d'une menace	• **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. • **Désinfecter ; bloquer si la désinfection est impossible**. Si vous choisissez cette option, le module Protection contre les fichiers malicieux essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les fichiers malicieux bloque ces fichiers. • **Interdire**. Si cette option est sélectionnée, le module Protection contre les fichiers malicieux bloque automatiquement les fichiers infectés sans tenter de les désinfecter. Avant de désinfecter ou de supprimer un fichier, le module Protection contre les fichiers malicieux crée une copie de sauvegarde au cas où la restauration du fichier serait requise ou si la possibilité de le désinfecter se présentait.
Analyser uniquement les nouveaux fichiers et les fichiers modifiés	La case active/désactive le mode d'analyse seulement des nouveaux fichiers et de ceux qui ont été modifiés depuis leur dernière analyse. Le module Protection contre les fichiers malicieux analyse les fichiers simples et les fichiers composés.
Analyser les archives	La case active/désactive l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Analyser les	La case active / désactive l'analyse des paquets de distribution.

paquets de distribution	
Analyser les fichiers aux formats Office	La case active/désactive la fonction qui permet au module Protection contre les fichiers malicieux d'analyser les fichiers au format Office DOC, DOCX, XLS, PPT et autres, lors de la recherche de virus. Les objets OLE appartiennent également aux fichiers au format Office.
Ne pas décompresser les fichiers composés de grande taille	Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie dans le champ **Taille maximale du fichier**. Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille. Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.
Décompresser les fichiers composés en arrière-plan	Si la case est cochée, Kaspersky Endpoint Security décompresse les fichiers composés, dont la taille dépasse la valeur indiquée dans le champ **Taille minimale du fichier** en arrière-plan et avec un retard après leur détection. Ces fichiers peuvent être utilisés pendant l'analyse. Les fichiers composés dont la taille est inférieure à la valeur indiquée dans le champ **Taille minimale du fichier** ne peuvent être utilisés qu'après avoir été décompressés et analysés. Si la case est décochée, Kaspersky Endpoint Security décompresse tous les fichiers composés. Les fichiers composés peuvent être utilisés uniquement après la décompression et l'analyse du contenu.

Protection contre les menaces Internet

Chaque fois que l'utilisateur travaille sur Internet, les informations enregistrées sur son ordinateur sont exposées à un risque d'infection par des virus et par d'autres applications présentant une menace. Ces menaces peuvent s'introduire dans l'ordinateur lors du téléchargement d'applications gratuites ou lors de la consultation de sites Internet, attaqués par des individus malintentionnés, avant la visite de l'utilisateur. Les vers de réseau peuvent s'introduire sur l'ordinateur des utilisateurs avant l'ouverture des pages Internet ou le téléchargement d'un fichier, directement au moment de la connexion à Internet.

Le module Protection contre les menaces Internet protège les informations qui arrivent sur l'ordinateur des utilisateurs et qui sont envoyées depuis celui-ci via les protocoles HTTP et FTP. Il permet également de déterminer si un lien est malveillant ou s'il mène à un site de phishing.

Chaque page Internet ou fichier auquel accède l'utilisateur ou une application via le protocole HTTP ou FTP est intercepté et analysé par le module Protection contre les menaces Internet pour détecter la présence éventuelle de virus et d'autres applications présentant une menace. Ensuite, l'application procède ainsi :

- Si aucun code malveillant n'a été détecté sur la page Internet ou dans le fichier, ils deviennent immédiatement accessibles à l'utilisateur.
- Si la page Internet ou le fichier que souhaite ouvrir l'utilisateur contient un code malveillant, l'application exécute l'action définie dans les paramètres de la Protection contre les menaces Internet.

Paramètres du module Protection contre les menaces Internet

Paramètre	Description
Action en cas de détection	• **Notifier**. Si vous choisissez cette option, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet autorise le chargement de cet objet sur l'ordinateur et Kaspersky Endpoint Security ajoute au

d'une menace	journal une entrée contenant des informations sur l'objet infecté et ajoute les informations relatives à l'objet infecté à la liste des menaces actives. • **Interdire le téléchargement**. Si cette action est sélectionnée, en cas de détection d'un objet infecté dans le trafic Internet, le module Protection contre les menaces Internet bloque l'accès à l'objet, affiche sur l'écran une fenêtre de notification sur le blocage et consigne dans le journal une entrée contenant les informations relatives à l'objet infecté.
Ne pas analyser le trafic Internet en provenance des adresses URL de confiance	Si la case est cochée, le module Protection contre les menaces Internet n'analyse pas le contenu des pages Internet/des sites Internet dont les adresses figurent dans la liste des URL de confiance.
URL de confiance	Contient les adresses des pages Internet/des sites Internet dont vous faites confiance au contenu. Le module Protection contre les menaces Internet n'analyse pas le contenu des pages Internet/des sites Internet dont les adresses figurent dans la liste des adresses Internet de confiance. Vous pouvez ajouter à la liste des adresses Internet de confiance l'adresse de la page Internet/du site Internet ou le masque de l'adresse de la page Internet/du site Internet. Si la case à côté de l'adresse de la page Internet/du site Internet est cochée, le module Protection contre les menaces Internet n'analyse pas le contenu de la page Internet/du site Internet.

Protection contre les menaces par emails

Le module Protection contre les menaces par emails analyse l'ensemble des messages électroniques entrants et sortants à la recherche d'éventuels virus et d'autres applications présentant une menace. Il démarre au lancement de Kaspersky Endpoint Security, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages reçus ou envoyés via les protocoles POP3, SMTP, IMAP, MAPI et NNTP. Si aucune menace n'a été détectée dans le message électronique, le message devient accessible et/ou est traité.

En cas de détection d'une menace dans le message électronique, le module Protection contre les menaces par emails exécute les actions suivantes :

1. Il attribue l'état *Infecté* au message électronique.

   Cet état est attribué au message électronique dans les cas suivants :

   - Si l'analyse du message électronique a détecté un segment de code d'un virus connu au sujet duquel les bases antivirus de Kaspersky Endpoint Security contiennent des informations.
   - Si le message électronique contient un segment de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

2. Il identifie le type d'objet détecté dans le message électronique (par exemple, virus, *cheval de Troie*).
3. Il bloque le message électronique.

4. Il affiche à l'écran une notification sur la détection d'un objet (si cela a été défini dans les paramètres des notifications).

5. Il exécute l'action définie dans les paramètres du composant Protection contre les menaces par emails.

Le module interagit avec les clients de messagerie installés sur l'ordinateur. Une extension intégrable est disponible pour le client de messagerie Microsoft Office Outlook® qui vous permet d'affiner les paramètres d'analyse des messages. L'extension du module Protection contre les menaces par emails s'intègre au client de messagerie Microsoft Office Outlook pendant l'installation de Kaspersky Endpoint Security.

Paramètres du module Protection contre les menaces par emails

Paramètre	Description
Action en cas de détection d'une menace	• **Désinfecter ; supprimer si la désinfection est impossible**. Si vous choisissez cette option, le module Protection contre les menaces par emails essaie de désinfecter automatiquement tous les messages électroniques infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails supprime les messages électroniques infectés. • **Désinfecter ; bloquer si la désinfection est impossible**. Si vous choisissez cette option, le module Protection contre les menaces par emails essaie de désinfecter automatiquement tous les messages électroniques infectés qu'il a détectés. Si la désinfection est impossible, le module Protection contre les menaces par emails bloque les messages électroniques infectés. • **Bloquer** Si cette option est sélectionnée, le module Protection contre les menaces par emails bloque automatiquement les messages électroniques infectés sans tenter de les désinfecter. Avant de désinfecter ou de supprimer un message infecté, le module Protection contre les menaces par emails crée une copie de sauvegarde au cas où la restauration du message électronique serait requise ou si la possibilité de le désinfecter se présentait.
Trafic POP3 / SMTP / NNTP / IMAP	Si la case est cochée, le module Protection contre les menaces par emails analyse le flux de messages électroniques reçu via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur. Si la case est décochée, le module Protection contre les menaces par emails n'analyse pas les messages électroniques transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur. Dans ce cas, les messages électroniques sont analysés par le plug-in du module Protection contre les menaces par emails intégré au client de messagerie Microsoft Office Outlook après leur réception sur l'ordinateur de l'utilisateur.
Extension dans Microsoft Office Outlook	Si la case est activée, l'analyse des messages électroniques transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI est activée au niveau de l'extension intégrée à Microsoft Office Outlook. En cas d'analyse du courrier à l'aide de l'extension du module Protection contre les menaces par emails pour Outlook, il est recommandé d'utiliser le Mode Exchange mis en cache (Use Cached Exchange Mode). Vous pouvez obtenir tous les détails sur le mode Exchange mis en cache et sur ses recommandations d'utilisation dans la base de connaissances de Microsoft.
Ne pas analyser les archives de plus de X Mo	Si la case est cochée, le module Protection contre les menaces par emails exclut de l'analyse les archives jointes aux messages électroniques dont la taille est supérieure à la valeur définie. Vous pouvez accéder au champ qui permet de définir la taille maximale des pièces jointes aux messages électroniques.

	Si la case est décochée, le module Protection contre les menaces par emails analyse les archives de toute taille jointes aux messages électroniques. Cette fonction permet d'accélérer l'analyse des emails.
Ne pas analyser les archives pendant plus de X s.	Si la case est cochée, la durée d'analyse des archives jointes aux emails est limitée à la valeur définie. Le champ qui permet de définir la durée maximale de l'analyse des archives jointes aux messages électroniques est accessible.
Filtre des pièces jointes	La fonction de filtrage des pièces jointes ne s'applique pas aux messages électroniques sortants. • **Désactiver le filtre**. Si ce paramètre est sélectionné, le module Protection contre les menaces par emails ne filtre pas les fichiers joints aux messages électroniques. • **Renommer les types de pièces jointes indiqués**. Si ce paramètre est sélectionné, le module Protection contre les menaces par emails remplace le dernier caractère du nom des fichiers joints du type défini par un trait de soulignement ("_"). • **Supprimer les types de pièces jointes indiqués**. Si ce paramètre est sélectionné, le module Protection contre les menaces par emails supprime les fichiers joints des types de messages électroniques indiqués. Vous pouvez indiquer les types de fichiers joints à renommer ou à supprimer des messages électroniques dans la liste des masques de fichiers.
Masques de fichiers	Liste des masques de fichiers que le module Protection contre les menaces par emails va renommer ou supprimer après le filtrage des pièces jointes dans les messages électroniques. Si la case en regard du masque de fichier est cochée, le module Protection contre les menaces par emails renomme ou supprime les fichiers de ce type pendant le filtrage des pièces jointes dans les messages électroniques.

Protection contre les menaces réseau

Le module Protection contre les menaces réseau (Intrusion Detection System en anglais) recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque l'activité réseau de l'ordinateur attaquant. Un message vous avertit après qu'une tentative d'attaque réseau a été effectuée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

L'activité réseau de l'ordinateur à l'origine de l'attaque est bloquée pendant une heure. Vous pouvez modifier les paramètres du blocage de l'ordinateur attaquant.

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Endpoint Security. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la mise à jour des bases et des modules de l'application.

Paramètres du module Protection contre les menaces réseau

Paramètre	Description

Bloquer l'ordinateur à l'origine de l'attaque pendant X minutes	Si la case est cochée, le module Prévention des intrusions ajoute l'ordinateur à l'origine de l'attaque à la liste des ordinateurs à bloquer. Cela signifie que la Protection contre les menaces réseau bloque l'activité réseau de l'ordinateur attaquant après la première tentative d'attaque réseau pendant la durée indiquée. Ce groupe protège automatiquement l'ordinateur de l'utilisateur contre d'éventuelles attaques réseau futures à partir de la même adresse. Vous pouvez modifier la durée de blocage de l'activité réseau de l'ordinateur à l'origine de l'attaque. La valeur par défaut est de 60 minutes.
Exclusions	La liste contient les adresses IP à l'origine des attaques réseau que le module Prévention des intrusions ne bloque pas. Kaspersky Endpoint Security n'ajoute pas au rapport les informations sur les attaques réseau en provenance des adresses IP de la liste des exclusions.
Mode de protection contre le MAC Spoofing	L'attaque MAC Spoofing consiste à substituer l'adresses MAC du périphérique réseau (adaptateur réseau). En fin de compte, les données envoyées au périphérique peuvent être redirigées vers le port auquel l'individu malintentionné est connecté. Kaspersky Endpoint Security permet de bloquer les attaques de type MAC Spoofing et de recevoir les notifications relatives aux attaques.

Pare-feu

Tout ordinateur connecté aux réseaux locaux et à l'Internet risque non seulement une infection par des virus et d'autres applications présentant une menace, mais il est aussi ouvert aux différentes attaques qui exploitent les vulnérabilités des systèmes d'exploitation et du logiciel.

Le Pare-feu garantit la protection des données personnelles stockées sur l'ordinateur de l'utilisateur, car il bloque la majorité des menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local. Le Pare-feu permet de détecter toutes les connexions réseau sur l'ordinateur de l'utilisateur et d'afficher une liste de leurs adresses IP en indiquant l'état de la connexion réseau par défaut.

Le module Pare-feu filtre toutes les activités du réseau en fonction des règles réseau. La configuration des règles réseau permet de définir le niveau de la protection de l'ordinateur qui peut varier entre un blocage complet de l'accès Internet et l'autorisation de l'accès illimité.

Paramètres du module Pare-feu

Paramètre	Description
Règles pour les paquets réseau	Tableau contenant la liste des règles pour les paquets réseau. Règles pour les paquets réseau sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Le tableau reprend les règles préinstallées pour les paquets réseau qui sont recommandées par les experts de Kaspersky pour une protection optimale du trafic réseau des ordinateurs sous l'administration des systèmes d'exploitation Microsoft Windows. Les règles pour les paquets réseau ont priorité sur les règles réseau pour les applications. Le Pare-feu établit une priorité d'exécution pour chaque règle pour le paquet réseau. La priorité de la règle pour les paquets réseau est définie par l'emplacement de la règle dans la liste des règles pour les paquets réseau. La première règle pour les paquets réseau de la liste est celle qui possède la priorité la plus élevée. Pare-feu traite les règles pour les paquets réseau selon leur ordre d'apparition dans la liste des pour les paquets réseau haut/bas. Le Pare-feu trouve dans la liste la première règle pour le paquet réseau convenant pour la connexion réseau et exécute son action : autorise ou bloque l'activité réseau. Le Pare-feu ignore toutes les règles pour les paquets réseau suivantes.

Réseaux	Le tableau qui contient les informations sur les connexions réseau que le Pare-feu a détectées sur l'ordinateur de l'utilisateur. Le réseau Internet reçoit par défaut l'état *Réseau public*. Vous ne pouvez pas modifier l'état du réseau Internet.
Règles réseau	Tableau des règles réseau pour les applications Conformément aux règles réseau, les modules de Kaspersky Endpoint Security règlent l'activité de fichiers et de réseau des applications dans les systèmes d'exploitation. Le module Pare-feu règle l'accès des applications aux ressources réseau.

Protection BadUSB

Certains virus modifient l'application interne des périphériques USB afin que le système d'exploitation considère le périphérique USB comme un clavier.

Le module Protection BadUSB permet d'empêcher la connexion de périphériques USB infectés qui imitent un clavier.

Quand un périphérique USB est connecté à l'ordinateur et que le système d'exploitation le considère comme un clavier, l'application génère un code numérique qu'elle propose à l'utilisateur de saisir via ce clavier ou via un clavier numérique (si disponible). C'est ce qu'on appelle l'autorisation du clavier. L'application autorise l'utilisation du clavier autorisé et bloque tout clavier qui n'a pas réussi l'autorisation.

Paramètres du module Protection BadUSB

Paramètre	Description
Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB	Si la case est cochée, l'application autorise l'utilisation d'un clavier virtuel pour autoriser le périphérique USB à partir duquel la saisie du code d'autorisation est impossible.

Fournisseur de protection AMSI

Le fournisseur de protection AMSI est prévu pour la prise en charge de l'interface Antimalware Scan Interface de Microsoft. L'*interface Antimalware Scan Interface (AMSI)* permet à une application tierce compatible avec AMSI d'envoyer des objets à Kaspersky Endpoint Security en vue d'une analyse complémentaire (par exemple, des scripts PowerShell) et d'obtenir les résultats de l'analyse de ces objets. Pour en savoir plus sur l'interface AMSI, consultez la *documentation de Microsoft*.

Le fournisseur d'événements de protection AMSI peut uniquement détecter une menace et la signaler à l'application tierce. Il ne peut pas la traiter. Après la réception de la notification sur la menace, l'application tierce empêche l'exécution des actions malveillantes (par exemple, elle interrompt le fonctionnement). Si l'objet est ajouté à l'exclusion de l'analyse, le Fournisseur de protection AMSI n'exécute pas l'analyse à la réception de la demande de l'application tierce.

Le composant Fournisseur de protection AMSI peut rejeter la demande d'une application tierce, par exemple, si cette application a excédé le nombre maximum de demande pour l'intervalle défini. Kaspersky Endpoint Security envoie les informations relatives au rejet de la demande de l'application tierce au Serveur d'administration. Le composant Fournisseur de protection AMSI ne rejette pas les demandes des applications tierces pour lesquelles la case **Ne pas bloquer l'interaction avec le fournisseur de protection AMSI** a été cochée.

Le module Fournisseur de protection AMSI est disponible pour les systèmes d'exploitation suivants pour postes de travail et serveurs de fichiers :

- Windows 10 Home / Pro / Education / Enterprise (32 / 64 bits) ;
- Windows Server 2016 (64 bits) ;
- Windows Server 2019 (64 bits) ;

Paramètres du module Fournisseur de protection AMSI

Paramètre	Description
Analyser les archives	La case active/désactive l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Analyser les paquets de distribution	La case active / désactive l'analyse des paquets de distribution des logiciels tiers.
Analyser les fichiers aux formats Office	La case active / désactive l'analyse des fichiers aux formats Office.
Ne pas décompresser les fichiers composés de grande taille	Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie dans le champ **Taille maximale du fichier**. Si la case est décochée, Kaspersky Endpoint Security analyse les fichiers composés de n'importe quelle taille. Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives, que la case **Ne pas décompresser les fichiers composés de grande taille** soit cochée ou non.

Contrôle des applications

Le composant Contrôle des applications surveille les tentatives de démarrage des applications par les utilisateurs et régit le démarrage des applications à l'aide des *règles de Contrôle des applications*.

Le lancement des applications dont aucun paramètre ne respecte les règles de Contrôle des applications est régi par le mode sélectionné de fonctionnement du module. Le mode *Liste noire* est sélectionné par défaut. Ce mode permet à n'importe quel utilisateur de lancer n'importe quelle application. Quand l'utilisateur tente de lancer une application interdite par les règles de Contrôle des applications, Kaspersky Endpoint Security bloque le lancement de cette application (si l'action **Appliquer les règles** a été choisie) ou enregistre les informations relatives au lancement de l'application dans le rapport (si l'action **Tester les règles** a été choisie).

Toutes les tentatives de l'utilisateur visant à lancer des applications sont consignées dans des rapports.

Paramètres du module Contrôle des applications

Paramètre	Description

Mode d'essai	Si le commutateur est activé, Kaspersky Endpoint Security autorise le lancement de l'application interdite dans le mode actuel du Contrôle des applications et consigne les informations relatives au lancement dans le rapport.
Mode de contrôle	Vous avez le choix entre les options suivantes : • **Liste blanche**. Si vous choisissez cette option, le Contrôle des applications interdit aux utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'autorisation de Contrôle des applications. • **Liste noire**. Si vous choisissez cette option, le Contrôle des applications permet à tous les utilisateurs de lancer n'importe quelle application, à l'exception des cas qui répondent aux règles d'interdiction de Contrôle des applications. Le choix du mode **Liste Blanche** entraîne la création automatique de deux règles de Contrôle des applications : • **Système d'exploitation et ses modules**. • **Programmes de mise à jour de confiance**. Il est impossible de modifier les paramètres et de supprimer les règles créées automatiquement. Vous pouvez activer ou désactiver ces règles.
Contrôler les DLL et les pilotes	Si la case est cochée, Kaspersky Endpoint Security contrôle le chargement des modules DLL lors du lancement des applications par les utilisateurs. Les informations relatives au module DLL et à l'application qui a chargé celui-ci seront enregistrées dans le rapport. Au moment d'activer la fonction de contrôle de chargement des modules DLL et des pilotes, assurez-vous que la règle par défaut *Système d'exploitation et ses modules* ou toute autre règle qui contient la catégorie KL *Certificats de confiance* est activée dans la section du Contrôle des applications et qu'elle garantit le chargement des modules DLL et des pilotes de confiance avant le lancement de Kaspersky Endpoint Security. L'activation du contrôle du chargement des modules DLL et des pilotes lorsque la règle *Système d'exploitation et ses modules* est désactivée peut provoquer l'instabilité du système d'exploitation. Kaspersky Endpoint Security contrôle uniquement les modules DLL et les pilotes chargés à partir du moment où la case **Contrôler les DLL et les pilotes** a été cochée. Il est conseillé de redémarrer l'ordinateur après avoir coché la case **Contrôler les DLL et les pilotes** pour permettre à Kaspersky Endpoint Security de surveiller tous les modules DLL et les pilotes, y compris ceux qui se chargent avant le lancement de Kaspersky Endpoint Security.
Modèles de messages	• **Message pour l'utilisateur**. Le champ de saisie contient le modèle du message qui apparaît suite au déclenchement d'une règle de Contrôle des applications bloquant le lancement de l'application. • **Message pour l'administrateur**. Le champ de saisie contient le modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage du lancement de l'application est intervenu par erreur.

Contrôle des périphériques

Contrôle des périphériques garantit la sécurité des données confidentielles en limitant l'accès des utilisateurs aux périphériques installés ou connectés à l'ordinateur :

- périphériques de mémoire (disques durs, disques amovibles, lecteurs de bande, CD/DVD) ;
- dispositifs de transmission des informations (modems, carte de réseau externe) ;
- dispositifs de conversion en sortie papier (imprimantes) ;
- bus de connexion (ci-après bus) : interfaces qui permettent de connecter les périphériques à l'ordinateur (USB, FireWire, Infrarouge, etc.).

Le Contrôle des périphériques gère l'accès utilisateur aux périphériques à l'aide des *règles d'accès aux périphériques* (ci-après règles d'accès) et des *règles d'accès aux bus de connexion* (ci-après règles d'accès aux bus).

Si l'accès à l'appareil dépend du bus de connexion (état), Kaspersky Endpoint Security n'enregistre pas l'événement de connexion/de déconnexion de l'appareil. Pour permettre à Kaspersky Endpoint Security d'enregistrer les événements de connexion/déconnexion de l'appareil, autorisez l'accès à l'appareil (l'état) ou ajoutez l'appareil à la liste de confiance.

Paramètres du module Contrôle des périphériques

Paramètre	Description
Autoriser la demande d'accès temporaire	Si la case est cochée, alors le bouton **Demander l'accès** dans l'interface locale de Kaspersky Endpoint Security est accessible. Cliquez sur ce bouton pour ouvrir la fenêtre **Demande d'accès au périphérique**. Cette fenêtre permet à l'utilisateur de demander un accès temporaire au périphérique bloqué.
Règles d'accès pour les périphériques et les réseaux Wi-Fi	Tableau reprenant tous les types possibles de périphériques selon la classification du module Contrôle des périphériques, ainsi que l'état d'accès à ceux-ci.
Bus de connexion	Tableau avec la liste de tous les types possibles de bus de connexion selon la classification du module Contrôle des périphériques, ainsi que l'état d'accès à ces types de bus.
Périph. de confiance	Tableau proposant les données suivantes : • **Nom**. La colonne affiche les noms des périphériques de confiance. • **Utilisateurs**. La colonne affiche les noms des utilisateurs et/ou les groupes d'utilisateurs qui ont toujours accès aux périphériques. • **Commentaires**. La colonne affiche les informations sur les périphériques de confiance que vous avez saisies à l'étape d'ajout des périphériques dans cette liste des périphériques de confiance. • **Modèle/identificateur de l'appareil**. La colonne affiche les modèles et/ou les identificateurs des périphériques de confiance.

	• **Type de périphérique**. Colonne qui affiche les types de périphérique auxquels appartient le périphérique.
Anti-Bridging	Tableau contenant les règles d'établissement des connexions. Si la règle est utilisée, Kaspersky Endpoint Security exécute les actions suivantes : • bloque la connexion active lors de l'établissement d'une nouvelle connexion si le type de périphérique indiqué dans la règle est utilisé pour les deux connexions ; • bloque les connexions établies à l'aides des types de périphérique soumis à des règles d'une priorité inférieure.
Modèles	• **Message pour l'utilisateur**. Le champ de saisie contient le modèle du message qui s'affiche lorsque l'utilisateur essaie de se connecter au périphérique bloqué ou d'exécuter une opération sur le contenu du périphérique qui lui est interdite. • **Message pour l'administrateur**. Le champ de saisie contient le modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès au périphérique ou l'interdiction des opérations impliquant le contenu du périphérique sont intervenus par erreur.

Contrôle Internet

Le module Contrôle Internet permet de contrôler l'activité utilisateur du réseau local d'entreprise : limiter ou autoriser l'accès aux sites Internet.

Une ressource Internet désigne aussi bien une page Internet individuelle ou plusieurs pages ainsi qu'un site Internet ou plusieurs sites regroupés selon des traits communs.

Le Contrôle Internet offre les possibilités suivantes :

- Économie du trafic.

  Pour contrôler le trafic le module offre la possibilité de limiter ou interdire le téléchargement des fichiers multimédia et de limiter ou interdire l'accès aux sites Internet sans rapport avec l'activité professionnelle.

- Délimitation de l'accès selon les catégories de contenu des sites Internet.

  Pour minimiser le trafic et les pertes éventuelles dues à l'abus d'accès, vous pouvez limiter ou interdire l'accès aux sites Internet de catégories spécifiques (par exemple, interdire l'accès aux sites Internet appartenant à la catégorie "Communication sur Internet").

- Une gestion centralisée d'accès aux sites Internet.

  Dans le cadre de l'utilisation de Kaspersky Security Center, il est possible de configurer l'accès aux ressources Internet tant pour des individus que pour des groupes.

Toutes les restrictions et tous les blocs appliqués pour accéder aux ressources Internet sont implémentés en tant que règles d'accès aux ressources Internet.

Paramètres du module Contrôle Internet

Paramètre	Description

Règle par défaut	La *règle par défaut* est une règle d'accès aux sites Internet qui ne figurent dans aucune des règles sélectionnées. Valeurs possibles : • **Autoriser tout ce qui ne figure pas dans la liste des règles** • **Interdire tout ce qui ne figure pas dans la liste des règles**
Liste des règles	Tableau contenant les règles d'accès aux sites Internet
Modèles de messages	• **Avertissement**. Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui avertit de la tentative d'accès au site Internet déconseillé est appliquée. • **Blocage**. Le champ de saisie contient un modèle de message qui s'affiche lorsque la règle qui bloque l'accès au site Internet est appliquée. • **Message pour l'administrateur**. Le champ de saisie contient le modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'accès au site Internet est intervenu par erreur.

Contrôle évolutif des anomalies

Le composant Contrôle évolutif des anomalies est disponible uniquement pour les produits Kaspersky Endpoint Security for Business Extended et Kaspersky Total Security for Business (pour en savoir plus sur les produits Kaspersky Endpoint Security for Business, consultez le site de Kaspersky).

Le module Contrôle évolutif des anomalies surveille et bloque les actions suspectes atypiques pour les ordinateurs du réseau de l'organisation. Le Contrôle évolutif des anomalies utilise un ensemble de règles (par exemple, la règle *Lancement de Windows PowerShell depuis une application de bureautique*) pour suivre les actions atypiques. Ces règles sont créées par les experts de Kaspersky sur la base des scénarios typiques d'action malveillantes. Vous pouvez choisir le comportement du Contrôle évolutif des anomalies pour chacune des règles et, par exemple, autoriser le lancement de scripts PowerShell pour automatiser l'exécution des tâches d'entreprise. Kaspersky Endpoint Security met à jour l'ensemble de règles à l'aide les bases de données de l'application. La mise à jour de l'ensemble de règles doit être confirmer manuellement.

Configuration du Contrôle évolutif des anomalies

La configuration du Contrôle évolutif des anomalies comprend les étapes suivantes :

1. Apprentissage du Contrôle évolutif des anomalies

   Une fois que le Contrôle évolutif des anomalies a été activé, les règles fonctionnent en *mode d'apprentissage*. Au cours de l'apprentissage, le Contrôle évolutif des anomalies surveille le déclenchement des règles et envoie les événements déclencheurs à Kaspersky Security Center. La durée du mode d'apprentissage est propre à chaque règle. Celle-ci est définie par les experts de Kaspersky. En règle générale, le mode d'apprentissage dure 2 semaines.

   Si une règle n'a jamais été déclenchée lors de l'apprentissage, le Contrôle évolutif des anomalies considère les actions associées à cette règle comme suspectes. Kaspersky Endpoint Security bloquera toutes les actions associées à cette règle.

Si la règle c'est déclenchée lors de l'apprentissage, Kaspersky Endpoint Security enregistre les événements dans rapport sur les déclenchements des règles et dans le stockage **Fonctionnement des règles en mode d'apprentissage**.

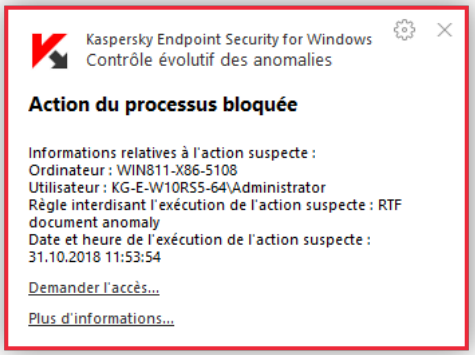
2. Analyse du rapport sur les déclenchements des règles

   L'administrateur analyse le rapport sur les déclenchements des règles ou le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Ensuite, l'administrateur peut sélectionner le comportement du Contrôle évolutif des anomalies lors du déclenchement d'une règle : bloquer ou autoriser. En outre, l'administrateur peut continuer à surveiller le déclenchement de la règle et prolonger le fonctionnement d'application en mode d'apprentissage. Si l'administrateur ne prend aucune mesure, l'application continuera également à fonctionner en mode d'apprentissage. Le décompte de la durée du mode d'apprentissage est remis à zéro.

La configuration du Contrôle évolutif des anomalies se déroule en temps réel. La configuration du Contrôle évolutif des anomalies se déroule de la manière suivante :

- Le Contrôle évolutif des anomalies commence automatiquement à bloquer les actions associées aux règles qui ne se sont pas déclenchées lors de l'apprentissage.
- Kaspersky Endpoint Security ajoute de nouvelles règles ou supprime les règles qui ne sont plus pertinentes.
- L'administrateur configure le fonctionnement du Contrôle évolutif des anomalies après avoir analysé le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**. Il est recommandé de vérifier le rapport sur les déclenchements des règles et le contenu du stockage **Fonctionnement des règles en mode d'apprentissage**.

Lorsqu'une application malveillante tente d'effectuer une action, Kaspersky Endpoint Security la bloque et affiche une notification (cf. ill. ci-après).



Notification du Contrôle évolutif des anomalies

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Kaspersky Endpoint Security autorise ou non l'exécution d'une action associée à une règle selon l'algorithme suivant (cf. ill. ci-dessous).

Algorithme de fonctionnement du Contrôle évolutifs des anomalies

Paramètres du module Contrôle évolutif des anomalies

Paramètre	Description
Rapport sur l'état des règles	Ce rapport contient des informations sur l'état des règles de détection du Contrôle évolutif des anomalies (par exemple, les états *Désactivé* ou *Bloquer*). Le rapport est créé pour tous les groupes d'administration.
Rapport sur les déclenchements des règles	Ce rapport contient les informations sur les actions suspectes détectées par le Contrôle évolutif des anomalies. Le rapport est créé pour tous les groupes d'administration.
Règles	Tableau des règles du Contrôle évolutif des anomalies Les règles ont été créées par les experts de Kaspersky sur la base des scénarios typiques d'activités potentiellement malveillantes.
Modèles de messages	• **Blocage**. Modèle de message destiné à l'utilisateur et qui s'affiche en cas de déclenchement de la règle du Contrôle évolutif des anomalies qui bloque l'action suspecte. • **Message pour l'administrateur**. Modèle du message à envoyer à l'administrateur du réseau local d'entreprise si l'utilisateur croit que le blocage de l'action est intervenu par erreur.

Endpoint Sensor

Endpoint Sensor est un module de Kaspersky Anti Targeted Attack Platform (KATA). Cette solution a été développée pour détecter en temps utiles les menaces telles que les attaques ciblées.

Le module s'installe sur les ordinateurs client. Sur ces ordinateurs, le module contrôle en permanence les processus, les connexions réseau ouvertes et les fichiers modifiés. Endpoint Sensor transmet les informations au serveur KATA.

Les fonctions du composant sont disponibles pour les systèmes d'exploitation suivants :

- Windows 7 Enterprise Service Pack 1 (32 / 64 bits) ;
- Windows 8.1.1 Enterprise (32 / 64 bits) ;
- Windows 10 RS3 / RS4 / RS5 / 19H1 (32 / 64-bit) ;
- Windows Server 2008 R2 Enterprise (64 bits) ;
- Windows Server 2012 Standard / R2 Standard (64 bits) ;
- Windows Server 2016 Standard (64 bits).

Pour en savoir plus sur le fonctionnement de KATA, *consultez l'aide de Kaspersky Anti Targeted Attack Platform*.

Sur les ordinateurs dotés du module Endpoint Sensor, il faut autoriser la connexion entrante avec le serveur KATA directement, sans passer par un serveur proxy.

Gestion de la tâche

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center 11 Web Console, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration ;
- des tâches pour la sélection d'ordinateurs.

Vous pouvez créer n'importe quelle quantité de tâches de groupe, de tâches pour une sélection d'ordinateurs et de tâches locales. Pour en savoir plus sur l'utilisation des groupes d'administration, des sélections d'ordinateurs et des plages d'ordinateurs, consultez l' *aide de Kaspersky Security Center*.

Paramètres de gestion des tâches

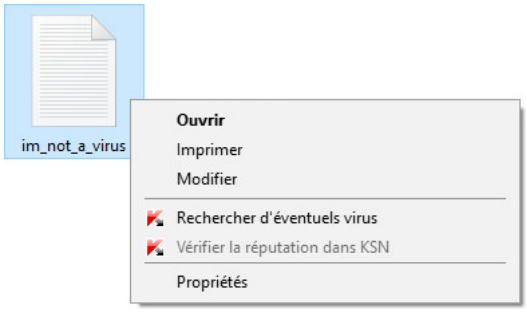
Paramètre	Description
Autoriser l'utilisation des tâches locales	Si la case est cochée, les tâches locales sont affichées dans l'interface locale de Kaspersky Endpoint Security. L'utilisateur, en l'absence de restrictions complémentaires de la stratégie, peut configurer les tâches et les lancer. Cependant, la configuration de la planification de

	l'exécution des tâches reste indisponible pour l'utilisateur. L'utilisateur ne peut exécuter des tâches que manuellement. Si la case est décochée, l'utilisation des tâches locales est interrompue. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. Les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de Kaspersky Endpoint Security ou via la ligne de commande. L'utilisateur peut toujours lancer la recherche de virus dans un fichier ou un dossier en choisissant l'option **Rechercher d'éventuels virus** dans le menu contextuel du fichier ou le dossier. Dans ce cas, la tâche d'analyse sera lancée selon les valeurs de paramètres définies par défaut pour la tâche d'analyse personnalisée.
Autoriser l'affichage des tâches de groupe	Si la case est cochée, les tâches de groupe créées dans Web Console apparaissent dans l'interface locale de Kaspersky Endpoint Security.
Autoriser la gestion des tâches de groupe	Si la case est cochée, il est permis d'administrer depuis l'interface locale de Kaspersky Endpoint Security les tâches de groupe créées dans Web Console.

Analyse depuis le menu contextuel

Kaspersky Endpoint Security permet de rechercher d'éventuels virus et d'autres programmes qui constituent une menace, des fichiers depuis le menu contextuel.

Lors de l'exécution de la tâche *Analyse depuis le menu contextuel*, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.



Analyse depuis le menu contextuel

Paramètres de la tâche Analyse depuis le menu contextuel

Paramètre	Description
Action en cas de détection d'une menace	• **Désinfecter ; supprimer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. • **Désinfecter ; informer si la désinfection est impossible**. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky

	Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives. • **Notifier**. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.
Optimisation de l'analyse	L'optimisation de l'analyse permet de réduire la durée de l'analyse depuis le menu contextuel. Pour optimiser l'analyse, vous pouvez analyser uniquement les nouveaux fichiers et les fichiers modifiés et limiter la durée de l'analyse des fichiers distincts.
Analyser les archives	La case active/désactive l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Analyser les paquets de distribution	La case active / désactive l'analyse des paquets de distribution.
Analyser les fichiers aux formats Office	La case active/désactive la fonction qui permet au module Protection contre les fichiers malicieux d'analyser les fichiers au format Office DOC, DOCX, XLS, PPT et autres, lors de la recherche de virus. Les objets OLE appartiennent également aux fichiers au format Office.
Ne pas décompresser les fichiers composés de grande taille	Si la case est cochée, Kaspersky Endpoint Security n'analyse pas les fichiers composés dont la taille est supérieure à la valeur définie.

Analyse des disques amovibles

Kaspersky Endpoint Security prend en charge la recherche de virus et d'autres programmes présentant une menace sur les disques amovibles lors de leur connexion à l'ordinateur.

Paramètres de la tâche Analyse des disques amovibles

Paramètre	Description
Action à exécuter lors de la connexion d'un disque amovible	• **Ne pas analyser** • **Analyse détaillée** Si vous choisissez cette option, Kaspersky Endpoint Security analyse tous les fichiers situés sur le disque amovible, y compris les fichiers joints à l'intérieur des objets composés, dès que le disque amovible a été connecté. • **Analyse rapide** Si vous choisissez cette option, Kaspersky Endpoint Security analyse uniquement les fichiers de certains formats les plus exposés à l'infection et il ne décompacte pas les objets composés dès que le disque amovible a été connecté.
Taille maximale du disque amovible	Si la case est cochée, Kaspersky Endpoint Security exécute l'action sélectionnée dans la liste déroulante **Action à exécuter lors de la connexion d'un disque amovible** sur les disques amovibles dont la taille est inférieure à la taille maximale définie. Si cette case est décochée, Kaspersky Endpoint Security exécute l'action sélectionnée dans la liste déroulante **Action à exécuter lors de la connexion d'un disque amovible** sur tous les disques amovibles quelle que soit leur taille.

Afficher la progression de l'analyse	Si la case est cochée, Kaspersky Endpoint Security affiche la progression de l'analyse des disques amovibles dans une nouvelle fenêtre et dans la fenêtre **Tâches**. Si la case est décochée, Kaspersky Endpoint Security exécute l'analyse des disques amovibles en arrière-plan.
Interdire l'arrêt de la tâche d'analyse	Si la case est cochée, le bouton **Arrêter** de la fenêtre **Tâches** et le bouton **Arrêter** de la fenêtre **Recherche de virus** ne sont pas disponibles dans l'interface locale de Kaspersky Endpoint Security.

Analyse en arrière-plan

L'*analyse en arrière-plan* est un mode d'analyse de Kaspersky Endpoint Security dans le cadre duquel aucune notification n'est affichée pour l'utilisateur. L'analyse en arrière-plan requiert moins de ressources de l'ordinateur que les autres types d'analyse (par exemple, l'analyse complète). Dans ce mode, Kaspersky Endpoint Security analyse les objets de démarrage automatique, la mémoire du noyau et la partition du système. L'Analyse en arrière-plan est lancée dans les cas suivants :

- après la mise à jour des bases antivirus ;
- trente minutes après le lancement de Kaspersky Endpoint Security ;
- toutes les six heures ;
- quand un ordinateur est inactif pendant cinq minutes ou plus.

L'analyse en arrière-plan réalisée quand l'ordinateur est en veille est interrompue lorsque l'une des conditions suivantes est remplie :

- L'ordinateur est réactivé.

  Si l'analyse en arrière-plan n'a pas été réalisée depuis plus de dix jours, l'analyse n'est pas interrompue.

- L'ordinateur (ordinateur portable) est passé en mode batterie.

Lors de l'analyse en arrière-plan, Kaspersky Endpoint Security n'analyse pas les fichiers dont le contenu se trouve dans le stockage cloud OneDrive.

Paramètres de l'application

Vous pouvez configurer les paramètres généraux de l'application suivants :

- mode de fonctionnement ;
- autodéfense ;
- performances ;
- données pour le débogage ;

- État de l'ordinateur à l'application des paramètres

Paramètres de l'application

Paramètre	Description
Lancer Kaspersky Endpoint Security for Windows au démarrage de l'ordinateur	Si la case est cochée, Kaspersky Endpoint Security se lance après le démarrage du système d'exploitation et protège l'ordinateur de l'utilisateur tout au long de la session d'utilisation. Lorsque la case est décochée, Kaspersky Endpoint Security ne démarre pas après le chargement du système d'exploitation, tant que l'utilisateur ne le démarre pas manuellement. La protection de l'ordinateur est désactivée et les données des utilisateurs peuvent être exposées à des menaces.
Activer la Désinfection active	Si la case est cochée, une notification contextuelle apparaît à l'écran lorsqu'une activité malveillante est détectée dans le système d'exploitation. Dans sa notification, Kaspersky Endpoint Security propose à l'utilisateur d'effectuer une réparation de l'infection active. Une fois que l'utilisateur a approuvé cette procédure, Kaspersky Endpoint Security neutralise la menace. Une fois la procédure de désinfection avancée terminée, Kaspersky Endpoint Security redémarre l'ordinateur. La technologie de désinfection avancée utilise des ressources informatiques considérables, ce qui peut ralentir d'autres applications. La technologie de désinfection avancée est disponible uniquement sur les ordinateurs tournant sous un système d'exploitation Microsoft Windows pour postes de travail. Il est impossible d'utiliser la technologie de désinfection avancée sur les ordinateurs tournant sous un système d'exploitation Microsoft Windows pour serveurs de fichiers.
Utiliser Kaspersky Security Center en guise de serveur proxy pour l'activation	Si la case est cochée, le Serveur d'administration de Kaspersky Security Center est utilisé en tant que serveur proxy pour activer l'application.
Activer l'autodéfense	Lorsque cette case est cochée, Kaspersky Endpoint Security empêche la modification ou la suppression des fichiers d'application sur le disque dur, les processus de mémoire et les entrées dans le registre système.
Désactiver la gestion externe des services systèmes	Si la case est cochée, Kaspersky Endpoint Security bloque toutes les tentatives d'administration des services de l'application depuis l'extérieur de l'ordinateur. Lorsqu'une tentative est faite pour gérer les services d'application à distance, une notification s'affiche dans la barre des tâches de Microsoft Windows, au-dessus de l'icône de l'application (sauf si le service de notification a été désactivé par l'utilisateur).
Reporter les tâches planifiées en cas d'alimentation par batterie	Si la case est cochée, le mode d'économie d'énergie est activé. Kaspersky Endpoint Security reporte les tâches planifiées. Vous pouvez démarrer manuellement les tâches d'analyse et de mise à jour, si nécessaire.
Céder les ressources aux autres applications	Quand Kaspersky Endpoint Security exécute des tâches planifiées, la charge sur le processeur et les sous-systèmes de disque peut augmenter, ce qui ralentit les autres programmes. Si la case est cochée, quand la charge augmente, Kaspersky Security suspend l'exécution des tâches programmées et libère des ressources du système d'exploitation pour les autres programmes.
Activer l'enregistrement	Si la case est cochée, Kaspersky Endpoint Security écrit des vidages en cas

des fichiers de vidage	de panne. Si la case est cochée, Kaspersky Endpoint Security n'écrit pas de vidage. L'application supprime également les fichiers de vidage existants du disque dur de l'ordinateur.
Activer la protection des fichiers de vidage et des fichiers de traçage	Si la case est cochée, l'accès aux fichiers dump est accordé aux administrateurs système et locaux, ainsi qu'à l'utilisateur qui a activé l'enregistrement des dumps ou de la trace. L'accès aux fichiers de trace est accordé uniquement aux administrateurs système et locaux. Si la case est décochée, tout utilisateur peut accéder aux fichiers de vidage et aux fichiers de traçage.
État de l'ordinateur à l'application des paramètres	Les paramètres de l'affichage des états des ordinateurs client doté de l'application Kaspersky Endpoint Security dans Web Console en cas d'erreur d'application de la stratégie ou d'exécution de la tâche.

Paramètres du réseau

Vous pouvez configurer les paramètres du serveur proxy pour la connexion à Internet et la mise à jour des bases antivirus.

Paramètres du réseau

Paramètre	Description
Paramètres du serveur proxy	Paramètres du serveur proxy utilisé pour l'accès à Internet des utilisateurs des ordinateurs clients. Kaspersky Endpoint Security utilise ces paramètres pour certains modules de protection, notamment pour la mise à jour des bases de données et des modules de l'application. Pour la configuration automatique du serveur proxy, Kaspersky Endpoint Security utilise le protocole WPAD (Web Proxy Auto-Discovery Protocol). Si ce protocole ne permet pas d'identifier l'adresse IP et/ou le port du serveur proxy, Kaspersky Endpoint Security utilise l'adresse du serveur proxy, indiquée dans Microsoft Internet Explorer.
Ne pas utiliser le serveur proxy pour les adresses locales	Si cette case est cochée, Kaspersky Endpoint Security n'utilise pas de serveur proxy lors d'une mise à jour à partir d'un dossier partagé.
Ports contrôlés	• **Contrôler tous les ports réseau**. Le mode de contrôle des ports de réseau via lesquels les modules de protection (Protection contre les fichiers malicieux, Protection contre les menaces Internet, Protection contre les menaces par emails) contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur. • **Contrôler uniquement les ports sélectionnés**. Mode de contrôle des ports réseau dans le cadre duquel les modules de protection contrôlent uniquement les ports réseau sélectionnés par l'utilisateur. La liste des ports qui sont normalement utilisés pour le transfert des messages électroniques et le trafic réseau est reprise dans le kit de distribution du logiciel.
Analyser les connexions sécurisées	Si la case est cochée, les modules Protection contre les menaces Internet, Protection contre les menaces par emails et Contrôle Internet analysent le trafic réseau chiffré

	transmis selon les protocoles suivants : • SSL 3.0 ; • TLS 1.0 / TLS 1.1 / TLS 1.2. Kaspersky Endpoint Security n'analyse pas les connexions sécurisées établies par des applications pour lesquelles la case **Ne pas analyser le trafic réseau** de la fenêtre **Exclusions de l'analyse pour l'application** a été cochée.
Lors de l'accès à un domaine avec un certificat douteux	• **Autoriser** Si vous choisissez cette option, Kaspersky Endpoint Security autorise l'établissement d'une connexions réseau lors de l'accès à un domaine avec un certificat douteux. Si vous accédez à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui reprend un avertissement et la raison pour laquelle il est déconseillé de visiter ce domaine. Le lien de la page affichant le message d'avertissement permet à l'utilisateur d'accéder au site Internet demandé. Après que vous avez cliqué sur le lien, Kaspersky Endpoint Security n'affiche plus d'avertissements sur le certificat douteux pendant une heure quand vous accédez à d'autres ressources dans le même domaine. • **Interdire**. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau établie avec ce domaine en cas d'accès à un domaine avec un certificat douteux. Lors de l'accès à un domaine avec un certificat douteux, Kaspersky Endpoint Security affiche dans le navigateur une page HTML qui indique la raison pour laquelle l'accès à ce domaine est bloqué.
En cas d'erreur lors de l'analyse des connexions sécurisées	• **Couper la connexion**. Si vous choisissez cette option, Kaspersky Endpoint Security bloque la connexion réseau en cas d'erreur d'analyse d'une connexion chiffrée. Lorsque l'option **Interrompre la connexion** est sélectionnée, Kaspersky Endpoint Security supprime toutes les exclusions répertoriées dans la fenêtre **Domaines avec erreurs d'analyse**. • **Ajouter le domaine aux exclusions**. Si vous choisissez cette option, en cas d'erreur lors de l'analyse d'une connexion sécurisée, Kaspersky Endpoint Security ajoute le domaine dont l'accès est à l'origine de l'erreur à la liste des domaines avec erreurs d'analyse et il n'analyse pas le trafic réseau chiffré lors de l'accès à ce domaine.
Bloquer les connexions selon le protocole SSL 2.0	Si cette case est cochée, Kaspersky Endpoint Security bloque les connexions réseau établies via le protocole SSL 2.0. Si cette case est désactivée, Kaspersky Endpoint Security ne bloque pas les connexions réseau établies via le protocole SSL 2.0 et ne surveille pas le trafic réseau transmis via ces connexions.
Déchiffrer les connexions chiffrées à l'aide d'un	Si la case est cochée, Kaspersky Endpoint Security déchiffre et contrôle le trafic réseau transmis via les connexions chiffrées établies dans le navigateur à l'aide d'un certificat EV.

certificat EV	
Domaines de confiance	Liste des domaines pour lesquels Kaspersky Endpoint Security n'analyse pas les connexions réseau sécurisées.
Applications de confiance	Liste des applications dont l'activité n'est pas surveillée par Kaspersky Endpoint Security pendant son fonctionnement.

Exclusions

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Vous pouvez exclure de l'analyse des objets à l'aide des méthodes suivantes :

- indiquez le chemin d'accès au fichier ou au dossier ;
- saisissez le hash de l'objet ;
- Utilisez des masques :
  - Le caractère `*` (astérisque) remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
  - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.
  - Le caractère `?` (point d'interrogation) remplace n'importe quel caractère unique dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.
- Entrez le nom de l'objet en fonction de la classification de l'Encyclopédie des virus de Kaspersky (par exemple, un logiciel légitime qui pourrait être utilisé par des criminels pour endommager votre ordinateur ou vos données personnelles).

Exclusions de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Les exclusions de l'analyse permettent d'utiliser des applications légitimes qui pourraient être employées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques vers des sites Internet payants. Ce genre d'application n'est pas considéré comme un virus. Vous pouvez obtenir des informations détaillées sur les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'Encyclopédie des virus de Kaspersky.

Kaspersky Endpoint Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des exclusions de l'analyse sur les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque du nom de la menace conformément au classement de l'Encyclopédie des virus de Kaspersky. Par exemple, vous utilisez souvent dans le cadre de votre travail l'application Radmin prévue pour l'administration à distance des ordinateurs. Kaspersky Endpoint Security classe cette activité parmi les activités suspectes et peut la bloquer. Pour exclure le blocage d'une application, il est nécessaire de créer une exclusion de l'analyse dans laquelle vous indiquerez le nom ou le masque du nom selon la classification de l'Encyclopédie des virus de Kaspersky.

Si votre ordinateur est doté d'une application qui récolte et envoie des informations à traiter, Kaspersky Endpoint Security peut la considérer comme une application malveillante. Pour éviter cela, vous pouvez exclure ce programme de l'analyse, en configurant Kaspersky Endpoint Security de manière décrite dans ce document.

Les exclusions de l'analyse peuvent être utilisées pendant le fonctionnement des modules et des tâches suivants de l'application définis par l'administrateur du système :

- Détection comportementale.
- Protection contre les Exploits.
- Prévention des intrusions.
- Protection contre les fichiers malicieux.
- Protection contre les menaces Internet.
- Protection contre les menaces par emails.
- Tâches d'analyse.

Liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et réseau (y compris l'activité malveillante), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Endpoint Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Kaspersky Endpoint Security exclut de l'analyse toute application ajoutée à la liste des applications de confiance.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance. L'analyse ignore ensuite les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Endpoint Security considère comme suspectes peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic réseau d'un ordinateur par Kaspersky Endpoint Security et un autre logiciel antivirus) et d'améliorer les performances de l'ordinateur, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre programmes présentant une menace. Pour exclure entièrement l'application de l'analyse Kaspersky Endpoint Security, il est nécessaire d'utiliser les exclusions de l'analyse.

Paramètres des exclusions

Paramètre	Description
Objets à détecter	Quelle que soit la configuration des paramètres de Kaspersky Endpoint Security, l'application détecte et bloque toujours les virus, les vers et les chevaux de Troie. Ces programmes peuvent provoquer des dégâts considérables à votre ordinateur. • Virus, vers

Sous-catégorie : virus et vers (Viruses_and_Worms)

Niveau de la menace : élevé

Les virus et les vers classiques exécutent sur l'ordinateur des actions qui n'ont pas été autorisées par l'utilisateur. Ils peuvent créer leurs propres copies qui possèdent la capacité d'auto-reproduction.

Virus classique

Une fois que le virus classique s'est introduit dans un système, il infecte un fichier quelconque, s'y active, exécute son action malveillante, puis ajoute sa copie à d'autres fichiers.

Le virus classique se multiplie uniquement sur les ressources locales de l'ordinateur et il est incapable de s'introduire lui-même dans un autre ordinateur. Il peut pénétrer dans d'autres systèmes uniquement s'il ajoute sa copie dans un fichier enregistré dans un dossier partagé, sur un cédérom d'installation ou si l'utilisateur envoie un email avec le fichier infecté en pièce jointe.

Le code du virus classique peut s'introduire dans divers secteurs de l'ordinateur, du système d'exploitation ou de l'application. En fonction de l'environnement dans lequel ils évoluent, on parle de *virus de fichiers*, *virus de démarrage*, *virus de script* et *virus de macro*.

Les virus peuvent infecter des fichiers de diverses manières. Les virus *écraseurs* (overwriting) remplacent le code du fichier infecté par leur propre code et suppriment ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *parasites* (Parasitic) modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les *virus compagnons* (Companion) ne modifient pas les fichiers mais créent des copies. Lorsque le fichier infecté est exécuté, son double est lancé, à savoir le virus. Il existe également des *virus-liens* (Link), des virus *qui infectent les modules objets* (OBJ), des virus *qui infectent les bibliothèques de compilateur* (LIB), les virus *qui infectent les textes source des programmes* et d'autres.

Ver

Le code du ver, à l'instar de celui du virus classique, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Le ver doit son nom à sa capacité à "ramper" d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

La principale caractéristique qui distingue les vers entre eux est leur mode de diffusion. Le tableau suivant reprend une description des différents types de vers en fonction du mode de diffusion.

Mode de diffusion des vers

Type	Nom	Description
Email-Worm	Vers de courrier	Ils se diffusent via le email.

		L'email infecté contient un fichier joint avec la copie du ver ou un lien vers ce fichier sur un site compromis ou créé spécialement à cette fin. Lorsque vous ouvrez le fichier joint, le ver est activé. Lorsque vous cliquez sur le lien, téléchargez le fichier, puis ouvrez celui-ci, le ver commence également à exécuter ses actions malveillantes. Ensuite, il continue à diffuser ses copies après avoir trouvé d'autres adresses email auxquelles il envoie des messages infectés.
IM-Worm	Clients IM	Ils se propagent via les clients IM. En règle générale, ce ver envoie aux contacts un message contenant un lien vers la copie du ver sur un site. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.
IRC-Worm	Vers de chats	Ils se diffusent via les canaux IRC (Internet Relay Chats), ces systèmes qui permettent de discuter en temps réel avec d'autres personnes. Ce ver publie un fichier avec sa copie ou un lien vers celle-ci dans le chat. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.
Net-Worm	Vers de réseau (vers de réseaux informatiques)	Ils se diffusent via les réseaux informatiques. À la différence des autres types de vers, le ver de réseau se propage sans l'intervention de l'utilisateur. Il recherche une application vulnérable sur les ordinateurs du réseau local. Pour ce faire, il envoie un paquet réseau spécial (un exploit) qui contient le code du ver ou une partie de celui-ci. Si le réseau abrite un ordinateur "vulnérable", celui-ci acceptera le paquet. Une fois qu'il s'est complètement introduit dans cet ordinateur, le ver s'active.
Ver P2P	Vers de réseau d'échange de fichiers	Ils se propagent via les réseaux d'échange de fichiers pair à pair. Afin d'infiltrer le réseau d'échange de fichiers, le ver se copie dans le dossier d'échange de fichiers qui se trouve normalement sur l'ordinateur de l'utilisateur. Le réseau d'échange de fichiers affiche les informations relatives à ce fichier et l'utilisateur peut "trouver" le fichier infecté comme n'importe quel autre fichier, le télécharger puis l'ouvrir. Les vers plus sophistiqués imitent le protocole d'un réseau d'échange de fichiers en particulier : ils répondent positivement aux recherches et proposent leur copie pour le téléchargement.
Ver	Autres vers	Parmi ces autres vers, citons : • Les vers qui diffusent leur copie via les ressources réseau. A l'aide des fonctions du système d'exploitation, ils consultent les répertoires réseau accessibles, se connectent aux ordinateurs du réseau mondial et tentent d'ouvrir leur disque en libre accès. À la différence des types de vers décrits ci-dessus, ces autres vers ne peuvent pas s'activer de manière

		autonome, mais uniquement lorsque l'utilisateur ouvre le fichier contenant la copie du ver. • Les vers qui n'adoptent aucun des modes de diffusion décrits dans ce tableau (par exemple, ceux qui se propagent via les téléphones portables).

- Chevaux de Troie

Sous-catégories : chevaux de Troie (Trojan_programs)

Niveau de la menace : élevé

À la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie. Ils s'infiltrent sur les ordinateurs via email ou via le navigateur lorsque l'internaute visite un site infecté. Les chevaux de Troie sont exécutés sur intervention de l'utilisateur. Ils entament leur action malveillante directement après l'exécution.

Le comportement des chevaux de Troie sur l'ordinateur infecté varie. Parmi les fonctions principales des chevaux de Troie, citons le blocage, la modification ou la suppression d'informations ainsi que la perturbation du fonctionnement des ordinateurs ou des réseaux. De plus, les chevaux de Troie peuvent recevoir ou envoyer des fichiers, les exécuter, afficher des messages, contacter des pages Internet, télécharger des applications et les installer et redémarrer l'ordinateur.

Les individus malintentionnés utilisent souvent des "sélections" composées de divers chevaux de Troie.

Les types de comportement des chevaux de Troie sont décrits dans le tableau suivant.

Types de comportement des chevaux de Troie sur l'ordinateur infecté

Type	Nom	Description
Trojan-ArcBomb	Chevaux de Troie (bombes dans les archives)	Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur. Lorsque l'utilisateur tente de décompresser une archive de ce genre, l'ordinateur peut commencer à ralentir, voire à s'arrêter et le disque peut se remplir de données "vides". Ces "bombes" sont particulièrement dangereuses pour les serveurs de fichiers et de messagerie. Si le serveur utilise un système de traitement automatique des données entrantes, ce genre de "bombe d'archive" peut entraîner l'arrêt du serveur.
Backdoor	Chevaux de Troie pour l'administration à distance	Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs. Ces programmes s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu malintentionné d'administrer l'ordinateur à distance.
Trojan	Chevaux de Troie	Cette catégorie reprend les programmes malveillants suivants : • **Chevaux de Troie traditionnels**. Ils exécutent uniquement les fonctions fondamentales des chevaux de Troie :le blocage, la modification ou la suppression d'informations, la perturbation du

		fonctionnement des ordinateurs ou des réseaux. Ils ne possèdent pas les fonctions complémentaires caractéristiques d'autres chevaux de Troie décrits dans ce tableau. • **Chevaux de Troie "multicibles"**. Ils possèdent des fonctions complémentaires appartenant à divers types de chevaux de Troie.
Trojan-Ransom	Chevaux de Troie exigeant le versement d'une rançon	Ces programmes "prennent en otage" les données de l'ordinateur après les avoir modifiées ou bloquées ou perturbent le fonctionnement de l'ordinateur de telle manière que l'utilisateur n'est plus en mesure d'exploiter les données. L'individu malintentionné exige le versement d'une somme d'argent en échange de l'envoi d'un programme qui rétablira le fonctionnement de l'ordinateur et les données qu'il abrite.
Trojan-Clicker	Chevaux de Troie qui cliquent	Ils accèdent à des pages Internet depuis l'ordinateur de la victime : ils envoient des instructions au navigateur ou remplacent les adresses Internet conservées dans les fichiers système. Grâce à ces programmes malveillants, les individus malintentionnés organisent des attaques réseau ou augmentent le nombre de visites sur le site afin d'accroître le nombre d'affichages de bannières publicitaires.
Trojan-Downloader	Chevaux de Troie qui téléchargent	Ils accèdent à la page Internet de l'intrus, y téléchargent d'autres applications malveillantes et les installent sur l'ordinateur de l'utilisateur. Ils peuvent contenir le nom du fichier de l'application malveillante à télécharger ou le recevoir à partir de la page Internet consultée.
Trojan-Dropper	Chevaux de Troie qui procèdent à des installations	Ils enregistrent sur le disque, puis installent d'autres chevaux de Troie présents dans le corps de ces programmes. Les individus malintentionnés peuvent utiliser ce genre de chevaux de Troie pour : • Installer un programme malveillant à l'insu de l'utilisateur : ces chevaux de Troie n'affichent aucun message réel ou fictif (par exemple, messages relatifs à une erreur dans une archive ou à la version incorrecte du système d'exploitation) ; • Protéger un autre programme malveillant connu : tous les antivirus ne sont pas en mesure d'identifier un programme malveillant au sein d'un cheval de Troie qui réalise des installations.

Trojan-Notifier	Chevaux de Troie qui envoient des notifications	Ils signalent à l'individu malintentionné que la communication avec l'ordinateur infecté est établie et transmettent des informations relatives à l'ordinateur : adresse IP, numéro du port ouvert ou adresse email. Ils contactent l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. Ces programmes sont souvent utilisés dans les sélections de différents chevaux de Troie. Ils indiquent à l'individu malintentionné que les autres chevaux de Troie ont bien été installés sur l'ordinateur de l'utilisateur.
Trojan-Proxy	Chevaux de Troie faisant office de proxy	Ils permettent à l'individu malintentionné de contacter anonymement des pages Internet via l'ordinateur de la victime ; le plus souvent, ils sont utilisés pour diffuser du spam.
Trojan-PSW	Chevaux de Troie qui volent des mots de passe	Il s'agit de chevaux de Troie qui volent des mots de passe (Password Stealing Ware) ; ils volent les données des comptes des utilisateurs, les données d'enregistrement d'un logiciel. Ils recherchent les données confidentielles dans les fichiers système et dans la base de registre et les transmettent à leur "maître" via email ou via FTP sur la page Internet de l'individu malintentionné ou par d'autres méthodes. Certains de ces programmes appartiennent à des groupes particuliers décrits dans ce tableau. Il s'agit des chevaux de Troie qui volent les comptes bancaires (Trojan-Banker), des chevaux de Troie qui volent les données des utilisateurs des clients IM (Trojan-IM) et des chevaux de Troie qui volent les données des adeptes de jeux en ligne (Trojan-GameThief).
Trojan-Spy	Chevaux de Troie espions	Ils espionnent l'utilisateur et collectent des informations sur les actions qu'il effectue lorsqu'il travaille sur son ordinateur. Ils peuvent intercepter les données que l'utilisateur saisit au clavier, faire des captures d'écran ou collecter des listes d'applications actives. Une fois qu'ils ont obtenu ces informations, ils les transmettent à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Trojan-DDoS	Chevaux de Troie pour attaques réseau	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). Ces programmes infectent généralement plusieurs ordinateurs pour attaquer simultanément un serveur.

		Les programmes de type DoS lancent l'attaque depuis un ordinateur avec l'accord de l'utilisateur. Les programmes de type DDoS (Distributed DoS) lancent des attaques distribuées depuis plusieurs ordinateurs, à l'insu de l'utilisateur de l'ordinateur infecté.
Trojan-IM	Chevaux de Troie qui volent les données des utilisateurs de clients IM	Ils volent les numéros et les mots de passe des utilisateurs des clients IM. Ils transmettent ces informations à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Rootkit	Rootkits	Ils masquent d'autres applications malveillantes et leur activité, et prolongent ainsi la persistance de ces applications dans le système d'exploitation. Ils peuvent également dissimuler des fichiers, des processus dans la mémoire d'un ordinateur infecté ou des clés de registre qui exécutent des applications malveillantes. Les rootkits peuvent masquer l'échange de données entre les applications sur l'ordinateur de l'utilisateur et les autres ordinateurs du réseau.
Trojan-SMS	Chevaux de Troie qui envoient des messages SMS	Ils infectent des téléphones mobiles et les utilisent pour envoyer des messages SMS vers des numéros payants.
Trojan-GameThief	Chevaux de Troie qui volent les données des adeptes de jeux en ligne	Ils volent les comptes des adeptes de jeux en ligne ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens.
Trojan-Banker	Chevaux de Troie qui volent les données de comptes bancaires.	Ils volent les données des comptes bancaires ou les données des comptes de système de porte-monnaie électronique, puis ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens.
Trojan-Mailfinder des adresses email	Chevaux de Troie qui récoltent des adresses email	Ils recueillent les adresses email sur l'ordinateur et les envoient à l'individu malintentionné par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. Les individus malintentionnés utilisent ensuite ces adresses pour diffuser du spam.

- Outils malveillants

Sous-catégories : outils malveillants (Malicious_tools)

Niveau de danger : moyen

Contrairement aux autres types de logiciels malveillants, les outils malveillants n'exécutent pas leurs actions immédiatement après leur démarrage. Elles peuvent être stockées et lancées en toute sécurité sur l'ordinateur de l'utilisateur. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants, s'introduire dans des ordinateurs ou exécuter d'autres actions malveillantes.

Les différentes fonctionnalités des outils malveillants sont regroupées en types présentés dans le tableau suivant.

Fonctionnalités des outils malveillants

Type	Nom	Description
Constructor	Constructeurs	Ils permettent de créer de nouveaux virus, vers ou chevaux de Troie. Certains constructeurs sont dotés d'une interface standard à base de fenêtres qui permet, à l'aide de menus, de sélectionner le type de programme malveillant à créer, son mode de résistance face aux débogueurs ainsi que d'autres propriétés.
Dos	Attaques réseau	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service).
Exploit	Exploits	L'exploit est un ensemble de données ou de code qui exploite une vulnérabilité de l'application dans laquelle il est exécuté afin de réaliser une action malveillante quelconque sur l'ordinateur. Par exemple, un exploit peut écrire ou lire des fichiers ou contacter des pages Internet "infectées". Divers exploits exploitent les vulnérabilités de diverses applications et services réseau. L'exploit sous la forme d'un paquet réseau se transmet via le réseau vers de nombreux ordinateurs à la recherche d'ordinateurs possédant des services réseau vulnérables. L'exploit d'un fichier DOC utilise la vulnérabilité de l'éditeur de test. Il peut commencer à exécuter les fonctions intégrées par l'individu malintentionné lorsque l'utilisateur ouvre le fichier infecté. L'exploit intégré à un email recherche les vulnérabilités dans un client de messagerie quelconque. Il peut commencer à exécuter l'action malveillante dès que l'utilisateur ouvre le message infecté dans le client de messagerie.

		Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploites de type *Nuker* sont des paquets réseau qui mettent l'ordinateur hors service.
FileCryptor	Encodeurs	Ils encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus.
Flooder	Programmes de "pollution" du réseau	Ils envoient une multitude de messages via les canaux réseau. Les programmes utilisés pour polluer les canaux IRC (Internet Relay Chats) appartiennent à cette catégorie. La catégorie Flooder ne reprend pas les applications qui "polluent" le email, les clients IM et les systèmes mobiles. Ces programmes sont regroupés dans des catégories distinctes décrites dans ce tableau (Email-Flooder, IM-Flooder et SMS-Flooder).
HackTool	Outils de piratage	Ils permettent de s'emparer de l'ordinateur sur lequel ils sont installés ou d'attaquer un autre ordinateur(par exemple, ajout d'autres utilisateurs au système sans l'autorisation de la victime ; purge des journaux du système afin de dissimuler les traces de leur présence dans le système). Il s'agit de quelques sniffers qui possèdent des fonctions malveillantes telles que l'interception des mots de passe. Les sniffers sont des programmes qui permettent de consulter le trafic réseau.
Hoax	Canulars	Ils effraient l'utilisateur à l'aide de messages semblables à ceux que pourrait produire un virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu.
Spoofer	Utilitaires d'imitation	Ils envoient des messages et des requêtes réseau au départ d'adresses fictives. Les individus malintentionnés les utilisent pour se faire passer pour l'expéditeur.
VirTool	Instruments pour la modification des programmes malveillants	Ils permettent de modifier d'autres programmes malveillants afin de les rendre invisibles pour les logiciels antivirus.
Email-Flooder	Programmes qui "inondent" le email.	Ils envoient de nombreux messages aux adresses email du carnet d'adresses ("pollution du courrier"). Ce flux important de messages empêche l'utilisateur de lire le courrier utile.
IM-Flooder	Programmes de "pollution" des clients IM	Ils envoient de nombreux messages aux utilisateurs de clients IM. Ce flux important de messages empêche l'utilisateur de lire les messages utiles.
SMS-Flooder	Programmes de "pollution"	Ils envoient de nombreux messages SMS vers les téléphones portables.

	des messages SMS	

- Applications publicitaires

  Sous-catégorie: applications publicitaires (Adware)

  Niveau de la menace : moyen

  Les applications publicitaires montrent des publicités à l'utilisateur. Elles affichent des bannières publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. Certains d'entre elles recueillent également des informations marketing sur l'utilisateur qu'elles renvoient à l'auteur : par exemple, catégorie de sites Internet visités, mots clés utilisés dans les recherches. A la différence des chevaux de Troie espions, elles transmettent ces informations avec l'autorisation de l'utilisateur.

- Numéroteurs automatiques

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

Type	Nom	Description
Client-IRC	Clients de chats	Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants.
Dialer	Numéroteurs automatiques	Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.
Downloader	Programmes de téléchargement	Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché.
Monitor	Programmes de surveillance	Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs).
PSWTool	Récupérateur de mots de passe	Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs.
RemoteAdmin	Programmes d'administration à distance	Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer.

		Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions.
Server-FTP	Serveurs FTP	Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP.
Server-Proxy	Serveurs proxy	Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.
Server-Telnet	Serveurs Telnet	Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet.
Server-Web	Serveurs Internet	Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP.
RiskTool	Outils utilisés sur l'ordinateur local	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs.
NetTool	Outils réseau	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs.
Client-P2P	Clients de réseaux d'échange de fichiers	Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants.
Client-SMTP	Clients SMTP	Envoient les emails en mode caché. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.
WebToolbar	Barre d'outils Internet	Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche.
FraudTool	Pseudo-programmes	Ils se font passer pour d'autres programmes. Par exemple, il existe des

		pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien.

- Autres

Sous-catégorie : programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

Niveau de danger : moyen

La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

Type	Nom	Description
Client-IRC	Clients de chats	Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants.
Dialer	Numéroteurs automatiques	Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.
Downloader	Programmes de téléchargement	Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché.
Monitor	Programmes de surveillance	Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs).
PSWTool	Récupérateur de mots de passe	Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs.
RemoteAdmin	Programmes d'administration à distance	Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer.

		Les applications légitimes d'administration à distance se distinguent des Backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions.
Server-FTP	Serveurs FTP	Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP.
Server-Proxy	Serveurs proxy	Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.
Server-Telnet	Serveurs Telnet	Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet.
Server-Web	Serveurs Internet	Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP.
RiskTool	Outils utilisés sur l'ordinateur local	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs.
NetTool	Outils réseau	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs.
Client-P2P	Clients de réseaux d'échange de fichiers	Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants.
Client-SMTP	Clients SMTP	Envoient les emails en mode caché. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.
WebToolbar	Barre d'outils Internet	Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche.
FraudTool	Pseudo-programmes	Ils se font passer pour d'autres programmes. Par exemple, il existe des

		pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien.

- **Fichiers compressés qui peuvent nuire**

  Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX.

  Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois.

  Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

  Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

  Kaspersky Endpoint Security identifie les programmes suivants :

  - *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie.
  - *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.

- **Fichiers compressés à plusieurs reprises**

	Kaspersky Endpoint Security analyse les objets compressés et le module de décompression dans les archives autoextractibles SFX. Pour masquer les applications dangereuses et empêcher leur découverte par les logiciels antivirus, les individus malintentionnés les compressent à l'aide de programmes spéciaux ou compressent le même objet plusieurs fois. Les experts antivirus de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent. Si Kaspersky Endpoint Security découvre un de ces compresseurs dans un objet, celui-ci contient probablement un programme malveillant ou une application qui pourrait être utilisée par l'individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur. Kaspersky Endpoint Security identifie les programmes suivants : • *Les fichiers compressés qui peuvent nuire* : ils servent à compresser des programmes malveillants, des virus, des vers ou des chevaux de Troie. • *Fichiers compressés à plusieurs reprises* (niveau de menace moyen) : l'objet est compressé à trois reprises par un ou plusieurs outils de compression.

Exclusions de l'analyse	Tableau contenant les informations relatives aux exclusions de l'analyse.
	Vous pouvez exclure de l'analyse des objets à l'aide des méthodes suivantes :
	
	• indiquez le chemin d'accès au fichier ou au dossier ;
	
	• saisissez le hash de l'objet ;
	
	• Utilisez des masques :
	
	  • Le caractère `*` (astérisque) remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
	
	  • Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT située dans le dossier nommé `Dossier` et ses sous-dossiers. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.
	
	  • Le caractère `?` (point d'interrogation) remplace n'importe quel caractère unique dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Dossier\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Dossier` qui ont l'extension TXT et un nom composé de trois caractères.

	• Entrez le nom de l'objet en fonction de la classification de l'Encyclopédie des virus de Kaspersky (par exemple, un logiciel légitime qui pourrait être utilisé par des criminels pour endommager votre ordinateur ou vos données personnelles).
Applications de confiance	Tableau des applications de confiance dont l'activité n'est pas analysée par Kaspersky Endpoint Security. Le module Contrôle des applications régit le lancement de chacune des applications, que cette application figure ou pas dans le table des applications de confiance.
Utiliser le stockage système sécurisé des certificats	Si la case est cochée, Kaspersky Endpoint Security exclut du contrôle les applications signées par la signature numérique de confiance. Le module Prévention des intrusions place automatiquement ces applications dans le groupe De confiance. Si la case est décochée, la recherche de virus est exécutée, que l'application possède une signature numérique ou non. Le module Prévention des intrusions répartit les applications en groupes de confiance selon les paramètres définis.

Rapports et stockage

Rapports

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, aux événements de chiffrement des données, à l'exécution de chaque tâche d'analyse, de mise à jour et de vérification de l'intégrité et au fonctionnement de l'application dans son ensemble sont consignées dans des rapports.

Les rapports se trouvent dans le dossier ProgramData\Kaspersky Lab\KES\Report.

Stockage

La *Sauvegarde* une liste de copies de sauvegarde des fichiers qui ont été supprimés ou modifiés pendant le processus de désinfection. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès à ce dossier sont accordées aux utilisateurs du groupe Administrators. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Paramètres des rapports et du stockage

Paramètre	Description
Supprimer les rapports après X jours	Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle défini dans le champ à droite. La durée maximale de conservation par défaut des rapports est de 30 jours. A l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport.
Taille maximale du fichier N Mo	Si la case est cochée, la taille maximale du fichier de rapport est définie par la valeur du champ de droite. Par défaut, la taille maximale du fichier est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Endpoint Security

	supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale.
Supprimer les objets après X jours	Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle défini dans le champ à droite. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens de la sauvegarde.
Taille maximale du stockage N Mo	Si la case est cochée, la taille maximale du stockage des fichiers est définie par la valeur du champ de droite. Par défaut, la taille maximale est limitée à 100 Mo. Quand le stockage des données atteint la taille maximale configurée, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens jusqu'à ce que la taille du stockage repasse en-dessous de la valeur maximale autorisée.
Transfert des données au Serveur d'administration	La liste des événements survenus sur les ordinateurs client dont les données doivent être transmises au Serveur d'administration.

Interface

Vous pouvez configurer les paramètres de l'interface de l'application.

Paramètres de l'interface

Paramètre	Description
Interaction avec l'utilisateur	• **Avec interface complète**. Si la case est cochée, la fenêtre principale de l'application n'est pas disponible sur l'ordinateur client doté de Kaspersky Endpoint Security. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel de l'icône de Kaspersky Endpoint Security. • **Avec interface simplifiée**. Si la case est cochée, l'utilisateur qui travaille sur le poste client doté de Kaspersky Endpoint Security voit un dossier portant le nom de l'application dans le menu **Démarrer** ainsi que l'icône de Kaspersky Endpoint Security dans la zone de notification de la barre des tâches de Microsoft Windows et les pop-ups de notification. De plus, s'il possède les autorisations requises, il peut modifier les paramètres de l'application depuis l'interface de celle-ci. • **Sans interface**. Quand cette option est choisie, l'utilisateur qui travaille sur un ordinateur client doté de Kaspersky Endpoint Security ne voit aucun signe de fonctionnement de Kaspersky Endpoint Security, notamment l'animation de l'icône de l'application pendant l'exécution des tâches.
Notifications	Paramètres des notifications relatives aux événements survenus pendant l'utilisation de Kaspersky Endpoint Security et la consignation des informations relatives aux événements dans le journal de Kaspersky Endpoint Security et/ou dans le journal des événements de Microsoft Windows. Les types de notification suivants sont disponibles : • Messages affichés au-dessus de l'icône de l'application dans la zone de notification de la barre des tâches de Windows : ◦ Si vous devez choisir l'action que doit exécuter Kaspersky Endpoint Security suite à cet événement, une fenêtre de notification apparaît. ◦ Si vous ne devez pas sélectionner l'action de Kaspersky Endpoint Security suite à cet événement, un message contextuel s'affiche.

	• Messages envoyés par email.
Avertissements	Liste des catégories d'événements de l'application dont l'apparition entraîne la modification de l' icône de Kaspersky Endpoint Security dans la zone de notifications de la barre de tâches de Microsoft Windows(ou).
Notifications sur l'état des bases antivirus locales	Paramètres de notification sur le caractère dépassé des bases antivirus que l'application utilise.
Protection par mot de passe	Si le commutateur est activé, Kaspersky Endpoint Security requiert la saisie du nom d'utilisateur et du mot de passe si l'utilisateur tente d'exécuter une opération couverte par la zone d'application du mot de passe à l'aide de l'application.
Ressources Internet du Support Technique	Liste des liens vers les sites Internet contenant des informations sur le Support Technique de l'application Kaspersky Endpoint Security. Les liens ajoutés apparaissent dans la fenêtre **Support Technique** de l'interface locale de Kaspersky Endpoint Security aux côtés des liens standard.

Administration de l'application via la ligne de commande

Vous pouvez administrer Kaspersky Endpoint Security via la ligne de commande. Vous pouvez consulter la liste des commandes d'administration de l'application à l'aide de la commande `HELP`. Pour obtenir de l'aide sur la syntaxe d'une commande en particulier, saisissez `HELP <commande>`.

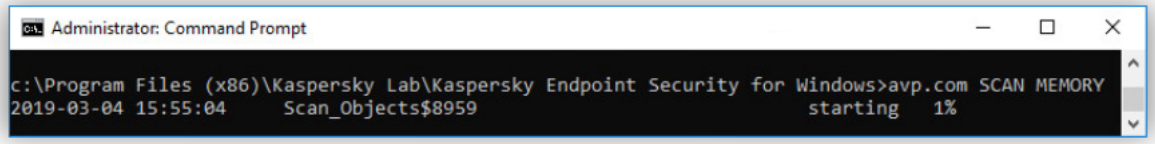
Commandes AVP

Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.
3. Utilisez le modèle suivant pour exécuter la commande :

```
avp.com <commande> [paramètres]
```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



Administration de l'application via la ligne de commande

SCAN. Recherche de virus

Lancer la tâche de recherche de virus.

Syntaxe de la commande

```
SCAN [<zone d'analyse>] [<action lorsqu'une menace est détectée>] [<types de fichiers>] [<exclusion de l'analyse>] [/ R [A]: <fichier de rapport>] [<technologie d'analyse>] [/ C: <fichier avec paramètres d'analyse>]
```

Zone d'analyse	
`<fichiers à analyser>`	Liste de fichiers et de dossiers séparés par un espace. Les longs chemins d'accès doivent être saisis entre guillemets. Les raccourcis (format MS-DOS) n'ont pas besoin d'être placés entre guillemets. Par exemple : • `"C:\Program Files (x86)\Example Folder"` : long chemin d'accès. • `C:\PROGRA~2\EXAMPL~1` : chemin court.

`/ALL`	Lancer la tâche *Analyse complète*. Kaspersky Internet Endpoint analyse les objets suivants : • Mémoire du noyau • Objets chargés au lancement du système d'exploitation • secteurs d'amorçage ; • Sauvegarde du système d'exploitation • tous les disques durs et amovibles.
`/MEMORY`	Analyser la mémoire du noyau.
`/STARTUP`	Analyser les objets chargés au lancement du système d'exploitation.
`/MAIL`	Analyser la boîte aux lettres Outlook.
`/REMDRIVES`	Analyser les disques amovibles.
`/FIXDRIVES`	Analyser les disques durs.
`/NETDRIVES`	Analyser les disques réseau.
`/QUARANTINE`	Analyser les fichiers dans la quarantaine de Kaspersky Endpoint Security.
`/@:<liste des fichiers.lst>`	Analyser les fichiers et les dossiers de la liste. Chaque fichier de la liste doit être saisi sur une nouvelle ligne. Les longs chemins d'accès doivent être saisis entre guillemets. Les raccourcis (format MS-DOS) n'ont pas besoin d'être placés entre guillemets. Par exemple : • `"C:\Program Files (x86)\Example Folder"` : long chemin d'accès. • `C:\PROGRA~2\EXAMPL~1` : chemin court.

Action en cas de détection d'une menace	
`/i0`	Notifier. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.
`/i1`	Désinfecter ; informer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si désinfection est impossible, Kaspersky Endpoint Security ajoute les informations relatives aux fichiers infectés détectés à la liste des menaces actives.
`/i2`	Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. Cette option est sélectionnée par défaut.
`/i3`	Désinfecter les fichiers infectés détectés. Si la désinfection est impossible, supprimer les fichiers infectés. Supprimer également les fichiers composés (par exemple, les archives) s'il est

	impossible de désinfecter ou de supprimer le fichier infecté.
`/i4`	Supprimer les fichiers infectés. Supprimer également les fichiers composés (par exemple, les archives) s'il est impossible de supprimer le fichier infecté.
`/i8`	Demander à l'utilisateur de confirmer l'action immédiatement après la détection d'une menace.
`/i9`	Demander à l'utilisateur de confirmer l'action après l'analyse.

Types de fichiers	
`/fe`	Fichiers analysés par extension. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables. Le format du fichier sera déterminé sur la base de son extension.
`/fi`	Fichiers analysés par format. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse uniquement les fichiers infectables. Avant de passer à la recherche du code malveillant dans le fichier, l'application analyse l'en-tête interne du fichier pour définir le format du fichier (par exemple, TXT, DOC, EXE). Lors de l'analyse, l'extension du fichier est également prise en compte.
`/fa`	Tous les fichiers. Si ce paramètre est sélectionné, Kaspersky Endpoint Security analyse tous les fichiers sans exception (quel que soit le format ou l'extension). Le paramètre est sélectionné par défaut.

Exclusions de l'analyse	
`-e:a`	Exclusion de l'analyse des archives au format RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
`-e:b`	Exclusion de l'analyse des bases de messagerie et des messages électroniques entrants et sortants.
`-e:<masque de fichier>`	Exclusion de l'analyse des fichiers sur la base d'un masque. Par exemple : • Le masque `*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe. • Le masque `example` reprend tous les chemins d'accès aux fichiers dont le nom est EXAMPLE.
`-e: <secondes>`	Exclusion de l'analyse des fichiers dont la durée d'analyse dépasse la valeur spécifiée en secondes.
`-es: <mégaoctets>`	Exclusion de l'analyse des fichiers dont la taille dépasse la valeur spécifiée en mégaoctets.

Mode de sauvegarde des événements dans le fichier de rapport.	
`/R:<fichier de rapport>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<fichier de rapport>`	Enregistrer tous les événements dans le fichier de rapport.

Technologies d'analyse	

`/iChecker=on|off`	La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse.
`/iSwift=on|off`	La technologie qui permet d'accélérer l'analyse en excluant certains fichiers. Les fichiers sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date de publication des bases de Kaspersky Endpoint Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse. La technologie iSwift est un outil développé à partir de la technologie iChecker pour le système de fichiers NTFS.

Paramètres complémentaires	
`/ C: <fichier avec paramètres de recherche de virus>`	Fichier avec les paramètres de la tâche de recherche de virus. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : `[<zone d'analyse>] [<action en cas de détection d'une menace>] [<types de fichiers>] [<exclusions de l'analyse>] [/R[A]:<fichier de rapport>] [<technologies d'analyse>]`.

Exemple :

- `avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" C:\Downloads\test.exe`
- `avp.com SCAN /C:scan_settings.txt`

UPDATE. Mise à jour des bases de données et des modules de l'application

Lancer la tâche *Mise à jour*.

Syntaxe de la commande

```
UPDATE [local]["<source de la mise à jour>"] [/R[A]:<fichier de rapport>] [/C:
<fichier avec les paramètres de mise à jour>]
```

Paramètres de la tâche de mise à jour	
`local`	Démarrage de la tâche de *mise à jour* qui a été créée automatiquement après l'installation de l'application. Vous pouvez modifier les paramètres de la tâche de *mise à jour* dans l'interface de l'application locale ou dans la console de Kaspersky Security Center. Si ce paramètre n'est pas configuré, Kaspersky Endpoint Security lance la tâche de *mise à jour* avec les paramètres par défaut ou avec les paramètres indiqués dans la commande. De cette façon, vous pouvez configurer les paramètres de la tâche Mise à jour, comme suit : • `UPDATE` lance la tâche de *mise à jour* avec les paramètres par défaut : la source de mise à jour correspond aux serveurs de mise à jour de Kaspersky, le compte est System et d'autres paramètres par défaut.

	• `UPDATE local` lance la tâche de *mise à jour* qui a été créée automatiquement après l'installation (tâche prédéfinie). • `UPDATE <paramètres de mise à jour>` lance la tâche de *mise à jour* avec des paramètres définis manuellement (voir ci-dessous).

Source des mises à jour	
`"<source de la mise à jour>"`	Adresse du serveur HTTP ou FTP ou du dossier partagé contenant le paquet de mises à jour. Vous ne pouvez indiquer qu'une seule source de mise à jour. Si la source des mises à jour n'est pas spécifiée, Kaspersky Endpoint Security utilise la source par défaut – les serveurs de mise à jour de Kaspersky Lab.

Mode de sauvegarde des événements dans le fichier de rapport.	
`/R:<fichier de rapport>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<fichier de rapport>`	Enregistrer tous les événements dans le fichier de rapport.

Paramètres complémentaires	
`/ C: <fichier avec les options de mise à jour>`	Fichier avec les paramètres de la tâche *Mise à jour*. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier peut avoir le contenu suivant : `["<source de mise à jour>"] [/ R [A]: <fichier de rapport>]`.

Exemple :

```
avp.com UPDATE local

avp.com UPDATE "ftp://mon_serveur/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Annulation de la dernière mise à jour

Annuler les dernières mises à jour des bases antivirus. Cela permet de revenir le cas échéant à l'utilisation de la version antérieure des bases et des modules de l'application, par exemple si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sûre.

Syntaxe de la commande

```
ROLLBACK [/R[A]:<fichier de rapport>]
```

Mode de sauvegarde des événements dans le fichier de rapport.	

`/R:<fichier de rapport>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<fichier de rapport>`	Enregistrer tous les événements dans le fichier de rapport.

Exemple :
```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Traces

Activer / désactiver le traçage. Par défaut, le traçage est désactivé.

Syntaxe de la commande

```
TRACES on | off [<niveau de traçage>] [<paramètres complémentaires>]
```

Niveau de traçage	
`<niveau de traçage>`	Niveau de détail du traçage Valeurs possibles : • `100` (critique). Uniquement les messages relatifs aux erreurs irrémédiables. • `200` (élevé). Messages relatifs à toutes les erreurs, y compris les erreurs irrémédiables. • `300` (diagnostique). Messages relatifs à toutes les erreurs et messages d'avertissement. • `400` (important). Messages relatifs à l'ensemble des erreurs, des avertissements, ainsi que des informations supplémentaires. • `500` (ordinaire). Messages relatifs à l'ensemble des erreurs, avertissements, ainsi que des informations détaillées sur le fonctionnement de l'application en mode normal (valeur par défaut). • `600` (bas). Tous les messages.

Paramètres complémentaires	
`all`	Exécuter la commande avec les paramètres `dbg`, `file` et `mem`.
`dbg`	Utiliser la fonction OutputDebugString et enregistrer le fichier de traçage. La fonction OutputDebugString envoie une chaîne de caractères au débogueur de l'application pour l'afficher. Pour en savoir plus, consulter le *site de MSDN*.
`file`	Enregistrer un fichier de traçage (sans limite de taille).
`rot`	Enregistrer les résultats du traçage dans un nombre limité de fichiers de taille limitée et écraser les anciens fichiers quand la limite est atteinte.
`mem`	Écrire les résultats du traçage dans les fichiers dump.

Exemples :

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Activation du profil

Lancer l'exécution du profil (par exemple, lancer la mise à jour des bases ou activer le module de protection).

Syntaxe de la commande

```
START <profil> [/R[A]:<fichier de rapport>]
```

Profil	
`<profil>`	Nom du profil. Un *profil* désigne un composant, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP START`.

Mode de sauvegarde des événements dans le fichier de rapport.	
`/R:<fichier de rapport>`	Enregistrer uniquement les événements critiques dans le fichier de rapport.
`/RA:<fichier de rapport>`	Enregistrer tous les événements dans le fichier de rapport.

Exemple :

```
avp.com START Scan_Objects
```

STOP. Désactivation du profil

Arrêter le profil en cours d'exécution (par exemple, arrêter l'analyse des disques amovibles ou désactiver le composant de protection).

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit jouir des autorisations **Configuration des paramètres de l'application**, **Désactivation des modules de la protection** et **Désactivation des modules de contrôle**.

Syntaxe de la commande

```
STOP <profil> /login=<nom d'utilisateur> /password=<mot de passe>
```

Profil	
`<profil>`	Nom du profil. Un *profil* désigne un composant, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP STOP`.

Autorisation	
`/login=<nom d'utilisateur> /password=<mot de passe>`	Données du compte de l'utilisateur dotés des autorisations indispensables de la Protection par mot de passe.

STATUS. État du profil

Afficher les informations sur l'état des profils de l'application (par exemple, `running` ou `completed`). Pour connaître la liste des profils disponibles, utilisez la commande `HELP STATUS`.

Kaspersky Endpoint Security affiche également les informations sur l'état des profils de service. Les profils de service peuvent être utiles lors de l'interaction avec le Support Technique de Kaspersky.

Syntaxe de la commande

```
STATUS [<profil>]
```

STATISTICS. Statistiques de l'exécution du profil

Afficher les statistiques sur le profil de l'application (par exemple, heure de l'analyse ou nombre de menaces détectées). Pour connaître la liste des profils disponibles, utilisez la commande `HELP STATISTICS`.

Syntaxe de la commande

```
STATISTICS <profils>
```

RESTORE. Restauration des fichiers

Restaurer un fichier depuis la Sauvegarde vers son emplacement d'origine. Si un fichier portant le même nom se trouve déjà à cet emplacement, le suffixe "-copy" est ajouté au nom du fichier. Le fichier restauré conserve son nom d'origine.

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit posséder l'autorisation **Restauration depuis la sauvegarde**.

La *Sauvegarde* est le stockage qui contient les copies de sauvegarde des objets qui ont été modifiés lors de la désinfection ou qui ont été supprimés. La *copie de sauvegarde* est une copie de fichier créée avant la désinfection ou la suppression de ce fichier. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Les copies de sauvegarde des fichiers sont enregistrées dans le dossier C:\ProgramData\Kaspersky Lab\KES\QB.

Les autorisations d'accès total à ce dossier sont accordées aux utilisateurs du groupe Administrateurs. Les autorisations d'accès limitées à ce dossier sont accordées à l'utilisateur, sous le compte duquel l'installation de Kaspersky Endpoint Security a eu lieu.

Kaspersky Endpoint Security n'offre pas la possibilité de configurer les autorisations d'accès des utilisateurs aux copies de sauvegarde des fichiers.

Syntaxe de la commande

```
RESTORE [/REPLACE] <nom du fichier> /login=<nom d'utilisateur> /password=<mot de passe>
```

Paramètres complémentaires	
`/REPLACE`	Écraser le fichier existant.
`<nom du fichier>`	Nom du fichier à restaurer.

Autorisation	
`/login=<nom d'utilisateur> /password=<mot de passe>`	Données du compte de l'utilisateur dotés des autorisations indispensables de la Protection par mot de passe.

Exemple :

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Exportation des paramètres de l'application

Exporter les paramètres de Kaspersky Endpoint Security dans un fichier. Le fichier est enregistré dans C:\Windows\SysWOW64.

Syntaxe de la commande

```
EXPORT <profil> <nom du fichier>
```

Profil	
`<profil>`	Nom du profil. Un *profil* désigne un composant, une tâche ou une fonction de Kaspersky Endpoint Security. Pour connaître la liste des profils disponibles, utilisez la commande `HELP`

	`EXPORT`.

Fichier à exporter	
`<nom du fichier>`	Nom dans lequel les paramètres de l'application vont être exportés. Vous pouvez exporter les paramètres du profil dans un fichier de configuration au format DAT ou CFG, un fichier au format TXT ou un document au format XML.

Exemples :

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importation des paramètres de l'application

Importer les paramètres de Kaspersky Endpoint Security depuis un fichier créé à l'aide de la commande `EXPORT`.

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit jouir des autorisations **Configuration des paramètres de l'application**, **Désactivation des modules de la protection** et **Désactivation des modules de contrôle**.

Syntaxe de la commande

```
IMPORT <nom du fichier> /login=<nom d'utilisateur> /password=<mot de passe>
```

Fichier à importer	
`<nom du fichier>`	Nom du fichier depuis lequel il faut importer les paramètres de l'application. Vous pouvez importer les paramètres de Kaspersky Endpoint Security depuis un fichier de configuration au format DAT ou CFG, un fichier au format TXT ou un document au format XML.

Autorisation	
`/login=<nom d'utilisateur> /password=<mot de passe>`	Données du compte de l'utilisateur dotés des autorisations indispensables de la Protection par mot de passe.

Exemple :

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Application du fichier clé

Appliquer un fichier clé pour activer Kaspersky Endpoint Security. Si l'application est déjà activée, la clé est ajoutée en tant que clé complémentaire.

Syntaxe de la commande

```
ADDKEY <nom du fichier> [/login=<nom d'utilisateur> /password=<mot de passe>]
```

Fichier clé	
`<nom du fichier>`	Nom du fichier de licence

Autorisation	
`/login=<nom d'utilisateur> /password=<mot de passe>`	Données du compte utilisateur Les données du compte utilisateur doivent être saisies uniquement si la Protection par mot de passe est activée.

Exemple :

```
avp.com ADDKEY file.key
```

LICENSE. Licence

Exécuter les opérations liées aux clés de l'application Kaspersky Endpoint Security.

Pour pouvoir exécuter la commande de suppression de clé de licence, la Protection par mot de passe doit être activée. L'utilisateur doit posséder l'autorisation **Suppression de la clé**.

Syntaxe de la commande

```
LICENSE <opération> [/login=<nom d'utilisateur /password=<mot de passe>]
```

Opération	
`/ADD <nom du fichier>`	Appliquer un fichier clé pour activer Kaspersky Endpoint Security. Si l'application est déjà activée, la clé est ajoutée en tant que clé complémentaire.
`/ADD <code d'activation>`	Activer Kaspersky Endpoint Security à l'aide d'un code d'activation. Si l'application est déjà activée, la clé est ajoutée en tant que clé complémentaire.
`/REFRESH <nom du fichier>`	Renouveler la durée de validité de la licence à l'aide d'un fichier clé. Ceci a pour effet d'ajouter une clé complémentaire. Elle est activée à l'expiration de la licence. Il est impossible d'ajouter une clé active à l'aide de cette commande.
`/REFRESH <code d'activation>`	Renouveler la durée de validité de la licence à l'aide d'un code d'activation. Ceci a pour effet d'ajouter une clé complémentaire. Elle est activée à l'expiration de la licence. Il est impossible d'ajouter une clé active à l'aide de cette commande.
`/DEL /login=<nom d'utilisateur> /password=<mot de passe>`	Supprimer la clé de licence La clé complémentaire est également supprimée.

Autorisation	

`/login=<nom d'utilisateur> /password=<mot de passe>`	Données du compte de l'utilisateur dotés des autorisations indispensables de la Protection par mot de passe.

Exemple :

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Achat d'une licence

Accéder au site de Kaspersky pour acheter une licence ou la renouveler.

PBATESTRESET. Réinitialiser les résultats de l'analyse avant le chiffrement

Réinitialiser les résultats de la vérification de la prise en charge du chiffrement du disque à l'aide de la technologie BitLocker. Les résultats évoquent également la compatibilité de l'ordinateur avec l'Agent d'authentification.

Avant de lancer le chiffrement du disque, l'application réalise une série de vérifications pour voir s'il est possible de chiffrer l'ordinateur à l'aide de la technologie BitLocker. Si le chiffrement est impossible, Kaspersky Endpoint Security enregistre les informations relatives à l'incompatibilité. Lors de la tentative de chiffrement suivante, l'application ne procède pas à la vérification mais signale que le chiffrement est impossible. Si la configuration matérielle a été modifiée, la vérification de la compatibilité du disque dur système avec l'Agent d'authentification ou de la prise en charge de la technologie BitLocker doit être précédée de la suppression des informations sur les incompatibilités obtenues par l'application lors de la vérification précédente.

EXIT. Quitter l'application

Arrêter Kaspersky Endpoint Security. L'application est déchargée de la mémoire vive de l'ordinateur.

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit avoir l'autorisation **Quitter l'application**.

Syntaxe de la commande

```
EXIT /login=<nom d'utilisateur> /password=<mot de passe>
```

EXITPOLICY. Désactiver la stratégie

Désactive la stratégie de Kaspersky Security Center sur l'ordinateur. Tous les paramètres de Kaspersky Endpoint Security peuvent être configurés, même les paramètres accompagnés d'un cadenas dans la stratégie ( ).

L'exécution de la commande requiert l'activation de la Protection par mot de passe. L'utilisateur doit posséder l'autorisation **Désactivation de la stratégie de Kaspersky Security Center**.

Syntaxe de la commande

```
EXITPOLICY /login=<nom d'utilisateur> /password=<mot de passe>
```

STARTPOLICY. Activation de la stratégie

Activer la stratégie de Kaspersky Security Center sur l'ordinateur. Les paramètres de l'application sont alors configurés conformément à la stratégie.

DISABLE. Désactivation de la protection

Désactiver la Protection contre les fichiers malicieux sur un ordinateur doté d'une licence pour Kaspersky Endpoint Security expirée. Il est impossible d'exécuter la commande sur un ordinateur sur lequel l'application n'a pas été activée ou qui ne possède pas une licence active.

SPYWARE. Détection de logiciels espion

Activer/désactiver la détection de logiciels espion. La détection de logiciels espion est activée par défaut.

Syntaxe de la commande

```
SPYWARE on|off
```

Commandes KESCLI

Les commandes KESCLI vous permettent de recevoir des informations à propos de l'état de la protection de l'ordinateur à l'aide du module OPSWAT, et d'effectuer des tâches standards, comme l'analyse des virus et la mise à jour des bases de données.

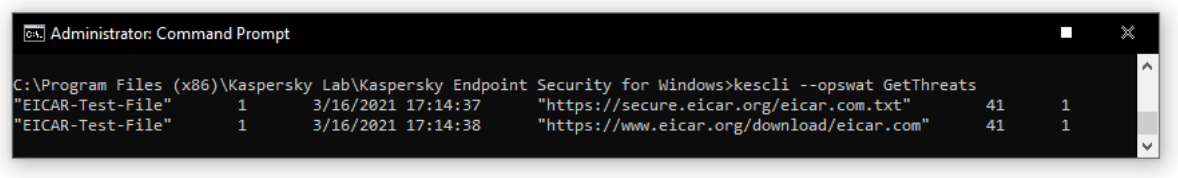
Vous pouvez consulter la liste des commandes KESCLI à l'aide de la commande `--help` ou en utilisant la commande abrégée `-h`.

Pour gérer Kaspersky Endpoint Security via la ligne de commande, procédez comme suit :

1. Lancez l'interpréteur de ligne de commande cmd au nom de l'administrateur.
2. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Endpoint Security.
3. Utilisez le modèle suivant pour exécuter la commande :

```
kescli <commande> [paramètres]
```

En conséquence, Kaspersky Endpoint Security exécute la commande (cf. ill. ci-dessous).



Administration de l'application via la ligne de commande

Analyse. Recherche de virus

Lancer la tâche de recherche de virus.

Syntaxe de la commande

```
--opswat Scan <zone d’analyse> <action en cas de détection d’une menace>
```

Vous pouvez vérifier l'état d'achèvement de la tâche *Analyse complète* à l'aide de la commande `GetScanState` et afficher la date et l'heure de la dernière analyse à l'aide de la commande `GetLastScanTime`.

Zone d'analyse	
`<fichiers à analyser>`	Liste de fichiers et de dossiers séparés par le symbole `;`. Par exemple, `C:\Program Files (x86)\Exemple de dossier`.

Action en cas de détection d'une menace	
`0`	Notifier. Si vous choisissez cette option, Kaspersky Endpoint Security, après avoir découvert des fichiers infectés, ajoute les informations relatives à ces fichiers dans la liste des menaces actives.
`1`	Désinfecter ; supprimer si la désinfection est impossible. Si cette option est sélectionnée, Kaspersky Endpoint Security essaie de désinfecter automatiquement tous les fichiers infectés qu'il a détectés. Si la désinfection est impossible, alors Kaspersky Endpoint Security les supprime. Cette option est sélectionnée par défaut.

Exemple :

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. État d'achèvement de l'analyse

Recevez des informations à propos de l'état d'achèvement de la tâche *Analyse complète* :

- `1` : l'analyse est en cours.
- `0` : l'analyse n'est pas en cours.

Syntaxe de la commande

```
--opswat GetScanState
```

Exemple :
`kescli --opswat GetScanState`

GetLastScanTime. Calcul du temps requis pour l'analyse

Recevez des informations à propos de la date et de l'heure d'achèvement de la dernière tâche *Analyse complète*.

Syntaxe de la commande

```
--opswat GetLastScanTime
```

Exemple :
`kescli --opswat GetLastScanTime`

GetThreats. Collecte de données à propos des menaces détectées

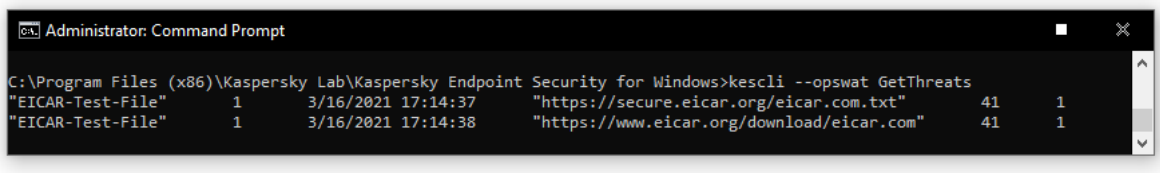
Recevez une liste des menaces détectées (*rapport sur les menaces*). Ce rapport contient des informations à propos des menaces et de l'activité des virus au cours des 30 derniers jours précédant la création du rapport.

Syntaxe de la commande

```
--opswat GetThreats
```

Lorsque cette commande est exécutée, Kaspersky Endpoint Security envoie une réponse au format suivant :

`<nom de l'objet détecté>` `<type d'objet>` `<date et heure de détection>` `<chemin d'accès au fichier>` `<action en cas de détection d'une menace>` `<niveau de danger de la menace>`



Administration de l'application via la ligne de commande

Type d'objet	

0	Inconnu (Inconnu).
1	Virus (Virware).
2	Chevaux de Troie (Trojware).
3	Programmes malveillants (Programme malveillant).
4	Programmes publicitaires (Programme publicitaire).
5	Numéroteurs automatiques (Programme pornographique).
6	Applications qui pourraient être utilisées par un cybercriminel pour nuire à l'ordinateur ou aux données de l'utilisateur (Programme à risque).
7	Objets compressés dont la méthode d'emballage peut être utilisée pour protéger du code malveillant (Compressé)
20	Objets inconnus (Xfiles).
21	Applications connues (Logiciel).
22	Fichiers cachés (Masqué).
23	Application nécessitant une attention particulière (Pupware).
24	Comportement anormal (Anomalie).
30	Non déterminé (Non détecté).
40	Bannières publicitaires (Bannière).
50	Attaque réseau (Attaque).
51	Accès au registre (Registre).
52	Activité suspecte (Soupçon).
60	Vulnérabilités (Vulnérabilité).
70	Phishing.
80	Pièce jointe indésirable (Pièce jointe).
90	Programme malveillant détecté par Kaspersky Security Network (Urgent).
100	Lien inconnu (URL suspecte).
110	Autre programme malveillant (Comportemental).

Action en cas de détection d'une menace	
0	Inconnu (inconnu).
1	La menace a été éliminée (ok).
2	L'objet a été infecté et n'a pas été désinfecté (infecté).
5	L'objet se trouve dans une archive et n'a pas été désinfecté (archive).
9	L'objet a été désinfecté (désinfecté).
10	L'objet n'a pas été désinfecté (non désinfecté).
11	L'objet a été supprimé (supprimé).
13	Une copie de sauvegarde de l'objet a été créée (sauvegardé).

15	L'objet a été déplacé vers la Sauvegarde (`quarantaine`).
23	L'objet a été supprimé au redémarrage de l'ordinateur (`supprimé au redémarrage`).
25	L'objet a été désinfecté au redémarrage de l'ordinateur (`désinfecté au redémarrage`).
29	L'objet a été déplacé vers la Sauvegarde par un utilisateur (`ajouté par l'utilisateur`).
30	L'objet a été ajouté aux exclusions (`ajouté aux exclusions`).
31	L'objet a été déplacé vers la Sauvegarde au redémarrage de l'ordinateur (`quarantaine au redémarrage`).
36	Faux positif (`fausse alerte`).
38	Le processus a été interrompu (`interrompu`).
40	L'objet n'a pas été détecté (`non trouvé`).
41	Impossible de traiter la menace (`non traitable`).
42	L'objet a été restauré (`restauré`).
43	L'objet a été créé à la suite d'une menace (`créé par une menace`).
44	L'objet a été restauré au redémarrage de l'ordinateur (`restauré au redémarrage`).
`0xffffffff`	L'objet n'a pas été traité (`abandonné`).

Niveau de danger de la menace	
`0`	Inconnu
`1`	Élevé
`2`	Analyse standard
`4`	Faible
`8`	Informations (inférieur à *Faible*)

UpdateDefinitions. Mise à jour des bases de données et des modules de l'application

Lancer la tâche *Mise à jour*. Kaspersky Endpoint Security utilise la source par défaut : les serveurs de mises à jour de Kaspersky.

Syntaxe de la commande

```
--opswat UpdateDefinitions
```

Vous pouvez afficher la date et l'heure de la dernière tâche *Mise à jour* terminée à l'aide de la commande `GetDefinitionsetState`.

Exemple :

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Calcul du temps requis pour la mise à jour

Recevez des informations à propos de la date et de l'heure d'achèvement de la dernière tâche *Mise à jour*.

Syntaxe de la commande

```
--opswat GetDefinitionState
```

Exemple :

```
kescli --opswat GetDefinitionState
```

EnableRTP. Activation de la protection

Sur l'ordinateur, activez les modules de protection suivants de Kaspersky Endpoint Security : Protection contre les fichiers malicieux, Protection contre les menaces Internet, Protection contre les menaces par emails, Protection contre les menaces réseau et Prévention des intrusions.

Syntaxe de la commande

```
--opswat EnableRTP
```

Vous pouvez vérifier l'état de fonctionnement de la Protection contre les fichiers malicieux à l'aide de la commande `GetRealTimeProtectionState`.

Exemple :

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. États de la Protection contre les fichiers malicieux

Recevez des informations à propos de l'état de fonctionnement du module Protection contre les fichiers malicieux :

- `1` : le module est activé.
- `0` : le module est désactivé.

Syntaxe de la commande

```
--opswat GetRealTimeProtectionState
```

Exemple :

```
kescli --opswat GetRealTimeProtectionState
```

Version. Identification de la version de l'application

Identifiez la version de Kaspersky Endpoint Security for Windows.

Syntaxe de la commande

```
--Version
```

Vous pouvez également utiliser la commande abrégée `-v`.

Exemple :
`kescli -v`

Application. Profils d'application

Un *profil* désigne un composant, une tâche ou une fonction de Kaspersky Endpoint Security. Les profils sont prévus pour administrer l'application via la ligne de commande. Vous pouvez utiliser des profils pour exécuter les commandes `SART`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` et `IMPORT`. Les profils permettent de configurer les paramètres de l'application (par exemple, `STOP DeviceControl`) ou de lancer une tâche (par exemple `START Scan_My_Computer`).

Les profils suivants sont disponibles :

- `AdaptiveAnomaliesControl` : contrôle évolutif des anomalies.
- `AMSI` : fournisseur de protection AMSI.
- `BehaviorDetection` : Détection comportementale.
- `DeviceControl` : Contrôle des périphériques.
- `EntAppControl` : Contrôle des applications.
- `File_Monitoring` ou `FM` : protection contre les fichiers malicieux.
- `Firewall` ou `FW` : Pare-feu.
- `HIPS` : Prévention des intrusions.
- `IDS` : Protection contre les menaces réseau.
- `IntegrityCheck` : Vérification de l'intégrité.
- `Mail_Monitoring` ou `EM` : Protection contre les menaces par emails.
- `Rollback` : Restauration de la mise à jour.
- `Scan_ContextScan` : Analyse depuis le menu contextuel.

- `Scan_IdleScan` : Analyse en arrière-plan.
- `Scan_Memory` : Analyse de la mémoire du noyau.
- `Scan_My_Computer` : Analyse complète.
- `Scan_Objects` : Analyse personnalisée.
- `Scan_Qscan` : Analyse des objets chargés au lancement du système d'exploitation.
- `Scan_Removable_Drive` : Analyse des disques amovibles.
- `Scan_Startup` ou `STARTUP` : Analyse des zones critiques.
- `Updater` : Mise à jour.
- `Web_Monitoring` ou `WM` : Protection contre les menaces Internet.
- `WebControl` : Contrôle Internet.

Kaspersky Endpoint Security prend également en charge l'utilisation de profils de service. Les profils de service peuvent être utiles lors de l'interaction avec le Support Technique de Kaspersky.

Sources d'informations sur l'application

Page de Kaspersky Endpoint Security sur le site Internet de Kaspersky

La page de Kaspersky Endpoint Security fournit des informations générales sur l'application, ses possibilités et ses particularités de fonctionnement.

La page de Kaspersky Endpoint Security propose un lien vers la boutique en ligne. Vous pourrez y acheter l'application ou prolonger vos droits d'utilisation.

Page de Kaspersky Endpoint Security dans la Base des connaissances

La *base de connaissances* est une rubrique du site du Support technique.

La page de Kaspersky Endpoint Security dans la base de connaissances propose des articles reprenant des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la base de connaissances peuvent répondre à des questions concernant non seulement Kaspersky Endpoint Security, mais également d'autres applications de Kaspersky. Ces articles peuvent également contenir des actualités du Support technique.

Discussion sur les applications de Kaspersky entre les membres de la communauté d'utilisateurs.

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky et aux autres utilisateurs de nos applications dans notre communauté.

Dans cette communauté, vous pouvez afficher les sujets existants, laisser vos commentaires et créer de nouveaux sujets de discussion.

Contacter le Support Technique

Cette section contient les informations sur les modes et les sur les conditions d'obtention d'assistance technique.

Comment obtenir une assistance technique

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans d'autres sources d'informations relatives à Kaspersky Endpoint Security, contactez le Support technique. Les experts du Support technique répondront à vos questions sur l'installation et l'utilisation de Kaspersky Endpoint Security.

Kaspersky fournit une assistance pour Kaspersky Endpoint Security pendant son cycle de vie (consultez la page relative au cycle de vie de l'application). Avant de contacter le Support Technique, veuillez prendre connaissance des règles d'octroi de l'assistance technique.

Vous pouvez contacter les experts du Support technique d'une des manières suivantes :

- En visitant le site Internet du Support Technique
- Envoyer une demande au Support Technique de Kaspersky via le portail Kaspersky CompanyAccount.

Support technique via Kaspersky CompanyAccount

Le Kaspersky CompanyAccount est un portail dédié aux entreprises qui utilisent des applications Kaspersky. Le portail Kaspersky CompanyAccount permet aux utilisateurs d'interagir avec les experts de Kaspersky par le biais de requêtes électroniques. Le portail Internet Kaspersky CompanyAccount permet de suivre le traitement des requêtes envoyées aux experts de Kaspersky et de conserver l'historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte Kaspersky CompanyAccount. Un compte permet de gérer de manière centralisée les requêtes électroniques des employés inscrits chez Kaspersky ainsi que de gérer les autorisations de ces employés au sein du Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien ;
- Allemand
- Polonais
- Portugais
- Russe
- Français

- Japonais

Vous pouvez également obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique.

Récupération d'informations pour le Support Technique

Une fois que les experts du Support Technique de Kaspersky sont au courant du problème survenu, ils peuvent vous demander de créer un *fichier de traçage*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

De plus, les experts du Support Technique peuvent avoir besoin d'informations complémentaires sur le système d'exploitation, les processus lancés sur l'ordinateur, ainsi que des rapports détaillés sur le fonctionnement des modules de l'application.

Lorsque les opérateurs du Support Technique cherchent à poser un diagnostic, ils peuvent vous demander de modifier certains paramètres de l'application :

- Activer la fonctionnalité de récupération des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules séparés de l'application, qui n'est pas disponibles via les outils standards de l'interface d'utilisateur.
- Modifier les paramètres de conservation des informations diagnostiques récupérées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Toutes les informations nécessaires pour exécuter les actions citées (la description de la suite des étapes, les paramètres modifiables, les fichiers de configuration, les scripts, les possibilités complémentaires de la ligne de commande, les modules de réparation, les utilitaires spécialisés, etc.), ainsi que la composition des données récupérées à des fins de débogage vous sont transmises par les experts du Support Technique. Les informations diagnostiques élargies récupérées sont enregistrées sur l'ordinateur de l'utilisateur. L'envoi automatique des données récupérées à Kaspersky n'est pas exécuté.

Les actions citées ci-dessus doivent être exécutées uniquement sous l'administration des experts du Support Technique à l'aide des instructions reçues. La modification indépendante des paramètres d'utilisation de l'application via les moyens, non décrits dans le Manuel de l'administrateur ou dans les recommandations des experts du Support Technique, peut amener au ralentissement et aux échecs dans le système d'exploitation, à la baisse du niveau de sécurité et à la perturbation de l'accessibilité et de l'intégrité des informations traitées.

Création d'un fichier de trace de l'application

La *trace de l'application* désigne l'enregistrement détaillé des activités de l'application et des messages sur les événements survenus pendant le fonctionnement de l'application.

Pour créer un fichier de trace de l'application, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Support Technique**.

   La fenêtre **Support Technique** s'ouvre.

2. Dans la fenêtre **Support Technique**, cliquez sur le bouton **Suivi du système**.

La fenêtre **Informations pour le Support Technique** s'ouvre.

3. Pour lancer le traçage, choisissez un des éléments suivants dans la liste déroulante **Trace de l'application** :

   - **activée**

     Choisissez cette option pour activer le traçage.

   - **Avec rotation**.

     Choisissez cette option pour activer le traçage et limiter la quantité maximale de fichiers de traçage et la taille maximale de chacun des fichiers de traçage. Quand le nombre maximum de fichiers de traçage de la taille maximale a été atteint, le fichier de traçage le plus ancien est supprimé et l'écriture d'un nouveau fichier de traçage débute.

     Si vous choisissez cette option, vous pouvez choisir une valeur pour les champs suivants :

     - **Nombre maximal de fichiers pour la rotation**

       Ce champ permet de désigner le nombre maximal de fichiers de traçage enregistrés.

     - **Taille maximale de chaque fichier**

       Ce champ permet de désigner la taille maximale de chacun des fichiers de traçage enregistrés.

4. Choisissez le niveau de traçage dans la liste déroulante **Niveau**.

   Il est recommandé de demander au spécialiste du Support Technique le niveau de traçage requis. Si les indications du Support Technique sont absentes, il est recommandé d'installer le niveau de traçage **Normal (500)**.

5. Relancez Kaspersky Endpoint Security.

6. Pour arrêter le traçage, revenez à la fenêtre **Informations pour le Support Technique** et choisissez l'option **Désactivé** dans la liste déroulante **Trace de l'application**.

Vous pouvez créer aussi les fichiers de traçage pendant l'installation de l'application via la ligne de commande, y compris avec l'aide du fichier setup.ini.

Création d'un fichier de trace des performances

La *trace des performances* désigne l'enregistrement détaillé des actions exécutées par l'application qui sont liées aux performances de l'application.

Pour créer un fichier de trace des performances, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Support Technique**.

   La fenêtre **Support Technique** s'ouvre.

2. Dans la fenêtre **Support Technique**, cliquez sur le bouton **Suivi du système**.

   La fenêtre **Informations pour le Support Technique** s'ouvre.

3. Pour lancer le traçage, choisissez un des éléments suivants dans la liste déroulante **Trace des performances** :

   - **activée**

Choisissez cette option pour activer le traçage.

- **Avec rotation**.

  Choisissez cette option pour activer le traçage et limiter la taille maximale du fichier de trace. Quand la taille du fichier atteint la valeur maximale, les nouveaux enregistrements écrasent les enregistrements plus anciens du fichier.

  Si vous avez choisi cette option, vous pouvez définir la taille maximale du fichier de trace dans le champ **Taille maximale du fichier**.

4. Choisissez un des niveaux de traçage suivants dans la liste déroulante **Niveau**.

   - **Léger. Si vous avez choisi cette option, alors pendant le traçage** Kaspersky Endpoint Security analyse les processus fondamentaux du système d'exploitation liés aux performances.

   - **Détaillé. Si vous avez choisi cette option, alors pendant le traçage** Kaspersky Endpoint Security analyse tous les processus du système d'exploitation liés aux performances.

5. Choisissez un des niveaux de traçage suivants dans la liste déroulante **Type de traçage**.

   - **Informations de base**. Si vous choisissez cette option, le traçage s'opère tandis que le système d'exploitation fonctionne.

   - **Au redémarrage. Si vous choisissez cette option, le traçage s'opère au redémarrage du système d'exploitation.**

6. Relancez Kaspersky Endpoint Security.

7. Pour arrêter le traçage, revenez à la fenêtre **Informations pour le Support Technique** et choisissez l'option **Désactivé** dans la liste déroulante **Trace des performances**.

Une fois le fichier de trace créé, vous pouvez procéder au téléchargement des résultats du traçage sur le serveur de Kaspersky.

À propos de la composition et de la conservation des fichiers de trace

L'utilisateur est seul responsable de la sécurité des informations récupérées, et plus exactement du contrôle et de la restriction de l'accès aux informations récupérées et conservées sur l'ordinateur avant leur envoi à Kaspersky.

Les fichiers de traçage sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application.

Les fichiers de traçage sont conservés dans le dossier ProgramData\Kaspersky.

Le fichier de trace a le format de nom suivant : `KES<numéro de version_dateXX.XX_timeXX.XX_pidXXX.><Type de fichier de trace>.log`.

Le fichier de trace de l'agent d'authentification est stocké dans le dossier Informations sur le volume système et porte le nom suivant : `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Vous pouvez consulter les données consignées dans les fichiers de traçage.

Tous les fichiers de traçage contiennent les données communes suivantes :

- Heure de l'événement.
- Numéro du flux d'exécution.

  Ces informations ne contiennent pas le fichier de traçage de l'Agent d'authentification.

- Module de l'application à l'origine de l'événement.
- Degré de gravité de l'événement (information, avertissement, critique, erreur).
- Description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande.

Kaspersky Endpoint Security enregistre les mots de passe de l'utilisateur dans le fichier de traçage uniquement sous forme chiffrée.

Contenu des fichiers de traçage SRV.log, GUI.log et ALL.log

Les fichiers de traçage SRV.log, GUI.log et ALL.log peuvent contenir, outre les informations générales, les informations suivantes :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur l'ordinateur local.
- Nom d'utilisateur et mot de passe s'ils sont transmis en clair. Ces données peuvent être consignées dans les fichiers de traçage lors de l'analyse du trafic Internet. Le trafic consigné dans les fichiers de traçage provient uniquement de trafmon2.ppl.
- Nom d'utilisateur et mot de passe s'ils figurent dans les en-têtes du protocole HTTP.
- Nom du compte utilisateur d'accès à Microsoft Windows, si celui-ci fait partie du nom du fichier.
- Votre adresse de messagerie électronique ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.
- Les sites Internet que vous visitez ainsi que les liens de ces sites. Ces données sont consignées dans les fichiers de traçage lorsque l'application analyse les sites Internet.
- Adresse du serveur proxy, nom de l'ordinateur, adresse IP, nom de l'utilisateur employé pour l'autorisation sur le serveur Proxy. Ces données sont consignées dans les fichiers de traçage si l'application utilise un serveur proxy.
- Adresses IP externes d'où la connexion avec votre ordinateur a été établie.
- Objet du message, identifiant, nom de l'expéditeur et adresse de la page Internet de l'expéditeur du message dans le réseau social. Ces données sont consignées dans les fichiers de traçage si le module Contrôle Internet est activé.

Contenu des fichiers de traçage HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Le fichier de traçage HST.log contient, outre les données générales, les informations relatives à l'exécution de la tâche de mise à jour des bases de données de l'application et des modules.

Le fichier de traçage BL.log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement de l'application, ainsi que les données indispensables à la résolution des problèmes de fonctionnement de l'application. Ce fichier est créé si l'application est lancée avec le paramètre avp.exe –bl.

Le fichier de trace Dumpwriter.log contient, outre les données générales, les informations de service indispensables à la résolution des problèmes survenus pendant l'écriture du fichier dump de l'application.

Le fichier de trace WD.log contient, outre les données générales, les informations sur les événements survenus pendant le fonctionnement du service avpsus, y compris les événements de mise à jour des modules de l'application.

Le fichier de traçage AVPCon.dll.log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu du fichier de traçage du module Fournisseur de protection AMSI

Outre les données générales, le fichier de traçage AMSI.log contient des informations sur les résultats des analyses sollicitées par des applications tierces.

Contenu du fichier de traçage du composant Protection contre les menaces par emails

Le fichier de traçage mcou.OUTLOOK.EXE.log peut contenir une partie des messages, y compris les adresses email.

Contenu du fichier de traçage du composant Analyse depuis le menu contextuel

Le fichier de traçage shellex.dll.log contient, outre les données générales, des informations sur l'exécution de la tâche d'analyse et les données nécessaires à l'élimination des incidents dans le fonctionnement de l'application.

Contenu des fichiers de traçage des plug-ins Internet de l'application

Les fichiers de traçage sont conservés sur l'ordinateur doté de Kaspersky Security Center 11 Web Console, dans le dossier Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 11\logs. Web Console commence à enregistrer les données après l'installation et supprime les fichiers de traçage après sa suppression.

Les fichiers de traçage pour Kaspersky Endpoint Security sont nommés de la manière suivante : `logs-kes_windows-<type du fichier de traçage>.DESKTOP-<date de la mise à jour du fichier>.log`.

Les fichiers de traçage des plug-ins Internet de l'application contiennent, outre les données générales, les informations suivantes :

- le mot de passe de l'utilisateur KLAdmin pour le déverrouillage de l'interface Kaspersky Endpoint Security (Protection par mot de passe) ;
- le mot de passe temporaire pour le déverrouillage de l'interface de Kaspersky Endpoint Security (Protection par mot de passe) ;
- le nom d'utilisateur et le mot de passe pour le serveur de messagerie SMTP (Notifications par e-mail) ;
- le nom d'utilisateur et le mot de passe pour le serveur proxy du réseau Internet (Serveur proxy) ;

- le nom d'utilisateur et le mot de passe pour la tâche *Modification de la sélection des modules de l'application* ;
- les identifiants et les chemins indiqués dans les propriétés de la stratégie et les tâches de Kaspersky Endpoint Security.

Contenu du fichier de traçage de l'agent d'Authentification

Le fichier de trace de l'agent d'Authentification contient, outre les données générales, les informations sur le fonctionnement de l'Agent d'authentification et sur les actions exécutée par l'utilisateur dans l'Agent d'authentification.

A propos de la création et de l'enregistrement des fichiers dump

Les vidages enregistrés peuvent contenir des données confidentielles. Afin de garantir le contrôle et la restriction de l'accès à ces données, il vous incombe de garantir vous-même la protection des fichiers dump.

Les fichiers dump sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application. Les fichiers dump sont conservés dans le dossier ProgramData\Kaspersky Lab.

Le fichier dump contient toutes les informations relatives à la mémoire de travail des processus de Kaspersky Endpoint Security au moment de la création de ce fichier dump. Le fichier dump peut contenir également des données personnelles.

Activation et désactivation de l'enregistrement des fichiers dump

Pour activer ou désactiver l'enregistrement des fichiers dump, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans une gauche partie, choisissez la sous-section **Paramètres de l'application** de la section **Paramètres généraux**.

   Les paramètres de l'application s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Données pour le débogage**, cliquez sur le bouton **Configuration**.

   La fenêtre **Données pour le débogage** s'ouvre.
4. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'enregistrement des fichiers dump** si vous souhaitez que l'application enregistre des fichiers dump pour l'application.
   - Décochez la case **Activer l'enregistrement des fichiers dump** si vous ne souhaitez pas que l'application enregistre des fichiers dump pour l'application.
5. Cliquez sur le bouton **OK** dans la fenêtre **Données pour le débogage**.
6. Cliquez sur le bouton **Enregistrer** dans la fenêtre principale de l'application afin d'enregistrer les modifications introduites.

Activation et désactivation de la protection des fichiers dump et de trace

Les fichiers dump et les fichiers de traçage contiennent des informations sur le système d'exploitation, ainsi que des données de l'utilisateur. Pour empêcher l'accès non autorisé à ces données, vous pouvez activer la protection des fichiers dump et des fichiers de traçage.

Si la protection des fichiers dump et des fichiers de traçage est activée, l'accès aux fichiers est réservé aux utilisateurs suivants :

- Les fichiers dump sont accessibles aux administrateurs local et système ainsi qu'à l'utilisateur qui a activé l'enregistrement des fichiers dump et des fichiers de traçage.
- Les fichiers de traçage sont accessibles uniquement aux administrateurs local et système.

Pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage, procédez comme suit :

1. Dans la fenêtre principale de l'application, cliquez sur le bouton **Configuration**.
2. Dans une gauche partie, choisissez la sous-section **Paramètres de l'application** de la section **Paramètres généraux**.

   Les paramètres de l'application s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Données pour le débogage**, cliquez sur le bouton **Configuration**.

   La fenêtre **Données pour le débogage** s'ouvre.
4. Exécutez une des actions suivantes :

   - Cochez la case **Activer la protection des fichiers dump et des fichiers de trace** si vous souhaitez activer la protection.
   - Décochez la case **Activer la protection des fichiers dump et des fichiers de trace**, si vous voulez désactiver la protection.
5. Cliquez sur le bouton **OK** dans la fenêtre **Données pour le débogage**.
6. Cliquez sur le bouton **Enregistrer** dans la fenêtre principale de l'application afin d'enregistrer les modifications introduites.

Les fichiers dump et les fichiers de traçage enregistrés alors que la protection étaient activées resteront protégés même après la désactivation de cette fonction.

Glossaire

Agent d'administration

Module de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce module est unique pour toutes les applications de Kaspersky qui fonctionnent sous Windows. Des versions distinctes de l'Agent d'administration sont prévues pour les applications qui fonctionnent sous d'autres systèmes d'exploitation.

Agent d'authentification

Interface permettant après le chiffrement du secteur d'amorçage du disque de réaliser la procédure d'authentification pour accéder aux disques durs chiffrés et pour charger le système d'exploitation.

Archive

Un ou plusieurs fichiers réunis au sein d'un fichier compressé. La compression et la décompression des données requièrent une application spéciale : un outil de compression.

Base des URL de phishing

Une liste d'adresses Web que les spécialistes de Kaspersky ont jugées liées au phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky.

Base des URL malveillantes

Liste des adresses de sites Internet dont le contenu pourrait constituer une menace. La liste est créée par des spécialistes de Kaspersky. Il est régulièrement mis à jour et est inclus dans le kit de distribution d'applications Kaspersky.

Bases antivirus

Bases de données contenant des informations sur les menaces de sécurité informatique connues de Kaspersky à la date de sortie de la base de données antivirus. Les signatures de base de données antivirus aident à détecter le code malveillant dans les objets analysés. Ces bases antivirus sont créées par les experts de Kaspersky et mises à jour toutes les heures.

Certificat de licence

Document fourni par Kaspersky avec le fichier clé ou le code d'activation. Il contient les informations concernant la licence octroyée.

Clé active

Clé utilisée au moment actuel pour faire fonctionner l'application.

Clé complémentaires

Clé qui confirme le droit d'utilisation de l'application, mais non utilisée pour le moment.

Connecteur de l'Agent d'administration

Fonction de l'application qui garantit la communication de l'application avec l'Agent d'administration. L'Agent d'administration permet d'administrer l'application à distance via Kaspersky Security Center.

Émetteur de certificat

Centre de certification qui a émis le certificat.

Faux positif

Situation où un fichier non infecté est considéré comme infecté par l'application de Kaspersky car son code évoque celui d'un virus.

Fichier infecté

Fichier qui contient un code malveillant (pendant l'analyse le code d'une application présentant une menace connue a été détecté). Les experts de Kaspersky vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

Forme normalisée de l'adresse du site Internet

La forme normalisée de l'adresse du site Internet est une représentation écrite de l'adresse du site Internet obtenue grâce à la normalisation. La normalisation est un processus de modification de la représentation écrite de l'adresse du site Internet conformément aux règles spécifiques (par exemple, exclusion du nom d'utilisateur, du mot de passe et du port de connexion de la représentation écrite de l'adresse du site Internet, conversion des caractères majuscules de l'adresse du site Internet en caractères minuscules).

Le but de la normalisation des adresses des sites Internet dans le contexte du fonctionnement des modules de protection est de vérifier une seule fois les adresses des sites Internet qui ont une équivalence physique, mais qui sont différentes du point de vue de la syntaxe.

Exemple :

La forme non normalisée de l'adresse : www.Example.com\.

La forme normalisée de l'adresse : www.example.com.

Groupe d'administration

Ensemble d'appareils regroupés selon les fonctions exécutées et les applications de Kaspersky installées. Les périphériques sont regroupés pour en faciliter la gestion dans son ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

Masque

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- Le caractère `*` (astérisque) remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` désigne tous les chemins d'accès aux fichiers portant l'extension .txt qui se trouvent dans n'importe quel dossier sur le disque C.

- Le caractère `?` (point d'interrogation) remplace n'importe quel caractère unique dans un nom de fichier ou de dossier, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\**\???.txt` reprend le chemin d'accès à tous les fichiers portant l'extension txt et dotés d'un nom de trois caractères qui se trouve dans les dossiers du disque C.

Il faut prendre en considération que le nom est toujours séparé de l'extension du fichier par un point.

Objet OLE

Fichier attaché ou intégré à un autre fichier. Les applications de Kaspersky permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel® dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

Réparation d'objets

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Certains objets infectés ne peuvent pas être désinfectés.

Tâche

Fonctions exécutées par l'application de Kaspersky sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète du périphérique, Mise à jour des bases de données.

Trusted Platform Module

Puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Le Trusted Platform Module s'installe en général sur la carte mère de l'ordinateur et interagit avec les autres modules du systèmes via le bus matériel.

Zone d'analyse

Objets analysés par Kaspersky Endpoint Security pendant l'exécution de l'analyse.

Zone de protection

Objets analysés en permanence durant le fonctionnement du module de protection principale. Les propriétés de la zone de protection des modules différents peuvent varier.

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

Notice sur les marques de commerce

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash, Reader et Shockwave sont des marques ou des marques déposées d'Adobe Systems Incorporated enregistrées aux États-Unis et/ou dans d'autres pays.

Apple, FireWire et Safari sont des marques d'Apple Inc. déposées aux Etats-Unis et dans d'autres pays.

AutoCAD est une marque ou une marque déposée aux Etats-Unis et/ou dans d'autres pays qui appartient à Autodesk, Inc. et/ou à ses filiales.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Borland est une marque ou une marque déposée de Borland Software Corporation aux Etats-Unis et dans d'autres pays.

Chrome, Google Chrome et Google Talk sont des marques de Google, Inc.

Citrix et Citrix Provisioning Services sont des marques de Citrix Systems, Inc. et/ou de ses filiales déposée à l'office des brevets des Etats-Unis et d'autres pays.

dBase est une marque de dataBased Intelligence, Inc.

EMC et SecurID sont des marques de commerce ou des marques déposées d'EMC Corporation aux États-Unis et/ou dans d'autres pays.

Radmin est une marque déposée de Famatech.

IBM est une marque d'International Business Machines Corporation déposées dans plusieurs juridictions à travers le monde.

ICQ est une marque ou une marque de service de ICQ LLC.

Intel est une marque d'Intel Corporation déposée aux États-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds déposée aux États-Unis et dans d'autres pays.

Logitech est une marque ou une marque déposée de Logitech aux États-Unis et (ou) dans d'autres pays.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MultiPoint, Outlook, PowerPoint, PowerShell, Segoe, Skype, Visual C++, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server et Windows Store sont des marques de Microsoft Corporation déposées aux États-Unis et dans d'autres pays.

Mozilla, Firefox et Thunderbird sont des marques de Mozilla Foundation.

Java et JavaScript sont des marques déposées de la société Oracle et/ou de ses filiales.